Copyright 2018 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC.

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

⚠️ WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

⚠️ CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

ℹ️ IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Safeguard Administration Guide
Updated - August 2018
Version - 2.3
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>19</td>
</tr>
<tr>
<td>Introduction to One Identity Safeguard</td>
<td>19</td>
</tr>
<tr>
<td>Key features</td>
<td>20</td>
</tr>
<tr>
<td>What's new in One Identity Safeguard 2.1</td>
<td>22</td>
</tr>
<tr>
<td>What's new in One Identity Safeguard 2.2</td>
<td>24</td>
</tr>
<tr>
<td>What's new in One Identity Safeguard 2.3</td>
<td>26</td>
</tr>
<tr>
<td>One Identity Safeguard Appliance specifications</td>
<td>27</td>
</tr>
<tr>
<td><strong>System requirements</strong></td>
<td>29</td>
</tr>
<tr>
<td>Desktop client system requirements</td>
<td>29</td>
</tr>
<tr>
<td>Web client system requirements</td>
<td>30</td>
</tr>
<tr>
<td>Supported platforms</td>
<td>31</td>
</tr>
<tr>
<td>Product licensing</td>
<td>33</td>
</tr>
<tr>
<td><strong>Installing the One Identity Safeguard desktop client</strong></td>
<td>35</td>
</tr>
<tr>
<td>Installing the desktop client</td>
<td>35</td>
</tr>
<tr>
<td>Starting the desktop client</td>
<td>36</td>
</tr>
<tr>
<td>Uninstalling the desktop client</td>
<td>36</td>
</tr>
<tr>
<td><strong>Setting up One Identity Safeguard for the first time</strong></td>
<td>37</td>
</tr>
<tr>
<td>Step 1: Authorizer Administrator creates administrators</td>
<td>38</td>
</tr>
<tr>
<td>Step 2: Appliance Administrator configures the appliance</td>
<td>38</td>
</tr>
<tr>
<td>Step 3: User Administrator adds users</td>
<td>39</td>
</tr>
<tr>
<td>Step 4: Asset Administrator adds managed systems</td>
<td>39</td>
</tr>
<tr>
<td>Step 5: Directory Administrator adds external identity stores</td>
<td>40</td>
</tr>
<tr>
<td>Step 6: User Administrator (or Authorizer Administrator) adds directory groups</td>
<td>40</td>
</tr>
<tr>
<td>Step 7: Security Policy Administrator adds access request policies</td>
<td>40</td>
</tr>
<tr>
<td><strong>Getting acquainted with the console</strong></td>
<td>42</td>
</tr>
<tr>
<td>Toolbar</td>
<td>42</td>
</tr>
<tr>
<td>Settings</td>
<td>43</td>
</tr>
<tr>
<td>User avatar</td>
<td>44</td>
</tr>
<tr>
<td>Navigation pane</td>
<td>45</td>
</tr>
<tr>
<td>Home</td>
<td>46</td>
</tr>
</tbody>
</table>
Dashboard .......................................................................................................................... 48
Access Requests .................................................................................................................. 48
Account Automation .......................................................................................................... 49
Activity Center ..................................................................................................................... 50
Applying search criteria ....................................................................................................... 51
Saving search criteria ........................................................................................................... 53
Generating an activity audit log report .................................................................................. 54
Scheduling an activity audit log report .................................................................................. 55
Editing or deleting a saved search or scheduled report .......................................................... 56
Viewing event details ............................................................................................................ 57
Auditing request workflow .................................................................................................... 57
Filtering report results ........................................................................................................... 59
Sorting report results ............................................................................................................ 59
Reports ................................................................................................................................ 60
Running an entitlement report ............................................................................................... 60
Administrative Tools ............................................................................................................. 61
Toolbar .................................................................................................................................. 63
Search box ............................................................................................................................. 65

Privileged access requests .................................................................................................... 69
Creating, editing, or removing a favorite request ................................................................. 70
Configuring alerts ................................................................................................................... 72
Toast notifications .................................................................................................................. 72
Email notifications ................................................................................................................... 73
Password release request workflow ...................................................................................... 73
Requesting a password release ............................................................................................... 73
Taking action on a password release request ......................................................................... 76
Approving a password release request .................................................................................. 77
Reviewing a completed password release request ................................................................ 79
Session request workflow ...................................................................................................... 79
About sessions and recordings ............................................................................................... 80
Requesting session access ..................................................................................................... 81
Taking action on a session request .......................................................................................... 84
Approving a session request ................................................................................................... 86
Launching the SSH client ......................................................................................................... 87
Launching an RDP session ....................................................................................................... 88
Reviewing a session request ................................................................. 90
Replaying a session ........................................................................... 91
Following and terminating a "live" session ........................................ 92

Toolbox .............................................................................................. 93
Viewing task status ........................................................................... 93
Stopping a task .................................................................................. 94

Accounts ............................................................................................ 95
General tab ......................................................................................... 96
Access Request Policies tab ............................................................... 98
Account Groups tab .......................................................................... 99
Check and Change Log tab ............................................................... 99
History tab .......................................................................................... 100
Exporting data .................................................................................. 101
Managing accounts ........................................................................... 102
Adding an account ............................................................................ 102
Adding a cloud platform account ..................................................... 104
Manually adding a tag to an account ................................................ 106
Adding an account to account groups .............................................. 106
Modifying an account ...................................................................... 107
Deleting an account ......................................................................... 107
Importing objects ............................................................................. 108
Creating an import file ...................................................................... 109
Checking, changing, or setting an account password ....................... 110
Viewing password archive ............................................................... 112

Account Groups ................................................................................ 113
General tab ......................................................................................... 114
Accounts tab ...................................................................................... 114
Access Request Policies tab .............................................................. 115
History tab .......................................................................................... 116
Managing account groups ................................................................. 117
Adding an account group ................................................................. 118
Adding a dynamic account group ..................................................... 118
General tab ........................................................................................ 119
Asset Account Rules tab ................................................................. 119
Assets tab .................................................................168
Access Request Policies tab ........................................169
History tab ...............................................................169
Managing asset groups .................................................171
  Adding an asset group ...............................................171
  Adding a dynamic asset group .....................................172
    General tab ................................................................172
    Asset Rules tab .......................................................173
    Summary tab ..........................................................174
  Adding assets to an asset group ....................................174
  Modifying an asset group ............................................175
  Deleting an asset group ..............................................175

Directories ......................................................................177
  General tab ..................................................................179
  Accounts tab ................................................................181
  Profiles tab ..................................................................183
    About profiles ..........................................................184
  Discovered Accounts tab .............................................185
  History tab ....................................................................186
  Managing directories ....................................................188
    Adding a directory .....................................................188
      General tab ............................................................189
        Attributes tab .......................................................191
    Checking a directory's connectivity ...............................193
    Adding directory accounts to a directory .......................193
    Managing directory account discovery jobs ....................195
      General tab ............................................................195
        Rules tab ...............................................................196
    Setting directory account passwords .............................198
    Creating a directory profile ........................................199
    Modifying a directory profile ......................................200
    Setting a default directory profile ................................201
    Adding accounts to a directory profile ............................201
    Modifying a directory ................................................202
    Deleting a directory ...................................................203
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updates</td>
<td>265</td>
</tr>
<tr>
<td>Asset Management settings</td>
<td>266</td>
</tr>
<tr>
<td>Account Discovery</td>
<td>267</td>
</tr>
<tr>
<td>Adding an asset account discovery setting</td>
<td>268</td>
</tr>
<tr>
<td>Directory Tags</td>
<td>271</td>
</tr>
<tr>
<td>Adding a tag for dynamic tagging of directory accounts</td>
<td>272</td>
</tr>
<tr>
<td>Deleting a directory account tag</td>
<td>274</td>
</tr>
<tr>
<td>Modifying a directory account tag</td>
<td>275</td>
</tr>
<tr>
<td>Copying a directory account tag to another directory</td>
<td>277</td>
</tr>
<tr>
<td>Viewing directory account tag assignments</td>
<td>278</td>
</tr>
<tr>
<td>Tags</td>
<td>278</td>
</tr>
<tr>
<td>Adding a tag for dynamic tagging of assets or asset accounts</td>
<td>279</td>
</tr>
<tr>
<td>Deleting an asset or asset account tag</td>
<td>283</td>
</tr>
<tr>
<td>Modifying an asset or asset account tag</td>
<td>284</td>
</tr>
<tr>
<td>Copying an asset or asset account tag to another partition</td>
<td>287</td>
</tr>
<tr>
<td>Viewing asset and asset account tag assignments</td>
<td>288</td>
</tr>
<tr>
<td>Backup and Retention settings</td>
<td>288</td>
</tr>
<tr>
<td>About backups</td>
<td>289</td>
</tr>
<tr>
<td>Archive Servers</td>
<td>289</td>
</tr>
<tr>
<td>Adding an archive server</td>
<td>290</td>
</tr>
<tr>
<td>Audit Log Management</td>
<td>292</td>
</tr>
<tr>
<td>Safeguard Backup and Restore</td>
<td>292</td>
</tr>
<tr>
<td>Run Now</td>
<td>294</td>
</tr>
<tr>
<td>Backup Settings</td>
<td>294</td>
</tr>
<tr>
<td>Download</td>
<td>295</td>
</tr>
<tr>
<td>Upload</td>
<td>295</td>
</tr>
<tr>
<td>Restore</td>
<td>296</td>
</tr>
<tr>
<td>Archive Backup</td>
<td>296</td>
</tr>
<tr>
<td>Safeguard Backup Retention</td>
<td>297</td>
</tr>
<tr>
<td>Certificates settings</td>
<td>297</td>
</tr>
<tr>
<td>About certificates</td>
<td>298</td>
</tr>
<tr>
<td>Audit Log Signing Certificate</td>
<td>299</td>
</tr>
<tr>
<td>Installing an audit log signing certificate</td>
<td>300</td>
</tr>
<tr>
<td>Creating a Certificate Signing Request for audit logs</td>
<td>300</td>
</tr>
<tr>
<td>Certificate Signing Request</td>
<td>301</td>
</tr>
</tbody>
</table>
Verifying SNMP configuration .................................................. 334
Starling .............................................................................. 334
Syslog ................................................................................. 336
Configuring a syslog server .................................................... 337
Verifying syslog server configuration ....................................... 337
Ticketing .............................................................................. 338
Configuring integration with external ticket system .................. 338
Messaging settings ................................................................. 339
Login Notification ................................................................ 339
Message of the Day ............................................................... 340
Profile settings ..................................................................... 340
Account Password Rules ....................................................... 341
Adding an account password rule ......................................... 341
Change Password .................................................................. 344
Adding change password settings .......................................... 344
Check Password .................................................................... 346
Adding check password settings ........................................... 347
Directory Account Password Rules ........................................ 348
Adding a directory account password rule ........................... 348
Directory Change Password .................................................. 350
Adding directory change password settings ........................ 351
Directory Check Password ..................................................... 352
Adding directory check password settings ............................ 353
Password Sync Groups .......................................................... 354
Adding a password sync group ............................................. 355
Modifying a password sync group ......................................... 356
Safeguard Access settings ...................................................... 357
Login Control ........................................................................ 357
Password Rules ...................................................................... 360
Modifying user password requirements .................................. 360
Sessions settings ..................................................................... 362
Session Recordings Storage Management ............................... 363
Assigning an archive server to an appliance ............................ 364
Sessions Module .................................................................... 364
SSH Banner .......................................................................... 365
SSH Host Key .............................................................................................................. 366

Users .......................................................................................................................... 367
General tab .................................................................................................................. 369
User Groups tab .......................................................................................................... 370
Partitions tab .............................................................................................................. 371
Entitlements tab .......................................................................................................... 371
Linked Accounts tab ................................................................................................. 372
History tab .................................................................................................................. 373
Managing users .......................................................................................................... 374
Adding a user ............................................................................................................. 375
  Authentication tab ................................................................................................... 376
  Contact Information tab ........................................................................................... 378
  Location tab ............................................................................................................. 379
  Permissions tab ........................................................................................................ 379
Requiring user to log in using secondary authentication .............................................. 380
  Configuring user to use Starling Two-Factor Authentication when logging into Safeguard ................................................................. 381
Adding a directory user account .................................................................................. 382
  Authentication tab ................................................................................................... 382
Adding a user to user groups ...................................................................................... 383
Assigning a user to partitions ..................................................................................... 384
Adding a user to entitlements ...................................................................................... 385
Linking a directory account to a user .......................................................................... 385
Modifying a user ......................................................................................................... 386
Deleting a user ........................................................................................................... 387
Importing objects ........................................................................................................ 388
Setting a local user’s password .................................................................................. 389
Unlocking a user’s account ......................................................................................... 389
Enabling or disabling a user ....................................................................................... 390

User Groups .................................................................................................................. 391
General tab .................................................................................................................. 392
Users tab ..................................................................................................................... 392
Entitlements tab .......................................................................................................... 393
History tab .................................................................................................................. 394
Managing user groups ............................................................................................... 396
Adding a user group .................................................................396
Adding a directory user group ..................................................396
Adding users to a user group .....................................................397
Adding a user group to an entitlement ......................................398
Modifying a user group ............................................................399
Deleting a user group ..............................................................399

**Disaster recovery** ...................................................................401
Enrolling and unjoining cluster members ....................................401
  Enrolling replicas into a cluster ................................................403
  Unjoining replicas from a cluster .............................................404
Maintaining and diagnosing cluster members ..............................405
  Failing over to a replica by promoting it to be the new primary ....406
  Activating a read-only appliance ..........................................407
  Diagnosing a cluster member ................................................408
  Patching cluster members .....................................................409
    About cluster patching .......................................................410
Using a backup to restore a clustered appliance ........................411
Resetting a cluster that has lost consensus ..............................412
Performing a factory reset .......................................................413
Unlocking a locked cluster ......................................................415
Troubleshooting tips ..............................................................415
Appliance states .......................................................................416

**Administrator permissions** ..................................................421
Appliance administrator permissions .........................................421
Asset administrator permissions ..............................................423
Auditor permissions ...............................................................425
Authorizer administrator permissions .......................................426
Directory administrator permissions .......................................427
Help Desk administrator permissions ......................................429
Operations administrator permissions ....................................429
Security Policy administrator permissions ...............................430
User administrator permissions ..............................................432

**Preparing systems for management** ....................................434
Prepare ACF - Mainframe systems ..........................................435
Prepare Amazon Web Services platforms .................................................. 436
Prepare Cisco devices ............................................................................. 436
Prepare Dell iDRAC devices ................................................................. 437
Prepare VMware ESXi hosts ................................................................. 437
Prepare Facebook hosts ......................................................................... 437
Prepare Fortinet FortiOS devices .......................................................... 438
Prepare F5 Big-IP devices ....................................................................... 438
Prepare HP iLO servers ........................................................................... 439
Prepare HP iLO MP (Management Processes) ......................................... 439
Prepare IBM i (AS/400) systems ............................................................. 439
Prepare JunOS Juniper Networks systems ............................................. 440
Prepare MongoDB ................................................................................ 440
Prepare MySQL servers .......................................................................... 441
Prepare Oracle databases ....................................................................... 441
Prepare PAN-OS (Palo Alto) networks ..................................................... 441
Prepare PostgreSQL ............................................................................... 442
Prepare RACF - Mainframe systems ....................................................... 442
Prepare SAP HANA ................................................................................ 443
Prepare SAP Netweaver Application Servers ........................................ 444
Prepare Sybase (Adaptive Server Enterprise) servers ............................. 445
Prepare SonicOS devices ....................................................................... 445
Prepare SonicWALL SMA or CMS appliances ........................................ 445
Prepare SQL Servers ............................................................................. 446
Prepare Top Secret - Mainframe systems .............................................. 447
Prepare Unix-based systems .................................................................. 448
Prepare Windows systems ..................................................................... 449
  Minimum required permissions for Windows assets .............................. 450

**Troubleshooting** .................................................................................. 453
Anti Cross-Site Request Forgery token error ........................................ 454
Cannot connect to remote machine through SSH or RDP ....................... 454
Cannot delete account .......................................................................... 454
Cannot play session message ................................................................ 455
Connectivity failures ............................................................................ 455
  Change password fails ...................................................................... 455
Incorrect authentication credentials ...................................................... 456
Missing or incorrect SSH host key ................................................................. 456
No cipher supported error ............................................................................ 457
Service account has insufficient privileges .................................................. 457
Domain user denied access to Safeguard ...................................................... 458
LCD status messages .................................................................................... 458
Appliance LCD and controls ......................................................................... 459
My Mac keychain password was lost ............................................................ 460
Password fails for Unix host ......................................................................... 461
Password is pending review .......................................................................... 461
  Password is pending a reset ......................................................................... 462
Profile did not run .......................................................................................... 462
Recovery kiosk ............................................................................................... 462
  Appliance information .................................................................................. 464
  Power options .............................................................................................. 465
    Rebooting the appliance ............................................................................ 465
    Shutting down the appliance ................................................................... 466
  Admin password reset .................................................................................. 466
  Factory reset .................................................................................................. 467
  Support bundle .............................................................................................. 468
Replica not adding ......................................................................................... 468
System services did not update or restart after password change ................. 468
Test Connection failures ............................................................................... 469
  Test Connection failures on archive server ................................................. 469
Certificate issue ............................................................................................. 470
Cipher support .................................................................................................. 470
Domain controller issue ................................................................................. 471
Networking issue ............................................................................................. 471
Windows WMI connection ............................................................................. 472
Timeout errors causing operations to fail ....................................................... 472
User locked out ............................................................................................... 472
User not notified ............................................................................................. 472

**Frequently asked questions** ...................................................................... 474
How do I access the API ................................................................................. 475
  How do I customize the response using API query parameters ................. 477
How do I audit transaction activity ............................................................... 478
How do I configure external federation authentication ................................. 479
    How do I add an external federation provider trust in Safeguard .................. 480
    How do I create a relying party trust for the IdP-STS ............................ 481
    How do I add an external federation user account ..................................... 482
    How do I manage accounts on unsupported platforms ............................... 483
    How do I modify the appliance configuration settings ............................. 484
    How do I prevent Safeguard messages when making RDP connections .......... 485
        Certificate chain of trust ................................................................... 487
    How do I see which assets and/or accounts are governed by a profile ......... 489
    How do I set the appliance system time .................................................... 489
    How do I setup discovery jobs .................................................................. 489
        Asset discovery job workflow ............................................................... 490
        Account discovery job workflow ......................................................... 491
        Directory account discovery job workflow ........................................ 492
    How do Safeguard database servers use SSL ............................................ 492
        ODBC Transport .................................................................................. 492
        Microsoft SQL Server ....................................................................... 493
        MySQL Server .................................................................................. 493
        Sybase ASE Server ........................................................................... 494
    What are the access request states ............................................................. 495
    What do I do when an appliance goes into quarantine .............................. 496
    What is required for One Identity Safeguard Privileged Sessions ............. 497
    What is required to integrate with Starling Identity Analytics & Risk Intelligence 498
    What needs to be set up to use Application to Application ....................... 499
        How do I make a request using the Application to Application service ...... 499
    What role-based email notifications are generated by default .................. 504
    When does the rules engine run for dynamic grouping and tagging .......... 505
    Why did the password change during an open request ........................... 505
    Why join Safeguard to One Identity Starling ........................................... 506
        How do I set up a Starling account ..................................................... 507

**Safeguard Desktop Player** ........................................................................ 509
    Recording navigation ................................................................................ 512
    Exporting video ....................................................................................... 514
    Key descriptions ...................................................................................... 515
Introduction

The One Identity Safeguard Administration Guide is intended for IT administrators, Unix administrators, security administrators, system auditors, and other IT professionals who are installing and configuring One Identity Safeguard for the first time.

NOTE: The term "Unix" is used informally in the Safeguard documentation to denote any operating system that closely resembles the trademarked system, Unix.

Introduction to One Identity Safeguard

The One Identity Safeguard Appliance is built specifically for use only with the Safeguard privileged management software, which is pre-installed and ready for immediate use. The appliance is hardened to ensure the system is secured at the hardware, operating system and software levels. The hardened appliance approach protects the privileged management software from attacks while simplifying deployment and ongoing management -- and shortening the timeframe to value.

The privileged management software provided with One Identity Safeguard consists of the following modules:

- **One Identity Safeguard for Privileged Passwords** automates, controls and secures the process of granting privileged credentials with role-based access management and automated workflows. Deployed on a hardened appliance, Safeguard for Privileged Passwords eliminates concerns about secured access to the solution itself, which helps to speed integration with your systems and IT strategies. Plus, its user-centered design means a small learning curve and the ability to manage passwords from anywhere and using nearly any device. The result is a solution that secures your enterprise and enables your privileged users with a new level of freedom and functionality.

- **One Identity Safeguard for Privileged Sessions** allows you to issue privileged access for a specific period or session to administrators, remote vendors and high-risk users with full recording and replay. With this ability, you can easily meet your auditing and compliance demands. In addition, Safeguard for Privileged Sessions serves as a proxy to ensure your critical assets are protected from any malicious software that might be lurking on an administrator’s machine. It provides a single
point of control from which you can authorize connections, limit access to specific resources, view active connections, record all activity, and terminate connections. Safeguard for Privileged Sessions is a critical component of the One Identity privileged access management products and is deployed on the same hardened secure appliance as Safeguard for Privileged Passwords.

Key features

The following key features are available when you have both Safeguard for Privileged Passwords and Safeguard for Privileged Sessions running on the same hardened secure appliance.

### Table 1: One Identity Safeguard key features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release control</td>
<td>Manages password requests from authorized users for the accounts they are entitled to access via a secure web browser connection with support for mobile devices.</td>
</tr>
<tr>
<td>Workflow engine</td>
<td>A workflow engine supports time restrictions, multiple approvers and reviewers, emergency access, and expiration of policy. It also includes the ability to input reason codes and/or integrate directly with ticketing systems. An access request can be automatically approved or require multiple sets of approvals.</td>
</tr>
<tr>
<td>Discovery</td>
<td>Quickly discover any privileged account or system on your network with host, directory and network-discovery options.</td>
</tr>
<tr>
<td>Approval Anywhere</td>
<td>Leveraging One Identity Starling, you can approve or deny any access request anywhere without being on the VPN.</td>
</tr>
<tr>
<td>Favorites</td>
<td>Quickly access the passwords that you use the most right from the Home screen.</td>
</tr>
<tr>
<td>Always online</td>
<td>Safeguard appliances can be clustered to ensure high availability. Passwords and sessions can be requested from any appliance in a Safeguard cluster. This distributed clustering design also enables the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.</td>
</tr>
<tr>
<td>RESTful API</td>
<td>Safeguard uses a modernized API based on a REST architecture which allows other applications and systems to connect and interact with it. The API enables quick and easy integration with diverse systems and applications spanning many programming languages.</td>
</tr>
<tr>
<td>Activity Center</td>
<td>Using the Activity Center, you can quickly and easily view all actions executed by Safeguard users and integrated processes. Activity Center reports can be searched, customized and filtered to</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>zero-in</strong></td>
<td>zero-in on the actions of a single user or to audit a variety of actions across a subset of departments. In addition, you can schedule queries, and save or export the data.</td>
</tr>
<tr>
<td>Two-factor authentication support</td>
<td>Protecting access to passwords with another password isn’t enough. Enhanced security by requiring two-factor authentication to Safeguard. Safeguard supports any Radius-based 2FA solution and One Identity's Starling Two-Factor Authentication service.</td>
</tr>
<tr>
<td>Smartcard support</td>
<td>Authentication of your privileged users can be integrated with Microsoft's Active Directory support for Smartcards or manually uploaded to the Safeguard appliance itself.</td>
</tr>
<tr>
<td>Full session audit, recording and replay</td>
<td>Every packet sent and action that takes place on the screen -- including mouse movements, clicks and keystrokes -- is recorded and available for review. The time and content of the session are cryptographically signed for forensics and compliance purposes. Only actual activity is recorded, and recordings are compressed to a fraction of the size required by other solutions to minimize offline storage requirements.</td>
</tr>
<tr>
<td>Proxy access</td>
<td>Safeguard for Privileged Sessions proxies all sessions to target resources. Since users have no direct access to resources, the enterprise is protected against viruses, malware and other dangerous items on the user's system. Safeguard for Privileged Sessions can proxy and record Unix/Linux, Windows, network devices, firewalls, routers and more.</td>
</tr>
<tr>
<td>Work the way you want</td>
<td>Safeguard for Privileged Sessions enables administrators to choose their access tools and tool preferences (for example, PuTTY) when gaining access to privileged sessions. This creates a frictionless solution that gives administrators the access they need while meeting compliance and security regulations.</td>
</tr>
<tr>
<td>Command detection</td>
<td>During a privileged session, Safeguard can detect commands that are being run on the target host. All actions are logged and can be sent out, if configured, to various logging mechanisms (syslog, email, SNMP).</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>For an RDP session, Safeguard can detect the title of any window that is opened on the desktop during a privileged session.</td>
</tr>
<tr>
<td>Indexing</td>
<td>Create a searchable list of commands and programs that were run during the recorded session. Auditors have a quick and easy view to session activities.</td>
</tr>
</tbody>
</table>
Auto-login

Sessions access request launch and auto-login enhances security and compliance by never exposing the account credentials to the user.

Protocol support

Safeguard for Privileged Sessions provides full support for the SSH and RDP protocols. In addition, administrators can decide what options within the protocols they want to enable/disable.

Secure access to legacy systems

Use smartcard, two-factor authentication or other strong authentication methods to gain access to systems. Because Safeguard acts as a gateway or proxy to the system, it enables strong authentication to targets that cannot or do not support those methods natively.

What's new in One Identity Safeguard 2.1

One Identity Safeguard 2.1 introduces the following new features and enhancements.

Table 2: Safeguard 2.1: Features and enhancements

<table>
<thead>
<tr>
<th>Feature/Enhancement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional platform support</td>
<td>Safeguard now supports the management of assets on the following additional platforms:</td>
</tr>
<tr>
<td></td>
<td>- ACF2 - Mainframe r14 and r15</td>
</tr>
<tr>
<td></td>
<td>- ACF2 - Mainframe LDAP r14 and r15</td>
</tr>
<tr>
<td></td>
<td>- Debian GNU/Linux 9</td>
</tr>
<tr>
<td></td>
<td>- ESXi 6.5</td>
</tr>
<tr>
<td></td>
<td>- Fedora 26</td>
</tr>
<tr>
<td></td>
<td>- Fortinet FortiOS 5.2 and 5.6</td>
</tr>
<tr>
<td></td>
<td>- F5 Big-IP 12.1.X and 13.0</td>
</tr>
<tr>
<td></td>
<td>- MAC OS X 10.13</td>
</tr>
<tr>
<td>Cluster patching</td>
<td>The cluster patching process now allows you to patch all cluster members without having to first unjoin a replica and re-enroll it after it has been updated. During the cluster patch operation, access request workflow is available so authorized users can request password releases and session access.</td>
</tr>
<tr>
<td>Federated login</td>
<td>One Identity Safeguard supports the SAML 2.0 Web Browser SSO Profile, allowing you to configure federated authentication with many different Identity Provider STS (IdP-STS) servers and services, such as Microsoft's AD FS and Azure AD.</td>
</tr>
<tr>
<td>Feature/Enhancement</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Immediate recording archival</td>
<td>One Identity Safeguard provides the ability to immediately archive session recordings from a specific Safeguard appliance to a specified archive target. When an archive server is configured, session recordings are removed from the Safeguard appliance and stored on the archive server.</td>
</tr>
<tr>
<td>Lights Out Management (BMC)</td>
<td>The Lights Out Management feature allows you to remotely manage the power state and serial console to Safeguard using the baseboard management controller (BMC). When a LAN interface is configured, this enables the Appliance Administrator to power on an appliance remotely or to interact with the recovery kiosk.</td>
</tr>
<tr>
<td>Multi-request</td>
<td>Authorized Safeguard users can now request multiple password releases or sessions in a single request. In addition, these requests can be saved as a &quot;favorite&quot; access request, providing quick access to the request from the user's Home page.</td>
</tr>
<tr>
<td>Safeguard Desktop Player enhancements</td>
<td>The new version of the Safeguard Desktop Player includes the following new features:</td>
</tr>
<tr>
<td></td>
<td>- Ability to display user activity as subtitles when playing back a recorded session. The user activity that can be displayed as subtitles includes windows titles, executed commands, mouse activity, and keystrokes, as they occurred during the recorded session.</td>
</tr>
<tr>
<td></td>
<td>- New timeline with user event indicators showing when user activities and screen changes occurred within the recorded session. Clicking an indicator on the timeline takes you to the relevant user event in the recording.</td>
</tr>
<tr>
<td></td>
<td>- Ability to export the sessions recording file, including the user event subtitles, as a video file.</td>
</tr>
<tr>
<td>Security Policy Administrator dashboard</td>
<td>The new Access Request dashboard allows Security Policy Administrators to review and manage access requests from a single location. From this view, the Security Policy Administrator can revoke a request, follow an active session, or terminate a session.</td>
</tr>
<tr>
<td>Restore/Suspend accounts</td>
<td>Safeguard allows you to suspend Safeguard managed accounts when they are not in use to reduce the vulnerability of password attacks on privileged accounts.</td>
</tr>
</tbody>
</table>
**Feature/Enhancement**  | **Description**
---|---
**NOTE:** This new feature applies to Windows platforms (Windows server and Active Directory accounts) and Unix platforms (AIX, HP-UX, Linux, Solaris, and Mac OS X accounts).

**TLS 1.2 Only**  | To remediate security vulnerabilities identified in early versions of the TLS encryption protocol, Appliance Administrators can configure Safeguard to respond only to TLS 1.2 requests. This allows organizations to comply with the security and strong cryptography requirements in PCI-DSS.

**X11 Forwarding**  | When configuring the settings for SSH session access requests, Security Policy Administrators can now enable **Allow X11 Forwarding**, which forwards a graphical X-server session from the server to the client.

---

**What's new in One Identity Safeguard 2.2**

One Identity Safeguard 2.2 introduces the following new features and enhancements.

**Table 3: Safeguard 2.2: Features and enhancements**

<table>
<thead>
<tr>
<th>Feature/Enhancement</th>
<th>Description</th>
</tr>
</thead>
</table>
| Additional platform support | Safeguard now supports the management of assets on the following additional platforms:  
  - FreeBSD  
  - MongoDB  
  - PostgreSQL  
  - RACF - Mainframe LDAP  
  - SAP HANA |
| Application to Application (A2A) integration | Using the Application to Application service, third-party applications can interact with Safeguard in the following ways:  
  - Credential retrieval: A third-party application can retrieve a credential from the Safeguard vault in order to perform automated functions on the target asset. In addition, you can replace hard coded passwords in procedures, scripts, and other programs with programmatic calls.  
  - Access request broker: A third-party application can initiate an access request on behalf of an authorized user. |
<table>
<thead>
<tr>
<th>Feature/Enhancement</th>
<th>Description</th>
</tr>
</thead>
</table>
| Asset administrator dashboard           | The **Account Automation** tab on the **Dashboard** allows Asset and Directory administrators to view information regarding accounts that are failing different types of tasks, including:  
  - Accounts where password check tasks failed.  
  - Accounts where password change tasks failed.  
  - Accounts where SSH key change tasks failed.  
  - Accounts where suspend tasks failed.  
  - Accounts where restore tasks failed.                                                                                                                                                                                                                     |
| Dynamic grouping and tagging            | Dynamic grouping and tagging helps classify assets allowing Safeguard to assign automatically provisioned systems and accounts to a policy.  
  Tags allow Asset administrators to add additional metadata to accounts and assets to enrich the data on the object as it is added to Safeguard. Tags can be dynamically added to assets and accounts based on tagging rules or they can be added manually.  
  Policy administrators can create rules based on tags or from attribute information that is on the account or asset (for example, name, platform, partition, network address, and so on) to define group membership. |
| Event subscription                      | As a Safeguard user, you can now control the email notifications you receive. Using the **Manage Email Notifications** control in your **My Account** pane, you can remove the events for which you do not want to receive email notifications.  
  As a Safeguard administrator, you can use the API to subscribe to the events for which you are interested in receiving notifications.                                                                                                                       |
| Audit log archive                       | Safeguard allows you to define and schedule an audit log management task to rotate audit logs from the Safeguard appliance and archive older audit logs to a designated archive server.                                                                                                                                                   |
| Site awareness and network segmentation | As an Appliance administrator, you can define managed networks (network segments) for your organization so Safeguard can more effectively manage assets and accounts,                                                                                                                                                  |
and service access requests. Managed network information is used for scheduling tasks, such as password change and account discovery, and for session management in a clustered environment to distribute the task load. That is, by using managed networks the load is distributed in such a way that there is minimal cluster traffic and appliances that are closest to the target asset are used to perform the task.

Attribute search
The attribute search functionality in the user interface allows you to limit an object list based on the object attributes. For example, in the Accounts view, you can now filter the accounts list based on whether the specified attribute contains the search string entered.

Starling Join
The newest versions of One Identity’s on-premises products offer a mandatory One Identity Hybrid Subscription, which helps you transition to a hybrid environment on your way to the cloud. The subscription enables you to join Safeguard with the One Identity Starling software-as-a-service platform. This gives your organization immediate access to a number of cloud-delivered features and services, which expand the capabilities of Safeguard. When new products and features become available to One Identity Starling, the One Identity Hybrid Subscription allows you to use these immediately for Safeguard to add value to your subscription.

Starling Identity Analytics & Risk Intelligence integration
The Starling Identity Analytics & Risk Intelligence service collects and evaluates information from data sources, such as Safeguard, to provide you with valuable insights into your users and entitlements. When integrated with Safeguard, Starling Identity Analytics & Risk Intelligence allows you to identify Safeguard users and entitlements that are classified as high risk and view the rules and details attributing to that classification.

What's new in One Identity Safeguard 2.3

One Identity Safeguard 2.3 introduces the following new features and enhancements.

Table 4: Safeguard 2.3: Features and enhancements

<table>
<thead>
<tr>
<th>Feature/Enhancement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronized passwords</td>
<td>As an Asset Administrator, you now have the ability to synchronize passwords so accounts can use the same password on the same or different assets.</td>
</tr>
</tbody>
</table>
One Identity Safeguard Appliance specifications

The Safeguard appliance is built specifically for use only with the Safeguard privileged management software that is already installed and ready for immediate use. It comes hardened to ensure the system is secure at the hardware, operating system, and software levels.

The One Identity Safeguard 2000 Appliance specifications and power requirements are as follows.

Table 5: Safeguard 2000 Appliance: Feature specifications

<table>
<thead>
<tr>
<th>Safeguard 2000</th>
<th>Feature / Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel Xeon E3-1275v5 3.60 GHz</td>
</tr>
<tr>
<td># of Processors</td>
<td>1</td>
</tr>
<tr>
<td># of Cores per Processor</td>
<td>4</td>
</tr>
<tr>
<td>L2/L3 Cache</td>
<td>4 x 256KB L2, 8MB L3 SmartCache</td>
</tr>
<tr>
<td>Chipset</td>
<td>Intel C236 Chipset</td>
</tr>
<tr>
<td>DIMMs</td>
<td>DDR4-2400 ECC Unbuffered DIMMs</td>
</tr>
<tr>
<td>RAM</td>
<td>32GB</td>
</tr>
<tr>
<td>Internal HD Controller</td>
<td>LSI MegaRAID SAS 9391-4i 12Gbps SAS3</td>
</tr>
<tr>
<td>Disk</td>
<td>4 x Seagate EC2.5 1TB SAS 512e</td>
</tr>
<tr>
<td>Availability</td>
<td>TPM 2.0, EEC Memory, Redundant PSU</td>
</tr>
<tr>
<td>I/O Slots</td>
<td>x16 PCIe 3.0, x8 PCIe 3.0</td>
</tr>
<tr>
<td>RAID</td>
<td>RAID10</td>
</tr>
<tr>
<td>NIC/LOM</td>
<td>3 x Intel i210-AT GbE</td>
</tr>
<tr>
<td>Power Supplies</td>
<td>Redundant, 700W, Auto Ranging (100v~240V), ACPI compatible</td>
</tr>
<tr>
<td>Fans</td>
<td>4 x 40mm Counter-rotating, Non-hot-swappable</td>
</tr>
<tr>
<td>Chassis</td>
<td>1U Rack</td>
</tr>
<tr>
<td>Dimensions</td>
<td>43 x 437.0 x 597.0 (mm)</td>
</tr>
<tr>
<td>(HxWxD)</td>
<td>1.7 x 17.2 x 23.5 (in)</td>
</tr>
<tr>
<td>Weight</td>
<td>Max: 46 lbs (20.9 Kg)</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>FIPS Compliant Chassis</td>
</tr>
</tbody>
</table>
### Table 6: Safeguard 2000 Appliance: Power requirements

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Voltage</td>
<td>100-240 Vac</td>
</tr>
<tr>
<td>Frequency</td>
<td>50-60Hz</td>
</tr>
<tr>
<td>Power Consumption (Watts)</td>
<td>170.9</td>
</tr>
<tr>
<td>BTU</td>
<td>583</td>
</tr>
</tbody>
</table>
System requirements

One Identity Safeguard has two graphical user interfaces that allow you to manage access requests, approvals and reviews for your managed accounts and systems:

- The Windows desktop client consists of an end-user view and administrator view.
- The web client is functionally similar to the desktop client end-user view.

Ensure that your system meets the minimum hardware and software requirements for these clients.

Desktop client system requirements

The desktop client is a native Windows application suitable for use on end-user machines. You install the desktop client by means of an MSI package which you can download from the appliance web client portal. You do not need administrator privileges to install One Identity Safeguard.

**NOTE:** When you install the Windows desktop client, these additional components are installed which are used by the One Identity Safeguard for Privileged Sessions module:

- Safeguard Desktop Player: Used to play back a recorded session.
- Safeguard PuTTY: Used to launch an SSH client if PuTTY is not available on the machine.

### Table 7: Desktop client requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology</td>
<td>Microsoft .NET Framework 4.6</td>
</tr>
<tr>
<td>Windows platforms</td>
<td>64-bit editions of:</td>
</tr>
<tr>
<td></td>
<td>- Windows 7</td>
</tr>
<tr>
<td></td>
<td>- Windows 8.1</td>
</tr>
</tbody>
</table>
### Component Requirements

- Windows 10
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

**NOTE:** Internet Explorer security must be set to use TLS 1.0 or higher. Ensure the proper "Use TLS" setting is enabled on the Advanced tab of the Internet Options dialog (In Internet Explorer, go to Tools | Internet Options | Advanced tab).

**NOTE:** If the appliance setting, **TLS 1.2 Only** is enabled, (Administration Tasks | Settings | Appliance | Appliance Information), ensure the desktop client also has TLS 1.2 enabled. If the client has an earlier version of TLS enabled, you will be locked out of the client and will not be able to connect to Safeguard.

| Safeguard Desktop Player | The sessions player is only supported on 64-bit operating systems. |

### Web client system requirements

**Table 8: Web client requirements**

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web browsers</td>
<td>Desktop browsers:</td>
</tr>
<tr>
<td></td>
<td>- Google Chrome 66 (or later)</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Internet Explorer 11 and Edge</td>
</tr>
<tr>
<td></td>
<td>- Mozilla Firefox 52 (or later)</td>
</tr>
<tr>
<td>Mobile device browsers:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Apple Safari iOS 10 (or later)</td>
</tr>
<tr>
<td></td>
<td>- Google Chrome on Android</td>
</tr>
</tbody>
</table>

The web client is implemented for modern web browser technology, using:

- HTML5
### Supported platforms

One Identity Safeguard supports a variety of platforms.

**NOTE:** The following table lists the platforms and versions that have been tested. Additional assets may be added to Safeguard. If you do not see a particular platform listed when adding an asset, use the "Other" or "Other Linux" option on the Management tab of the Asset dialog. For more information, see Management tab on page 138.

In addition, platforms that support RDP and SSH protocols are generally supported for Privileged Sessions management.

#### Table 9: Supported platforms: Assets that can be managed

<table>
<thead>
<tr>
<th>Platform</th>
<th>Version</th>
<th>Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACF2 - Mainframe</td>
<td>r14, r15</td>
<td>zSeries</td>
</tr>
<tr>
<td>ACF2 - Mainframe LDAP</td>
<td>r14, r15</td>
<td>zSeries</td>
</tr>
<tr>
<td>AIX</td>
<td>6.1, 7.1, 7.2</td>
<td>PPC</td>
</tr>
<tr>
<td>Amazon Web Services</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>CentOS Linux</td>
<td>6</td>
<td>x86, x86_64</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>x86_64</td>
</tr>
<tr>
<td>Cisco IOS</td>
<td>12.X, 15.X</td>
<td></td>
</tr>
<tr>
<td>Cisco PIX</td>
<td>7.X, 8.X</td>
<td></td>
</tr>
<tr>
<td>Debian GNU/Linux</td>
<td>6, 7, 8, 9</td>
<td>MIPS, PPC, x86, x86_64, zSeries</td>
</tr>
<tr>
<td>Dell iDRAC</td>
<td>7, 8</td>
<td></td>
</tr>
<tr>
<td>F5 Big-IP</td>
<td>12.1.X, 13.0</td>
<td></td>
</tr>
<tr>
<td>Fedora</td>
<td>21, 22, 23, 24, 25, 26</td>
<td>x86, x86_64</td>
</tr>
<tr>
<td>Platform</td>
<td>Version</td>
<td>Architecture</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Fortinet FortiOS</td>
<td>5.2, 5.6</td>
<td>x86, x86_64</td>
</tr>
<tr>
<td>FreeBSD</td>
<td>10.4, 11.1</td>
<td>x86, x86_64</td>
</tr>
<tr>
<td>HP iLO</td>
<td>iLO 2, 3, 4</td>
<td>x86</td>
</tr>
<tr>
<td>HP iLO MP</td>
<td>2, 3, 4</td>
<td>IA-64</td>
</tr>
<tr>
<td>HP-UX</td>
<td>11iv2 (B.11.23), 11iv3 (B.11.31)</td>
<td>IA-64, PA-RISC</td>
</tr>
<tr>
<td>IBM i</td>
<td>7.1, 7.2</td>
<td>PPC</td>
</tr>
<tr>
<td>Junos - Juniper Networks</td>
<td>12, 13, 14, 15</td>
<td></td>
</tr>
<tr>
<td>MAC OS X</td>
<td>10.9, 10.10, 10.11, 10.12, 10.13</td>
<td>x86_64</td>
</tr>
<tr>
<td>MongoDB</td>
<td>3.4, 3.6</td>
<td></td>
</tr>
<tr>
<td>MySQL</td>
<td>5.6, 5.7</td>
<td></td>
</tr>
<tr>
<td>Oracle Database</td>
<td>11g Release 2, 12c Release 1</td>
<td></td>
</tr>
<tr>
<td>Oracle Linux (OEL)</td>
<td>6</td>
<td>x86, x86_64</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>x86_64</td>
</tr>
<tr>
<td>PAN-OS</td>
<td>6.0, 7.0</td>
<td></td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>9.6.7, 10.2</td>
<td></td>
</tr>
<tr>
<td>RACF - Mainframe</td>
<td>z/OS V2.1 Security Server, z/OS V2.2 Security Server</td>
<td>zSeries</td>
</tr>
<tr>
<td>RACF - Mainframe LDAP</td>
<td>z/OS V2.1 Security Server, z/OS V2.2 Security Server</td>
<td>zSeries</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux (RHEL)</td>
<td>6</td>
<td>PPC, x86, x86_64, zSeries</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>PPC, x86_64, zSeries</td>
</tr>
<tr>
<td>SAP HANA</td>
<td>2.0</td>
<td>Other</td>
</tr>
<tr>
<td>SAP Netweaver Application Server</td>
<td>7.3, 7.4</td>
<td>SPARC, x86, x86_64</td>
</tr>
<tr>
<td>Solaris</td>
<td>10</td>
<td>SPARC, x86_64</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td></td>
</tr>
</tbody>
</table>
### Platform Version Architecture

<table>
<thead>
<tr>
<th>Platform</th>
<th>Version</th>
<th>Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>SonicOS</td>
<td>5.9, 6.2</td>
<td></td>
</tr>
<tr>
<td>SonicWALL SMA or CMS</td>
<td>11.3.0</td>
<td></td>
</tr>
<tr>
<td>SQL Server</td>
<td>2012, 2014, 2016</td>
<td>IA-64, PPC, x86, x86_64, zSeries</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>11, 12</td>
<td>PPC, x86_64, zSeries</td>
</tr>
<tr>
<td>Sybase (Adaptive Server Enterprise)</td>
<td>15.7, 16</td>
<td></td>
</tr>
<tr>
<td>Top Secret - Mainframe</td>
<td>r14, r15</td>
<td>zSeries</td>
</tr>
<tr>
<td>Top Secret - Mainframe LDAP</td>
<td>r14, r15</td>
<td>zSeries</td>
</tr>
<tr>
<td>Twitter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ubuntu</td>
<td>14.04 LTS, 15.04, 15.10, 16.04 LTS, 16.10, 17.04</td>
<td>x86, x86_64</td>
</tr>
<tr>
<td>VMware ESXi</td>
<td>5.5, 6.0, 6.5</td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td>Vista, 7, 8, 8.1, 10</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Platform</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Active Directory</td>
<td>Windows 2008+ DFL/FFL</td>
</tr>
<tr>
<td>OpenLDAP</td>
<td>2.4</td>
</tr>
</tbody>
</table>

**Table 10: Supported platforms: Directories that can be searched**

**Product licensing**

One Identity Safeguard is made up of a core set of features, such as the UI and Web Services layers, and a number of modules. The One Identity Safeguard 2000 Appliance ships with the following modules, each requiring a valid license to enable functionality:

- Privileged Passwords
- Privileged Sessions

You must install a valid license for each Safeguard module to operate. More specifically, if any module is installed, Safeguard will show a license state of **Licensed** and is
operational. However, depending on which models are licensed, you will see limited functionality. That is, even though you will be able to configure access requests:

- If a Privileged Passwords module license is not installed, you will not be able to request a password release.
- If a Privileged Sessions module license is not installed, you will not be able to initiate a session access request.

As an Appliance Administrator:

- If you are receiving a "license expiring" notification, apply a new license using that module's Update License link in Administrative Tools | Settings | Appliance | Licensing.
- If all licensed modules have expired, you will be prompted to add a new license when logging into the Safeguard desktop client.
- If only one of the licensed modules have expired, apply a new module license by clicking + in Administrative Tools | Settings | Appliance | Licensing.

As a Safeguard user, if you get an "appliance is unlicensed" notification, contact your Appliance Administrator.

For more information on adding or updating a Safeguard license, see Licensing.
Installing the One Identity Safeguard desktop client

To define and enforce security policy for your enterprise, you must first install the desktop client application which gives you access to the Administrative Tools.

These topics explain how to install, start and uninstall the Safeguard desktop client application:

- Installing the desktop client
- Starting the desktop client
- Uninstalling the desktop client

Installing the desktop client

**NOTE:** When you install the Windows desktop client, the following components are also installed:

- Safeguard Desktop Player which is used to replay recorded sessions.
- Safeguard PuTTY which is used to launch the SSH client for SSH session requests.

To install the Safeguard desktop client application

1. To download the Safeguard desktop client Windows installer .msi file, open a browser and navigate to:
   - https://<Appliance IP>/Safeguard.msi
   - Save the Safeguard.msi file in a location of your choice.
2. Run the MSI package.
3. Select Next in the Welcome dialog.
4. Accept the End-User License Agreement and select Next.
5. Select **Install** to begin the installation.
6. Select **Finish** to exit the desktop client setup wizard.

### Starting the desktop client

The following steps assume the Safeguard 2000 appliance has been configured and licensed. As a Safeguard user, if you get an "appliance is unlicensed" notification, contact your Appliance Administrator.

**To start the desktop client application**

1. From the Windows Start menu, choose **Safeguard**.
2. On the server selection screen, enter or select the server's network DNS name or IP address to connect to the appliance over the network and click (or tap) **Connect**.
   
   **NOTE:** When entering an IPv6 address, enclose the IPv6 address in square brackets.

3. On the user login screen, enter your credentials and click (or tap) **Log in**.
   - User Name: Enter your user or display name.
     
     **NOTE:** When using directory account credentials, enter your domain\name.
   
   - Password: Enter the password associated with the user entered above.
4. If your Safeguard user account requires you to log in with secondary authentication, enter the secure password (or token code) for your authentication service provider account and click (or tap) **Submit**.

   **NOTE:** The type and configuration of the secondary authentication provider (RSA SecureID, One Identity Starling Two-Factor Authentication, Microsoft Azure, etc.) determines what you must provide for secondary authentication. Check with your system administrator for more information about how to log into Safeguard with secondary authentication.

### Uninstalling the desktop client

**To uninstall the desktop client**

1. In the Windows Control Panel, open **Programs and Features**.
2. Right-click (or press and hold) the Safeguard application and choose **Uninstall**.
Setting up One Identity Safeguard for the first time

Before One Identity Safeguard can manage your privileged account passwords and privileged sessions, you must first add all the objects you need to write access request policies, such as users, accounts, and assets. By following these procedures you will set up a hierarchy of administrators that ensures your company follows role-based access control. For more information, see Administrator permissions on page 421.

NOTE: The setup steps in this section assume you have already performed the initial One Identity Safeguard 2000 Appliance installation and configuration steps in the One Identity Safeguard Appliance Setup Guide provided with your hardware equipment and have added a user with Authorizer Administrator permissions.

In addition:

- If you have not already done so, it is highly recommended that you change the default password for your bootstrap administrator account.
- Before Safeguard can reset local account passwords on Windows systems, you must change the local security policy to disable "User Account Control: Run all administrators in Admin Approval Mode".
- One Identity Safeguard for Privileged Sessions: For some systems (SUSE and some Debian systems) that use SSH, you must enable password authentication in the package generated configuration file (sshd_config). For example, in the debian sshd_config file, set the following parameter: PasswordAuthentication yes.

Step 1: Authorizer Administrator creates administrators
Step 2: Appliance Administrator configures the appliance
Step 3: User Administrator adds users
Step 4: Asset Administrator adds managed systems
Step 5: Directory Administrator adds external identity stores
Step 6: User Administrator (or Authorizer Administrator) adds directory groups
Step 7: Security Policy Administrator adds access request policies
Step 1: Authorizer Administrator creates administrators

1. Log into the desktop client using the Authorizer Administrator account.
2. Customize the Password Rules. (Settings | Safeguard Access | Password Rules)
3. Add users for the following administrator permissions (Adding a user):
   a. User Administrator
   b. Help Desk Administrator
   c. Appliance Administrator
   d. Operations Administrator
   e. Auditor
   f. Asset Administrator
   g. Directory Administrator
   h. Security Policy Administrator

   !NOTE: A user can have more than one set of permissions. For a list of permissions granted to the different Safeguard administrators, see Administrator permissions.

Step 2: Appliance Administrator configures the appliance

1. Log into the desktop client using the Appliance Administrator account.
2. If you are using both the Privileged Passwords and Privileged Sessions modules, ensure the Network Interface X0 (primary interface) and Network Interface X1 (sessions interface) information is configured (Settings | Appliance | Networking). This includes the following for each:
   a. IP address
   b. Netmask
   c. Default gateway
   d. DNS servers
   e. DNS suffixes

   For more information, see Networking on page 261.
3. Ensure the access request and password management features are enabled. (Settings | Access Request | Enable or Disable Services).
4. Configure the External Integration settings that apply (Settings | External Integration):
   a. Email: Configure the SMTP server to be used for email notifications. Safeguard provides default email templates for most events, which can also be customized.
   b. External Federation: Configure a relying party trust relationship with one or more federated authentication servers or services.
   c. Secondary authentication: Configure the secondary authentication service providers to be used for two-factor authentication.
   d. SNMP: Configure SNMP subscriptions for sending SNMP traps to your SNMP console when certain events occur.
   e. Starling: Join Safeguard to Starling to take advantage of other Starling services, such as Starling Two-Factor Authentication and Starling Identity Analytics & Risk Intelligence.
   f. Syslog: Configure the syslog servers where event notifications are to be sent.
   g. Ticketing: Add external ticketing servers tracking system.

5. Safeguard ships with default certificates and default SSH algorithms for the Unix and Linux platforms. However, you can replace the certificates to be used or add new algorithms.
   a. To specify different certificates to be used, see Certificates settings.
   b. To add new SSH algorithms, use the API endpoint:
      https://<Appliance IP>/service/core/swagger/SessionSshAlgorithms

Step 3: User Administrator adds users

1. Log into the desktop client using the User Administrator account.
2. Add users who can log into Safeguard (Adding a user).
3. Grant Help Desk Administrator permissions to one or more users.

Step 4: Asset Administrator adds managed systems

1. Log into the desktop client using the Asset Administrator account.
2. Add partitions and, optionally, delegate partition ownership to other users (Adding a partition).
3. (Optional) Set the following Profile settings (or edit the default rules and settings defined when the partition was added):
   a. Account Password Rules
   b. Change Password
   c. Check Password
   d. Password Sync Groups
4. (Optional) create partition profiles or edit the default profiles created (Creating a partition profile).
5. Add assets to the appropriate partitions and profiles (Adding an asset).
6. Add accounts to control access to the assets (Adding an account).

**Step 5: Directory Administrator adds external identity stores**

1. Log into the desktop client using the Directory Administrator account.
2. Add directories (Adding a directory).
3. Add directory accounts to directories (Adding directory accounts to a directory).
4. Create directory profiles (Creating a directory profile).

**Step 6: User Administrator (or Authorizer Administrator) adds directory groups**

1. Log into the desktop client using the User Administrator account.
2. Add directory groups (Adding a directory user group).
3. Reset the time zone on each imported directory account.

**Step 7: Security Policy Administrator adds access request policies**

1. Log into the desktop client using the Security Policy Administrator account.
2. Set Reasons. (Settings | Access Request | Reasons)
3. Configure Approval Anywhere. (Settings | External Integration | Approval Anywhere).
4. Add user groups (Adding a user group).
5. Add local or directory users to local user groups (Adding users to a user group).
6. Add account groups (Adding an account group).
7. Add accounts to account groups (Adding accounts to an account group).
8. Add entitlements (Adding an entitlement).
9. Add users or user groups to entitlements (Adding users or user groups to an entitlement).
10. Create access request policies (Creating an access request policy).
Getting acquainted with the console

One Identity Safeguard has two graphical user interfaces that allow you to manage password and session requests, approvals and reviews for your managed accounts and systems:

- Windows desktop client
  The desktop client consists of an end-user view and an administrator view. The administrative functionality is dynamically enabled based on the user’s permissions.

- Web client
  The web client is functionally similar to the desktop client end-user view. It exposes the access request workflow functionality and is meant primarily for the non-administrative user. The web client uses a responsive UI design to adapt to the user’s device -- from desktops to tablets or mobile phones.

**NOTE:** Since the functionality of these two user interfaces are similar, this guide only describes the Windows desktop client.

The Safeguard desktop client console consists of these main components:

- Toolbar
- Navigation pane

**Toolbar**

The toolbar along the top-right corner of the Safeguard console, has these controls:

**Table 11: Toolbar controls**

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>Configure the desktop client application, including notifications and Home page widgets, or view product information, including contact information.</td>
</tr>
<tr>
<td>User avatar</td>
<td>Modify personal information, view notifications, or log out of the Safeguard client.</td>
</tr>
</tbody>
</table>
Settings

The Safeguard console Settings (_allocation) allows you to configure the desktop client application.

Notifications

Use the following options to control notifications within Safeguard:

- **Run in the System Tray** when you close the application.
  When you enable the Run in the System Tray option, you cannot modify the toast notifications option. However, when you disable the Run in the System Tray option, you can enable or disable toast notifications.

  _NOTE:_ When you enable the Run in the System Tray option, you cannot modify the toast notifications option because in that mode, you always get notifications.

- **Enable Toast Notifications** to display event alerts on your console.
  Toast notifications are alerts that appear when the desktop client application is not the active foreground application; for example, when you are in another application or when you have minimized the desktop client.

**Reset Notifications:** Click (or tap) Reset Notifications to re-enable any notifications pop ups that have been previously suppressed.

Widgets

Click (or tap) the toggles to enable or disable the Home page widgets:

- Requests
- Approvals
- Reviews

All widgets are enabled by default, indicating that the corresponding controls display on your Home page. The toggles appear blue with the switch to the right when a widget is enabled and gray with the switch to the left when a widget is disabled.

About

Click (or tap) About Safeguard to display the following information.
Table 12: About dialog tabs

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>About</td>
<td>The trademark and copyright information.</td>
</tr>
<tr>
<td>Contact</td>
<td>Information about how to get in touch with One Identity.</td>
</tr>
<tr>
<td>Components</td>
<td>A list of third-party components used in Safeguard.</td>
</tr>
<tr>
<td>Third Party License Text</td>
<td>The license text for third-party components that require this text to be included in the product documentation.</td>
</tr>
</tbody>
</table>

**User avatar**

Click (or tap) the user avatar (or the Welcome link with your user name) to modify your personal information, manage email notifications, view current notifications, or log out of Safeguard.

**My Account**

Click (or tap) **My Account** to modify your personal information and manage your email notifications.

**NOTE:** Safeguard Active Directory users cannot use **My Account** to modify their email address, phone number, or change their password. They must do these actions in Active Directory.

**To update your personal information**

1. From the toolbar, select your user avatar and choose **My Account**.
2. To change your image, select ☑ **Change Photo**.
3. To change your email address or **Contact Information**, type into the appropriate box.
4. To change your user password, click (or tap) **Change Password**.
5. Click (or tap) **Done** to close the My Accounts pane.

**To manage the notifications you receive**

1. From the toolbar, select your user avatar and choose **My Account**.
2. Click (or tap) **Manage Email Notifications**.
   - The **Manage Email Notifications** dialog displays the type of events for which you are receiving email notifications.
NOTE: When there are no delegated owners assigned to a partition, email notifications related to partitions are sent to the Asset administrator. However, when a delegated owner is specified to manage the assets and accounts in a partition, email notifications related to partitions are sent to the delegated owner, not to the Asset administrator.

3. From this dialog, you can define the types of events for which you want to receive notifications.

   By default, all events are selected. Clear the check box for any events for which you do not want to receive an email notification.

   TIP: Select the check box next to the Events heading to select all of the events in the list. Similarly, clear the check box next to the Events heading to clear all of the event check boxes.

4. Click (or tap) OK to save your selections and close the dialog.
5. Click (or tap) Done to close the My Accounts pane.

Log Out

Click (or tap) Log Out to log out of the Safeguard desktop client.

Navigation pane

The Home page left navigation pane has these links:

<table>
<thead>
<tr>
<th>Table 13: Navigation pane options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Page</strong></td>
</tr>
<tr>
<td>Home</td>
</tr>
<tr>
<td>Dashboard</td>
</tr>
<tr>
<td>Activity Center</td>
</tr>
<tr>
<td>Reports</td>
</tr>
<tr>
<td>Administrative Tools</td>
</tr>
</tbody>
</table>
Where you define and management all of the administrative Safeguard settings.

Home

When you log into Safeguard, you begin your session on the Home page. The Message of the Day displays on the right side. The rest of the Home page is tailored to your user rights and permissions. If you are authorized by an entitlement to request, approve, or review access requests, then your Home page gives you a quick view to the access request tasks that need your immediate attention.

NOTE: You can turn Requests, Approvals, and Reviews widgets on or off in Settings.

NOTE: The Appliance Administrator sets the Message of the Day. For more information, see Message of the Day on page 340.

Requester's Home page view

Click (or tap) the New Request tile to open the New Access Request dialog which lists the assets and accounts you are authorized to access. From this dialog you specify the assets, accounts and the type of access you are requesting, and additional details about the request.

For more information, see:

- Requesting a password release
- Requesting session access

Expand Requests to view the requests awaiting action.

For more information, see:

- Taking action on a password release request
- Taking action on a session request

The Favorites pane (right pane) displays a list of requests you have marked as a "favorite", providing a quick way to request access.

Use the toolbar buttons at the top of the Favorites pane to manage your favorite requests.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ New</td>
<td>Select this button to create a new favorite request. Clicking this button</td>
</tr>
<tr>
<td>Button</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Favorite</td>
<td>displays the <strong>New Access Request</strong> dialog allowing you to select the assets, accounts, type of access, and additional details about the request.</td>
</tr>
<tr>
<td>✓</td>
<td>Select this button to display additional options for managing your favorite requests:</td>
</tr>
<tr>
<td></td>
<td>• Request Selected</td>
</tr>
<tr>
<td></td>
<td>• Color Selected</td>
</tr>
<tr>
<td></td>
<td>• Remove Selected</td>
</tr>
<tr>
<td></td>
<td><strong>TIP:</strong> Select the check box to the left of a favorite request to use these additional buttons. Selecting the request itself will launch the <strong>New Access Request</strong> dialog allowing you to edit and submit the request.</td>
</tr>
</tbody>
</table>

To submit a favorite request, click the request or select the check box to the left of a request and select **Request Selected**. The **New Access Request** dialog displays allowing you to edit your selections or enter a required reason or comment before submitting it.

For more information, see:

- Creating, editing, or removing a favorite request

**Approver's Home page view**

Your job is to approve or deny the access requests listed on your Home page. Expand **Approvals** to view the requests awaiting your approval.

For more information, refer to these topics:

- Approving a password release request
- Approving a session request

**NOTE:** As an "approver" user, unless you are also designated as a requester, you will see no favorites listed.

**Reviewer's Home page view**

Your job is to review completed access requests listed on your Home page. Expand **Reviews** to view the completed requests requiring your review.

For more information, refer to these topics:

- Reviewing a completed password release request
- Reviewing a session request

**NOTE:** As a "reviewer" user, unless you are also designated as a requester, you will see no favorites listed.
Dashboard

The Dashboard contains operational information that allows administrators with the proper permissions to view and manage access requests and accounts failing tasks from a single location.

Table 15: Dashboard tabs

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Requests</td>
<td>Displays information about access requests in different stages of the workflow.</td>
</tr>
<tr>
<td>Account Automation</td>
<td>Displays information about accounts that are failing different types of tasks.</td>
</tr>
</tbody>
</table>

Access Requests

The Access Requests tab on the Dashboard allows Security Policy Administrators to review and manage access requests from a single location. Clicking one of the access request tiles across the top of the view displays additional information about the access requests belonging to that category. In addition, you can review the request workflow, launch a live session, terminate a session, or revoke a specific request.

This dashboard is available to Safeguard users assigned the following administrative permissions:

- Auditor: Read-only view.
- Security Policy: Full control.

Table 16: Access Requests: Tiles

<table>
<thead>
<tr>
<th>Tile</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Sessions</td>
<td>Displays a list of all currently opened sessions.</td>
</tr>
<tr>
<td>Passwords Out</td>
<td>Displays a list of all password release requests that are currently checked out.</td>
</tr>
<tr>
<td>Pending Approval</td>
<td>Displays a list of access requests waiting for approval.</td>
</tr>
<tr>
<td>Pending Review</td>
<td>Displays a list of access requests waiting review.</td>
</tr>
<tr>
<td>Open Requests</td>
<td>Displays a list of all currently opened access requests, including session requests and password release requests.</td>
</tr>
</tbody>
</table>

Use the toolbar at the top of the details grid to perform the following tasks.
### Table 17: Access Requests: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>⌚ Workflow</td>
<td>Select to review the transactions that took place in the selected request. Clicking this button displays the Request Workflow dialog allowing you to audit the transactions that occurred during the request's workflow from request to approval to review.</td>
</tr>
<tr>
<td>⌚ View Live Session</td>
<td>Select to view a live session for the selected session request. Clicking this button launches the Safeguard Desktop Player allowing you to follow an active session. For more information, see Safeguard Desktop Player on page 509.</td>
</tr>
<tr>
<td>✗ Terminate Session</td>
<td>Select to terminate the live session for the selected session request.</td>
</tr>
<tr>
<td>☑ Revoke Request</td>
<td>Select to retract the selected access request.</td>
</tr>
<tr>
<td>☐ Export</td>
<td>Select to create a .csv file of the currently displayed access request grid and save it to a location of your choice.</td>
</tr>
<tr>
<td>☐ Columns</td>
<td>Select to display a list of columns that can be displayed in the grid. Select the check box for data to be included in the grid. Clear the check box for data to be excluded from the grid.</td>
</tr>
</tbody>
</table>

### Viewing details

Additional detailed information is available for access requests listed in the request grids on the Access Requests view.

**To see the details of an access request**

1. Double-click (or double-tap) a request to view additional details.
2. Double-click (or double-tap) to close the request details.

   **NOTE:** Clicking ☑ Refresh at the top of the view also closes the details in addition to retrieving the latest access requests.

### Account Automation

The Account Automation tab on the Dashboard allows Asset and Directory administrators to view information regarding accounts that are failing different types of tasks. This dashboard includes both automated and manual tasks in the failure results. Clicking one of the failure task tiles across the top of the view displays additional information about the accounts belonging to that category.
This dashboard is available to Safeguard users assigned the following administrative permissions:

- Asset Administrator: Full control for accounts related to all Safeguard assets.
- Auditor: Read-only view.
- Delegated Partition Owner: Control for accounts related to the accounts and assets managed through delegation.
- Directory Administrator: Full control for accounts related to the directories managed by Safeguard.

### Table 18: Account Automation: Tiles

<table>
<thead>
<tr>
<th>Tile</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Check Failures</td>
<td>Displays a list of accounts where password check tasks failed.</td>
</tr>
<tr>
<td>Password Change Failures</td>
<td>Displays a list of accounts where password change tasks failed.</td>
</tr>
<tr>
<td>SSH Key Change Failures</td>
<td>Displays a list of accounts where SSH key change tasks failed.</td>
</tr>
<tr>
<td>Suspend Account Failures</td>
<td>Displays a list of accounts where suspend tasks failed.</td>
</tr>
<tr>
<td>Restore Account Failures</td>
<td>Displays a list of accounts where restore tasks failed.</td>
</tr>
</tbody>
</table>

Use the toolbar at the top of the details grid to perform the following tasks.

### Table 19: Account Automation: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔷️ Rerun task</td>
<td>Select to rerun the selected task.</td>
</tr>
<tr>
<td>🕒 Export</td>
<td>Select to create a .csv file of the currently displayed account automation grid and save it to a location of your choice.</td>
</tr>
<tr>
<td>📊 Columns</td>
<td>Select to display a list of columns that can be displayed in the grid. Select the check box for data to be included in the grid. Clear the check box for data to be excluded from the grid.</td>
</tr>
</tbody>
</table>

### Activity Center

The Activity Center is the place to go to view the details of specific events or user activity. The appliance records all activities performed within One Identity Safeguard. Any administrator has access to the audit log information; however, your administrator permission set determines what audit data you can access. For more information, see Administrator permissions on page 421.
The toolbar at the top of the main Activity Center page contains these options.

### Table 20: Activity Center: Main page toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✗ Clear</td>
<td>Resets the current search criteria back to the default settings (all activity occurring within the last 24 hours.)</td>
</tr>
<tr>
<td>⌚ Schedule</td>
<td>Allows you to define when the activity audit log report is to be generated and sent via email. For more information, see Scheduling an activity audit log report on page 55.</td>
</tr>
<tr>
<td>📚 Open</td>
<td>Allows you to access previously saved search and scheduled reports.</td>
</tr>
<tr>
<td>☑️ Save</td>
<td>Saves the current search criteria which can be used later to generate the report. For more information, see Saving search criteria on page 53.</td>
</tr>
<tr>
<td>Run</td>
<td>Generates an activity audit log report based on the search criteria specified.</td>
</tr>
</tbody>
</table>

In addition, query tiles display the criteria you have applied to search the activity data. By default, only the Activity category and Time frame tiles display. Use the + Add button to specify additional query criteria to retrieve the information you are looking for. For more information, see Applying search criteria on page 51.

Once an activity audit log report is generated, the results page contains the search results grid and these toolbar options.

### Table 21: Activity Center: Results page toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>← Back</td>
<td>takes you back to the query page where you can modify the search criteria.</td>
</tr>
<tr>
<td>⏺ Refresh</td>
<td>closes the details and updates the search results page.</td>
</tr>
</tbody>
</table>

## Applying search criteria

Use the Activity Center’s query builder to add and remove data from your activity audit log report to get the information you need.

By default, an activity audit log report includes all activity occurring within the last 24 hours. However, using the query tiles provided you can specify search criteria to retrieve specific information from the activity audit log. The search criteria available includes:

- Activity category
- Time frame
- User
- Asset
- Account
- Search keyword or value

To apply search criteria to the audit log

1. From the Safeguard desktop Home page, select \( \text{Activity Center} \).
2. To limit the report to a particular type of activity, click the Activity category tile (I would like to see) and select the activity category to be included in the report.
3. To specify a different time frame, click the Time frame tile (occurring within the) and select the time frame to be included in the report.

   \( \text{NOTE:} \) If using the Custom option, specify the custom time range.

4. To see activity attributed to a specific user, click (or tap) the \( \text{Add} \) button and select Add User.
   - In the Users selection dialog, select the user to be included in the report.

   \( \text{NOTE:} \) You can specify only one user.

5. To see activity involving a specific asset, click (or tap) the \( \text{Add} \) button and select Add Asset.
   - In the Assets selection dialog, select the asset to be included in the report.

   \( \text{NOTE:} \) You can specify only one asset.

6. To see activity involving a specific account, click (or tap) the \( \text{Add} \) button and select Add Account.
   - In the Accounts selection dialog, select the account to be included in the report.

   \( \text{NOTE:} \) You can specify only one account.

7. You can also search session activity for a specific keyword or value.
a. Change the activity category to **Session Specific Activity (or In-Session Activity)**.
b. Click (or tap) the **Add** button and select **Add Search value**.
c. In the **Enter a Search Value** dialog, enter the keyword or value (e.g., regedit) and click (or tap) **OK**.

An additional tile (that includes) appears listing the keyword or value specified.

NOTE: If you change the activity category, the keyword tile will be dimmed indicating it will not be included in the query.

8. To remove or edit your selections, use the icons in the upper right corner of a query tile:

   - **Clear**: Resets the value back to the default.
     
     NOTE: **Clear** is only available for Activity category and Time frame.

   - **Delete**: Removes the query tile from the search criteria.

   - **Edit**: Displays the corresponding dialog allowing you to modify your selection.

     TIP: You can also click (or tap) a query tile to edit your selection.

### Saving search criteria

You can save the current search criteria defined to be used at a later time to generate an activity audit log report. You can save the current search criteria from the main Activity Center view (query builder page) or from the results view.

**To save the current search criteria**

1. From the Safeguard desktop Home page, select **Activity Center**.
2. Specify the search criteria to be used to generate the desired report. For more information, see Applying search criteria on page 51.
3. Click (or tap) **Save**.
4. In the **Save Search** dialog, enter the following information:
   
a. **Name**: Enter a name for the search.

   b. **Description**: Optionally, enter descriptive text to describe the search.
5. Click (or tap) **OK**.
6. To run a previously saved search, click (or tap) **Open**.
   
a. Select a search from the list.
   
   The criteria for the selected search is displayed in the right pane.

   b. Click **Open**.
The query tiles for the selected search appear in the Activity Center page, where you can then select Run to generate the report.

**Generating an activity audit log report**

*To generate an activity audit log report*

1. From the Safeguard desktop Home page, select Activity Center.
2. Use the query tiles to specify the content of the report.
   
   **NOTE:** By default the audit log returns all activity occurring within the last 24 hours. Use the query tiles on the Activity Center page to include specific information from the activity audit log in your results. For more information, see Applying search criteria on page 51.

3. Click (or tap) Run.
   
   **NOTE:** You can also save search criteria for use at a later time. For more information, see Saving search criteria on page 53.

The information displayed by default depends on the type of activity report generated. For example, the "All Activity" report displays the following information for each event:

- **State:** The left-most column displays one of the following regarding the availability of a recorded session:
  - Blank: Indicates that there is no recorded session available.
  - (green dot): Indicates that a live session is taking place. A Security Policy Administrator can click this button to launch the desktop player to follow what is happening in the current session.
  - Play: Indicates that there is a recorded session available locally on the appliance. Clicking this button launches the desktop player to play back the selected recording.
  - Download: Indicates that there is a recorded session available on the archive server. Clicking this button downloads the recording for playback.

   **NOTE:** These icons only appear on an "All Activity" or "Session Specific Activity" report.

- **User:** The name of the user who triggered the event.
- **Date:** The date and time the event occurred.
- **Activity Category:** The category that defines the type of activity that occurred.
- **Event:** The event that occurred.

4. Double-click (or double-tap) an event to view additional details. Double-click to close the details.

Once a report is generated, you can use the buttons above the grid as described below.
### Table 22: Activity Center: Results grid toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time frames</td>
<td>To rerun the report using a different time frame, select one of the following links:</td>
</tr>
<tr>
<td></td>
<td>- Last 24 Hours (default)</td>
</tr>
<tr>
<td></td>
<td>- Last 7 Days</td>
</tr>
<tr>
<td></td>
<td>- Last 30 Days</td>
</tr>
<tr>
<td></td>
<td>- Last 60 Days</td>
</tr>
<tr>
<td></td>
<td>- Last 90 Days</td>
</tr>
<tr>
<td></td>
<td>- Custom</td>
</tr>
<tr>
<td></td>
<td>Specify the time range for the Custom time frame.</td>
</tr>
<tr>
<td></td>
<td>After selecting a different time frame, click (or tap) Run.</td>
</tr>
<tr>
<td><img src="image" alt="Workflow" /> Workflow</td>
<td>Select an access request event and click (or tap) Workflow to audit the transactions that occurred during the request's workflow from request to approval to review.</td>
</tr>
<tr>
<td><img src="image" alt="TIP" /></td>
<td><strong>TIP:</strong> For session requests, you can also replay a recorded session or live session from the Request Workflow dialog. For more information, see Replaying a session on page 91.</td>
</tr>
<tr>
<td><img src="image" alt="Run" /> Run</td>
<td>Select to regenerate the report using the specified time frame.</td>
</tr>
<tr>
<td><img src="image" alt="Export" /> Export</td>
<td>Select to create a .json file of the search results and save it in a location of your choice.</td>
</tr>
<tr>
<td><img src="image" alt="Schedule" /> Schedule</td>
<td>Select to schedule the generation of the activity audit log report.</td>
</tr>
<tr>
<td><img src="image" alt="Save" /> Save</td>
<td>Select to save the current search criteria.</td>
</tr>
<tr>
<td><img src="image" alt="Column" /> Column</td>
<td>Select to display a list of columns that can be displayed in the grid. Select the check box for data to be included in the report. Clear the check box for data to be excluded from the report.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The additional columns available depend on the type of activity included in the report.</td>
</tr>
</tbody>
</table>

### Scheduling an activity audit log report

Safeguard allows you to schedule the generation of an activity audit log report, which will then be sent via email. The emailed report will be an attachment in .json format.
To schedule an activity audit log report

1. From the Safeguard desktop Home page, select Activity Center.
2. Specify the search criteria to be used to generate the desired report. For more information, see Applying search criteria on page 51.
3. Click (or tap) Schedule.
4. In the Schedule Report dialog, enter the following information:
   a. Name: Enter a name for the report.
   b. Description: Optionally, enter descriptive text for the report.
   c. Send To: Read-only field displaying the email address of the user currently logged into the Safeguard client.
      
      NOTE: This field is required. If this field is blank, you must set your email address in My Accounts. For more information, see User avatar on page 44.
   d. Interval: Select the interval, start time, and frequency at which the report is to be generated:
      • Never: Select this option to save the report to run at a later time.
      • Minute: Select the time of day and frequency (minute repeat interval).
      • Hour: Select the time of day and frequency (hourly repeat interval).
      • Day: Select the time of day and frequency (daily repeat interval).
      • Week: Select the time of day, frequency (weekly repeat interval), and the days of the week when the report is to be generated.
      • Month: Select the time of day, day of the month or week of the month and day of the week, and frequency (monthly repeat interval).
      
      NOTE: Best Practice: Do not use the Minute interval.
   e. Time Zone: Select the time zone to be used.
5. Click (or tap) Schedule Report.

Editing or deleting a saved search or scheduled report

Click the Open toolbar button to display a list of saved searches and scheduled reports. From this dialog, you can delete or edit a saved search or scheduled report.

1. From the Safeguard desktop Home page, select Activity Center.
2. Click (or tap) Open.
   
The Select a Saved Search dialog displays, which contains a list of all saved searches and scheduled reports.
3. Select a saved search or scheduled report from the list.
   The search criteria defined for the search or report appear in the right pane.
4. Click (or tap) one of the toolbar buttons or right-click commands:
   - [Delete]
   - [Edit]
   - [Edit Schedule]
5. If you selected [Delete], click (or tap) Yes in the confirmation dialog.
   The selected search or schedule will be removed from the list.
6. Depending on the type of search selected (saved search or scheduled report), the following editing capabilities are available:
   - [Edit] displays the Save Search dialog, allowing you to modify the name and description for a saved search or schedule.
     
     **NOTE:** The Edit button is available for a saved search or a scheduled report with an interval of Never.
   - [Edit Schedule] displays the Schedule Report dialog, allowing you to modify the schedule settings for a scheduled report.
     
     **NOTE:** The Edit Schedule button is available for a saved search or a scheduled report. Using the command for a saved search allows you to convert it to a scheduled report.

   **NOTE:** Clicking the Open button at the bottom of the Select a Saved Search dialog, closes the dialog and returns you to the Activity Center view, where the query tiles for the selected search or report appear. You can then select Run to generate the report.

### Viewing event details

Additional detailed information is available for some activity events.

**To see the details of a specific event**

1. Double-click (or double-tap) an event to view additional details.
2. On Password management events, select Details to see the details of the password change or check tasks.
3. Double-click (or double-tap) to close the event details.

### Auditing request workflow

In addition to reviewing activity, you can use the Activity Center to audit the transactions that occurred during the request workflow process, from request to approval to review. For
session requests, you can also play back a recorded or live session if Record Sessions is enabled in the entitlement's policy.

**NOTE:** If you are an authorized reviewer, you can audit an access request's workflow of a completed request awaiting review from the Home page as well.

**To audit request workflow**

1. Open the Activity Center, use the query tiles to specify the content of the report and click (or tap) **Run**.

   **TIP:** You can change the activity category tile to specify that you want to see Access Request Activity, Session Specific Activity events, or both.

2. Select an access request event and click (or tap) **Workflow** to audit the transactions that occurred during the request's workflow from request to approval to review.

   **TIP:** If you ran an all activity report, use the filter in the Events column to locate the access request activities.

3. For session requests that have Record Session enabled in the policy, you can play back a recorded or active session:
   a. Locate an access request session event and click (or tap) **Play** to launch the Safeguard Desktop Player.

      **NOTE:** A (green dot) indicates the session is "live". A user with Security Policy administrator permissions can click this icon to follow an active session.

      **NOTE:** If the session recording has been archived and removed from the local Safeguard file system, you will see a **Download** button instead of a **Play** button. Click (or tap) **Download** to download the recording and then click (or tap) **Play**.

   b. Accept the certificate to continue.

   c. Use one of the following methods to play back the session recording:
      - Click **Play Channel** from the toolbar at the top of the player.
      - Click the thumbnail in the upper right corner of the Information page.
      - Click **Play Channel** next to a channel in the Channels pane.

4. For SSH session requests that have the Enable Command Detection option selected in the policy, you can review a list of the commands and programs run during the session.

For RDP session requests that have the Enable Windows Title Detection option selected in the policy, you can review a list of all the windows opened on the desktop during the privileged session.

   a. Click the Sessions Events link above the transaction grid to view a list of all the session events and recordings available for the selected session.
b. To see the individual events that occurred during a particular Initialize Session transaction:
   - Click (or tap) **Show Details** to display additional information about the Initialize Session event, including Session Events.
   - Click (or tap) the **events** link to view the commands and programs run during that particular Initialize Session event.

The **Session Events** dialog displays listing the events with a time stamp showing when the event occurred as well as in which recording if multiple recordings were created.

**Filtering report results**

To find information in an activity audit log report or entitlement report, use the controls in the grid heading row to filter the data.

**To filter columns**

1. Click (or tap) **Filter** to open the filter list.
2. Select individual objects in the filter list to display specific information.

   **NOTE:** You can also choose the **Select All** check box at the top of the filter list and clear individual objects.

   **TIP:** When a column has selected filter criteria, Safeguard highlights the **filter symbol.**

**Sorting report results**

Use the controls in the grid heading row to sort report results or rearrange the columns of data.

**To sort or move columns**

**NOTE:** An arrow in the column heading identifies the sort criteria and order, ascending or descending, being used to display information.

1. Click the column heading to be used for the sort criteria.
2. The sort order is in ascending order. To change it to descending order, click the heading a second time.
3. To specify a secondary sort order, press the **SHIFT** key and then click the heading of the column to be used for the secondary sort order.
4. To change the order of the columns, click the heading of the column to be moved.
5. Drag and drop the column to a new location within the grid.
Reports

Reports allows the Auditor and Security Policy administrators to view and export entitlement reports that show which assets and accounts a selected user is authorized to access.

Reports toolbar

The toolbar at the top of Reports contains these options.

Table 23: Reports toolbar options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄 Refresh</td>
<td>Refresh updates the entitlement report.</td>
</tr>
<tr>
<td>📄 Export</td>
<td>Export creates a .json file of the report in a location of your choice.</td>
</tr>
</tbody>
</table>

One Identity Safeguard provides these entitlement reports.

Table 24: Entitlement reports

<table>
<thead>
<tr>
<th>Entitlements By...</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Lists information about the accounts a selected user is authorized to request.</td>
</tr>
<tr>
<td>Asset</td>
<td>Lists information about the accounts associated with a selected asset and the users who have authorization to request those accounts.</td>
</tr>
<tr>
<td>Account</td>
<td>Lists information about the users who have authorization to request a selected account, including asset and directory accounts.</td>
</tr>
</tbody>
</table>

Running an entitlement report

To run an entitlement report

1. From the Safeguard desktop Home page, select 🔄 Reports.
2. Choose a type of report: User, Asset or Account.
3. Browse to select specific objects for the report.
   - In the selection dialog, select one or more objects to be included in the report, then click (or tap) OK.
4. The top of the report displays the following information:
User:
- Name: The name of the user.
- Accounts: Number of accounts each user is allowed to access.

Asset:
- Name: The name of the asset.
- Accounts: Number of accounts on this asset that can be accessed.
- Requesters: Number of users allowed to request access to the asset’s accounts.
- Partition: The name of the partition to which the asset belongs.
- Users: The name of the requesters allowed to request access.

Account:
- Name: Name of the account.
- Asset: Name of the asset associated with the account.
- Requesters: Number of requesters allowed to access an account.

5. Select an item from the top pane to view additional details.

| NOTE: | For Entitlements by Assets, you can continue to drill down into the details of an item. For example, you can view both the Total Accounts tab and the People tab to see more details about the users that can request the accounts on an asset. Select an item from the results to drill down further into the details about the users and the accounts. |

6. To filter the results, use the filter control in the column heading. For more information, see Filtering report results on page 59.

**Administrative Tools**

The **Administrative Tools** allow you to add all the objects you need to write access request policies, such as users, accounts, and assets. From this view, you can also configure all of the Safeguard settings.

| NOTE: | You must have administrator permissions to use the **Administrative Tools** and the administrator permissions you have determine what you can view and modify. |

The navigation pane along the left side of the console gives you access to these administrative tools.
<table>
<thead>
<tr>
<th>Administrative Tools</th>
<th>Description</th>
<th>Administrator permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toolbox</td>
<td>Where you can gain quick access to all the tasks you can perform from a single portal.</td>
<td>Users with any Safeguard administrator privileges.</td>
</tr>
<tr>
<td>Accounts</td>
<td>Where you associate account identities with managed systems.</td>
<td>Asset Administrator or Auditor</td>
</tr>
<tr>
<td>Account Groups</td>
<td>Where you define sets of accounts which you can add to the scope of an access request policy.</td>
<td>Auditor or Security Policy Administrator</td>
</tr>
<tr>
<td>Assets</td>
<td>Where you add computers, servers, network devices, or applications to be managed by a Safeguard appliance.</td>
<td>Asset Administrator or Auditor</td>
</tr>
<tr>
<td>Asset Groups</td>
<td>Where you define sets of assets which you can add to the scope of an access request policy.</td>
<td>Auditor or Security Policy Administrator</td>
</tr>
<tr>
<td>Directories</td>
<td>Where you add external identity providers such as Microsoft Active Directory to Safeguard.</td>
<td>Auditor or Directory Administrator</td>
</tr>
<tr>
<td>Entitlements</td>
<td>Where you specify the access request policies that restrict system access to authorized users.</td>
<td>Auditor or Security Policy Administrator</td>
</tr>
<tr>
<td>Partitions</td>
<td>Where you define collections of assets which can be used to segregate assets for delegation.</td>
<td>Asset Administrator, Auditor, or delegated partition owner</td>
</tr>
<tr>
<td>Settings</td>
<td>Where you configure Safeguard to run backups, install updates, manage clusters, manage certificates, enable event notifications, configure external integration, define profile configurations settings, define user password rules, define discovery rules, and run troubleshooting tools.</td>
<td>Users with any Safeguard administrator privileges, however, the settings available depend on the administrative permissions assigned.</td>
</tr>
<tr>
<td>Users</td>
<td>Where you set up users who can log into Safeguard.</td>
<td>Bootstrap, Asset Administrator, Auditor, Authorizer Administrator, Help Desk Administrator, Security Policy Administrator, or User</td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>Description</td>
<td>Administrator permissions</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>User Groups</td>
<td>Where you define sets of Safeguard users which you can add to an entitlement.</td>
<td>Bootstrap, Auditor, Authorizer Administrator, Security Policy Administrator, or User Administrator</td>
</tr>
</tbody>
</table>

All of the **Administrative Tools** views have the following components, except for the **Toolbox** and **Settings**:

- **Toolbar** across the top of the view.
- **Object list** (left pane)
- **Search box** at the top of the object list.
- **Details pane** (right pane)

### Toolbar

The toolbar at the top of the views (except for the **Toolbox** and **Settings**), contain these options, depending on your **Administrator permissions** and the administrative tool you are in.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Add" /></td>
<td>Add objects to the Safeguard appliance.</td>
</tr>
<tr>
<td><img src="image" alt="Delete" /></td>
<td>Remove objects from the appliance.</td>
</tr>
<tr>
<td><img src="image" alt="Refresh" /></td>
<td>Refresh the screen.</td>
</tr>
<tr>
<td><img src="image" alt="Import" /></td>
<td>Add a set of objects from a .csv file. For more information, see Importing objects on page 388.</td>
</tr>
<tr>
<td><img src="image" alt="User Security" /></td>
<td>Menu options include: Set Password and Unlock accounts. For more information about these options, refer...</td>
</tr>
</tbody>
</table>

**NOTE:** Whenever you add, modify, or delete an object in **Administrative Tools**, the changes you make cannot be seen by other administrators running Safeguard on other clients unless they click (or tap) **Refresh**.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>to Setting a local user’s password and Unlocking a user’s account.</td>
</tr>
<tr>
<td>Account Security</td>
<td>Menu options include: Set Password, Check Password, and Change Password. For more information, see Checking, changing, or setting an account password on page 110.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Set administrator permissions for users. For more information, see Administrator permissions on page 421.</td>
</tr>
<tr>
<td>Set as Default</td>
<td>Set a directory or partition as the default. For more information, see Setting a default partition, Setting a default partition profile, and Setting a default directory profile.</td>
</tr>
<tr>
<td>Download SSH Key</td>
<td>Add the SSH Key to the selected asset. For more information, see Downloading a public SSH key on page 166.</td>
</tr>
<tr>
<td>Password Archive</td>
<td>Display the password history for the selected account. For more information, see Viewing password archive on page 112.</td>
</tr>
<tr>
<td>Access Requests</td>
<td>Enable or disable access request services for the selected account.</td>
</tr>
<tr>
<td>Discovery</td>
<td>Add or manage asset discovery jobs. For more information, see Discovery on page 156.</td>
</tr>
<tr>
<td>Show Ignored</td>
<td>Display the hidden assets.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hide Ignored</td>
<td>Hide assets marked as &quot;Ignore&quot;.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>Only available for Assets.</td>
</tr>
<tr>
<td>Sync Now</td>
<td>Run the directory addition and deletion synchronization process on demand. In addition, it runs through the discovery, if there are discovery rules and configurations set up.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>Only available for Directories.</td>
</tr>
</tbody>
</table>

**Search box**

The search box located at the top of the object list pane can be used to filter the data being displayed. When you enter a text string into the search box, the results include items that have a string attribute that "contains" the text that was entered.

| NOTE:          | This same basic search functionality is also available for many of the detail panes and selection dialogs allowing you to filter the data displayed in the associated pane or dialog.                                                                                                                                                                                                                     |

When searching for objects in the object lists, an attribute search functionality is also available where you can filter the results, based on a specific attribute. That is, the search term matches if the specified attribute "contains" the text. To perform an attribute search, click the icon to select the attribute to be searched.

Rules for using the search functionality:

- Search strings are not case sensitive.
- Wild cards are not allowed.
- Search strings must be an exact match. Do not add quotes or underlines. For example, from the Settings pane, enter password rules to return Safeguard Access > Password Rules. If you enter "password rules" or password_rules, the following message is returned: No matches found.
- When multiple search strings are included, all search criteria must be met in order for an object to be included in the results list.
- When you combine a basic search and an attribute search, the order they are entered into the search box matters. The attribute searches can be in any order, but the basic search must come after the attribute searches.
- In large environments, you will see a result number to tell you how many objects match the criteria; however, only the first 200 objects will be retrieved from the server. When you scroll down the list, more objects will be retrieved (paged) as needed.
To search for objects or object details

1. Enter a text string in the Search box. As you type, the list displays items whose string attributes contain the text that was entered.

   For example, enter T in the search box to search for items that contain the letter "T", or enter sse to list all items that contain the string "sse", such as "Asset".

   **NOTE:** The status bar along the bottom of the console shows the number of items returned.

2. To clear the search criteria, click (or tap) **Clear**.

   When you clear the search criteria, the original list of objects are displayed.

To conduct an attribute search

The attributes available for searching are dependent on the type of object being searched. The search drop-down menu lists the attributes that can be selected.

**NOTE:** The drop-down menu lists a limited number of attributes that can be searched; however, you can perform an attribute search using the English name of any attribute as it appears in the API. Nested attributes can be chained together using a period (.).

To see a list of all the attributes, see the API documentation. For information about the API, see [How do I access the API](#).

1. Click (or tap) the **icon and select the attribute to be searched.

   The selected attribute is added to the search box. For example, if you select **LastName**, **Last Name**: is added to the search box.

2. In the search box, enter the text string after the colon in the attribute label.

   **NOTE:** You can specify multiple attributes, repeating these steps to add an additional attribute to the search box. Do not add punctuation marks, such as commas or colons to separate the different attributes. When multiple attributes are included, all search criteria must be met in order for an object to be included in the results list.

   As you type, the list displays items whose selected attributes contain the text that was entered.

   **NOTE:** The status bar along the bottom of the console shows the number of items returned.

3. To clear the search criteria, click (or tap) **Clear**.

   When you clear the search criteria, the original list of objects are displayed.

Sorting object lists

By default the objects are listed in alphabetical order; however, you can use the controls located above the list to sort the object list.
To sort the object lists

1. Select **Ascending** or **Descending** under the **Search** box to sort the list in either alphabetical or reverse-alphabetical order.

2. To sort the list of **Accounts**, open the drop-down menu under the **Search** box and choose one of the following options before sorting the list in either **Ascending** or **Descending** order:
   - Name (Default)
   - Description
   - Asset
   - Profile
   - Partition

3. To sort the list of **Account Groups**, open the drop-down menu under the **Search** box and choose one of the following options before sorting the list in either **Ascending** or **Descending** order:
   - Name (Default)
   - Description
   - Dynamic

4. To sort the list of **Assets**, open the drop-down menu under the **Search** box and choose one of the following options before sorting the list in either **Ascending** or **Descending** order:
   - Name (Default)
   - Description
   - Platform
   - Network Address
   - Partition

5. To sort the list of **Asset Groups**, open the drop-down menu under the **Search** box and choose one of the following options before sorting the list in either **Ascending** or **Descending** order:
   - Name (Default)
   - Description
   - Dynamic

6. To sort the list of **Directories**, open the drop-down menu under the **Search** box and choose one of the following options before sorting the list in either **Ascending** or **Descending** order:
   - Name (Default)
   - Description
   - Platform
7. To sort the list of **Entitlements**, open the drop-down menu under the **Search** box and choose one of the following options before sorting the list in either **Ascending** or **Descending** order:
   - Priority (Default)
   - Name
   - Description

8. To sort the list of **Partitions**, open the drop-down menu under the **Search** box and choose one of the following options before sorting the list in either **Ascending** or **Descending** order:
   - Name (Default)
   - Description

9. To sort the list of **Users**, open the drop-down menu under the **Search** box and choose one of the following options before sorting the list in either **Ascending** or **Descending** order:
   - User Name (Default)
   - Description
   - First Name
   - Last Name
   - Email Address
   - Domain Name

10. To sort the list of **User Groups**, open the drop-down menu under the **Search** box and choose one of the following options before sorting the list in either **Ascending** or **Descending** order:
    - Name (Default)
    - Description
    - Type (Sorts by Local and Directory groups.)
Privileged access requests

One Identity Safeguard provides a workflow engine that supports time restrictions, multiple approvers, reviewers, emergency access, and expiration of policy. It also includes the ability to input reason codes and integrate directly with ticketing systems.

In order for a request to progress through the workflow process, authorized users perform "assigned" tasks. These tasks are performed from the user's Home page in the desktop client or web client.

As a Safeguard user, your Home page provides a quick view to the access request tasks that need your immediate attention. In addition, Safeguard can be configured to alert you when you have pending tasks awaiting your attention. For more information, see Configuring alerts on page 72.

The access request tasks you see on your Home page depend on the rights and permissions you have been assigned by an entitlement’s access request policies. For example:

- Designated "requesters" see tasks related to submitting new access requests, as well as actions to be taken once a request has been approved (for example, viewing passwords, copying passwords, launching sessions and checking in completed requests).
  
  Requesters can also define favorite requests, which then appear on their Home page for subsequent use. For more information, see Creating, editing, or removing a favorite request on page 70.

- Designated "approvers" see tasks related to approving (or denying) and revoking access requests.

- Designated "reviewers" see tasks related to reviewing completed (checked in) access requests, including playing back a session if session recording is enabled.

Password release requests and session requests use the same workflow engine; however, the actions taken on a session request are slightly different than those taken on a password release request. Therefore, we will cover each of these access request workflows separately:

- Password release request workflow
- Session request workflow
Creating, editing, or removing a favorite request

If designated as a requester, Safeguard allows you to add an access request as a Favorite to your Home page.

NOTE: Favorites are unique for the user; they are available when you log into the desktop client or the web client.

You can create a favorite request from your Favorites pane on your Home page or from the New Access Request dialog when creating or editing an access request.

**To create a favorite request from your Home page**

1. In the Favorites pane, click (or tap) + New Favorite.
2. In the New Access Request dialog, specify the assets, accounts, and type of asset to be included in the access request.
   a. On the Asset Selection tab, select the assets to be included in the access request.
   b. On the Account & Access Type tab, select the accounts to be included in the access request and the type of access being requested for each selected account.
      - **Account**: The available account appears in the Account column. When an asset has multiple accounts available, click (or tap) Select Account(s) to select an account from the displayed list.
      - **Access Type**: The type of access request appears in the Access Type column. When multiple access request types are available, this value appears as a hyperlink. Click (or tap) this hyperlink to select the access type.
3. Click (or tap) the Add to Favorites button.
4. In the Add to Favorites dialog, specify the following:
   a. **Name**: Enter a name for the request. Required
   b. **Description**: Enter descriptive text about the request.
   c. **Color**: Select the icon color to be used to display the request in your Favorites pane.

Click (or tap) Add.

The dialogs will close and the new favorite will be added to the Favorites pane on your Home page.
To create a favorite request from the New Access Request dialog

1. At the bottom of the New Access Request dialog, click (or tap) the Add to Favorites button when you are creating a new request.

   **NOTE:** The Add to Favorites button is enabled when you have selected the minimum required information (that is, at least one asset, account, and an access type) for the access request.

2. In the Add to Favorites dialog, specify the following:
   a. **Name:** Enter a name for the request. Required
   b. **Description:** Enter descriptive text about the request.
   c. **Color:** Select the icon color to be used to display the request in your Favorites list.

   Click (or tap) Add.

To change a favorite request’s icon color

1. At the top of the Favorites pane, click (or tap) the Color Selected button.

2. Select the check box to the left of the favorite request to be changed.

   **NOTE:** Selecting a favorite request, instead of the check box, displays the New Access Request dialog to edit and submit the access request.

3. Click (or tap) Color Selected.

4. In the Settings dialog, choose a color and select OK.

   The icon for the favorite now appears in the color you selected.

To remove a favorite request

1. At the top of the Favorites pane, click (or tap) the Color Selected button.

2. Select the check box to the left of the favorite request to be removed.

   **NOTE:** Selecting a favorite request, instead of the check box, displays the New Access Request dialog to edit and submit the access request.

3. Click (or tap) the Remove Selected button.

4. Select Yes to confirm.
Configuring alerts

All users are subscribed to the following email notifications; however, users will not receive email notifications unless they have been included in a policy as a requester (user), approver, or reviewer.

- Access Request Approved
- Access Request Denied
- Access Request Expired
- Access Request Pending Approval
- Access Request Revoked
- Password was Changed
- Review Needed

There are two ways to configure One Identity Safeguard to send event alerts to Safeguard users:

### Table 27: Notification types

<table>
<thead>
<tr>
<th>Notification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Toast notifications</strong></td>
<td>Configure alerts that appear on your console when the desktop client application is not the active foreground application.</td>
</tr>
<tr>
<td><strong>Email notifications</strong></td>
<td>Configure email notifications.</td>
</tr>
</tbody>
</table>

**Toast notifications**

Toast notifications are alerts that appear on your console when the desktop client application is not the active foreground application; for example, when you are in another application or when you have minimized the One Identity Safeguard desktop client.

**To enable toast notifications**

1. Open Settings.
2. Select the Enable Toast Notifications check box.

| **NOTE:** When you select the Run in the System Tray check box, you cannot modify the toast notifications option because in that mode, you always get notifications. |
Email notifications

You must configure One Identity Safeguard properly for users to receive email notifications:

- You must set your email address correctly in My Accounts. For more information, see User avatar on page 44.
- The Security Policy Administrator must configure the access request policies to notify people of pending access workflow events (that is, pending approvals and pending reviews). For more information, see Creating an access request policy on page 214.
- The Appliance Administrator must configure the SMTP server. For more information, see Enabling email notifications on page 327.

Password release request workflow

One Identity Safeguard for Privileged Passwords provides secure control of administrative accounts by storing account passwords until they are needed and releases them only to authorized persons. Then, Safeguard automatically updates the account passwords based on configurable parameters.

Typically a password release request follows this workflow.

1. **Request**: Users that are designated as an authorized "user" of an entitlement can request passwords for any account in the scope of that entitlement’s policies.

2. **Approve**: Depending on how the Security Policy Administrator configured the policy, a password release request will either require approval by one or more Safeguard users, or be auto-approved. This process ensures the security of account passwords, provides accountability, and provides dual control over the system accounts.

3. **Review**: The Security Policy Administrator can optionally configure an access request policy to require a review of completed password release requests for accounts in the scope of the policy.

The following topics explain the entire end-to-end password release process from request to approval to review.

Requesting a password release

If you are designated as an authorized "user" of an entitlement, you can request passwords for any account in the scope of the entitlement’s policies.

**NOTE**: You can configure One Identity Safeguard to notify you of pending password release workflow events, such as when a password release request is pending, denied or revoked, and so forth. For more information, see Configuring alerts on page 72.
To request a password release

1. From your Home page, click (or tap) New Request to open the New Access Request dialog.

   ![NOTE: You can also submit an access request from your Favorites pane, if you previously saved it as a favorite.

2. On the Asset Selection tab, select the assets to be included in the access request.
   Limit: 50 assets
   The assets available for selection are based on the scope defined in the entitlement’s access request policies.

3. On the Account & Access Type tab, select the accounts to be included in the access request and the type of access being requested for each selected account.
   - **Account**: The available account appears in the Account column. When an asset has multiple accounts available, either Select Account(s) or the account name appears as a hyperlink in the Account column. Click (or tap) the hyperlink in the Account column to display a list of accounts available and select the accounts to be included in the access request.
   - **Access Type**: The type of access request appears in the Access Type column. When multiple access request types are available, this value appears as a hyperlink, which when selected displays an additional dialog allowing you to select the access type. Select Password Request.

   To remove an asset or account from the list, select the entry in the grid and click (or tap) the — Delete toolbar button.

4. On the Request Details tab, configure the following settings, which will apply to all of the selected assets and accounts:
   a. **Normal Access**: Select this option to gain normal access to this password. Normal access ensures the access request goes through the entire end-to-end access release process from request to approval to review as defined in the policy by the Security Policy Administrator.

      ![NOTE: This option is only available if the policy has emergency access enabled.

   b. **Emergency Access**: Select this option to gain immediate emergency access to this password. When you use Emergency Access, the request requires no approval. For more information, see Creating an access request policy on page 214.

      ![NOTE: This option is only available if the policy has emergency access enabled.

   c. **Request Immediately**: Clear this option to enter a specific date and time for the request.

      ![NOTE: Enter the time in the user’s local time.
d. **Checkout Duration:** This either displays the checkout duration; or, if the **Allow Requester to Change Duration** option is enabled in the policy, it allows you to set the days, hours, and minutes that you want the password and overrides the checkout duration set in the access request policy. For more information, see [Creating an access request policy](#) on page 214.

e. **Ticket Number:** Enter a valid ticket number for this request.

| NOTE: Safeguard does not display the Ticket Number option unless the Security Policy Administrator selected **Require Ticket Number** for this policy. For more information, see Ticketing on page 338. |
| When multiple accounts are specified in the request, if any of the selected accounts require a ticket number, you must specify a valid ticket number. The specified ticket number will be applied to all of the requests associated with this access request. |

f. **Reason:** Select an access request reason code for this request.

Select the **Description** down arrow to view the description defined for the selected reason.

| NOTE: Safeguard does not display the Reason option unless the Security Policy Administrator selected reasons for this policy. For more information, see Reasons on page 249. |
| When multiple accounts are specified in the request, if any of the selected accounts require a reason, you must specify a reason. The specified reason will be applied to all of the requests associated with this access request. |

g. **Comment:** Enter information about this request.

| Limit: 255 characters |
| NOTE: When multiple accounts are specified in the request, if any of the selected accounts require a comment, you must enter a comment. The comment will be applied to all of the requests associated with this access request. |

5. To save the access request as a favorite, click (or tap) the **Add to Favorites** button.

The **Add to Favorites** dialog displays allowing you to specify a name and description for the access request. It also allows you to assign a color to the request's icon.

This access request is then added to your **Home** page **Favorites** pane. Selecting it from the **Favorites** pane displays the **New Access Request** dialog allowing you to edit the request details or enter a required reason or comment before submitting the request.

6. After entering the required information, click (or tap) **Submit Request**.

The **Access Request Result** dialog displays showing you the access requests submitted and whether a request was successful.
Taking action on a password release request

The actions that can be taken on a password release request depends on the state of the request.

To take action on a password release request

1. From your Home page, the Requests widget has these controls:
   a. Select (expand down) to open the list of active requests.
   b. Select Popout to float the Requests pane.
   
   You can then select and drag the pane to any location on the console and resize the window.

   ⚠️ NOTE: You enable or disable the Home page widgets in the Settings menu.

2. Open the list of requests and select one of these view filters:

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Requests in all states.</td>
</tr>
<tr>
<td>Available</td>
<td>Approved requests that are ready to view or copy.</td>
</tr>
<tr>
<td>Approved</td>
<td>Requests that have been approved, but the checkout time has not arrived.</td>
</tr>
<tr>
<td>Pending</td>
<td>Requests that are waiting for approval or for pending accounts restored when using the Safeguard suspend feature.</td>
</tr>
<tr>
<td>Revoked</td>
<td>Approved requests retracted by the approver.</td>
</tr>
<tr>
<td>Expired</td>
<td>Requests for which the checkout duration has elapsed.</td>
</tr>
<tr>
<td>Denied</td>
<td>Requests denied by the approver.</td>
</tr>
</tbody>
</table>

   ⚠️ NOTE: The number indicates how many requests are in that state.

3. Select an account to see the details of the password release request.

4. Take the following actions on password release requests:

<table>
<thead>
<tr>
<th>State</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>Select Copy to checkout the password. This puts the password into your copy buffer, ready for you to use. Select Check-In to complete the password checkout</td>
</tr>
<tr>
<td>State</td>
<td>Actions</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Show Password</strong> to view the password on your screen. The password displays on your screen for 20 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: Selecting either <strong>Copy</strong> or <strong>Show Password</strong> constitute a password &quot;checkout&quot;.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: If the password changes while you have it checked out, and your current request is still valid, select either <strong>Copy</strong> or <strong>Show Password</strong> again to obtain the new password.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Hide Password</strong> to conceal the password from view.</td>
</tr>
<tr>
<td>Approved</td>
<td>Select ✧ <strong>Cancel</strong> to remove the request.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: A password release request changes from &quot;Approved&quot; to &quot;Available&quot; when the requested time is reached. It stays available until you either cancel the request or it reaches the end of the duration period.</td>
</tr>
<tr>
<td>Pending</td>
<td>Select ✧ <strong>Cancel</strong> to remove the request.</td>
</tr>
<tr>
<td>Revoked</td>
<td>Select ✧ <strong>Resubmit Request</strong> to request the password again.</td>
</tr>
<tr>
<td></td>
<td>Select ✧ <strong>Remove</strong> to delete the request from the list.</td>
</tr>
<tr>
<td>Expired</td>
<td>Select ✧ <strong>Remove</strong> to delete the request from the list.</td>
</tr>
<tr>
<td>Denied</td>
<td>Select ✧ <strong>Resubmit Request</strong> to request the password again.</td>
</tr>
<tr>
<td></td>
<td>Select ✧ <strong>Remove</strong> to delete the request from the list.</td>
</tr>
</tbody>
</table>

**Approving a password release request**

Depending on how the Security Policy Administrator configured the policy, a password release request will either require approval by one or more Safeguard users, or be auto-approved. This process ensures the security of account passwords, provides accountability, and provides dual control over the system accounts.

**NOTE**: You can configure Safeguard to notify you of a password release request that requires your approval. For more information, see Configuring alerts on page 72.
To approve or deny a password release request

1. From your Home page, the Approvals widget has these controls:
   a. Select (expand down) to open the list of approvals.
   b. Select Popout to float the Approvals pane.

   You can then select and drag the pane to any location on the console and re-size the window.

   
   NOTE: You enable or disable the Home page widgets in the Settings menu.

2. Open the list of approvals and select one of these view filters:

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Password release requests in all states.</td>
</tr>
<tr>
<td>Pending</td>
<td>Requests that are waiting for approval.</td>
</tr>
<tr>
<td>Approved</td>
<td>Requests that have been approved, but not yet available to the requester.</td>
</tr>
</tbody>
</table>

   NOTE: The number indicates how many requests are in that state.

3. Once you open the list, select the requester’s name to see the details of the password release request.

4. Take the following actions on password release requests:

<table>
<thead>
<tr>
<th>State</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending</td>
<td>Select Approve or Deny a password release request. Optionally, enter a comment of up to 255 characters.</td>
</tr>
<tr>
<td>Pending Additional Approvers</td>
<td>Select to Deny a password release request. Optionally, enter a comment of up to 255 characters.</td>
</tr>
<tr>
<td>Approved</td>
<td>Select to Deny or Revoke an approved request.</td>
</tr>
</tbody>
</table>

   NOTE: You can revoke a request between the time the requester views it and checks it in.

   Any eligible approver can deny a password release request after it has already been approved or auto-approved. Once disallowed, the requester will no longer have access to the password, but he is given another opportunity to request that password again. The requester receives an email notifying him that the request was denied.
Reviewing a completed password release request

The Security Policy Administrator can configure an access request policy to require a review of completed password release requests for accounts in the scope of the policy.

NOTE: You can configure Safeguard to notify you of a password release request that requires your review. For more information, see Configuring alerts on page 72.

To review a completed password release request

1. From your Home page, the Reviews widget has these controls:
   a. Click (or tap) ▼ (expand down) to open the list of pending reviews.
   b. Click (or tap) ➤ Popout to float the Reviews pane.
      You can then select and drag the pane to any location on the console and resize the window.

   NOTE: You enable or disable the Home page widgets in the Settings menu.

2. Open the list of pending reviews and select an account name to see the details of the password release request.

3. Take the following action on password release requests:
   - Select ⌉ Workflow to review the transactions that took place in the selected request.
   - Select ⌎ Review to complete the review process.
      Optionally, enter a comment of up to 255 characters.

   Once the review is complete, it no longer appears on the Reviews pane.

   TIP: If one requester checks in the request and another requester wants to use it, the second requester is unable to check out the password until the original request has been reviewed. However, the Security Policy administrator can Close a request that has not yet been reviewed. This will bypass the reviewer in the workflow and allow the account to be accessed by another requester.

Session request workflow

One Identity Safeguard for Privileged Sessions allow authorized users to authorize connections, view active connections, limit access to specific resources, be alerted if connections exceed pre-set time limits and even terminate connections. Typically a session request follows this workflow.
1. **Request**: Users that are designated as an authorized "user" of an entitlement can request an RDP or SSH session for any asset in the scope of that entitlement’s policies.

2. **Approve**: Depending on how the Security Policy Administrator configured the policy, a session request will either require approval by one or more Safeguard users, or be auto-approved.

3. **Review**: The Security Policy Administrator can optionally configure an access request policy to require a review of completed requests for assets in the scope of the policy. In addition, if session recording is enabled in the policy, reviewers can audit the workflow transactions and launch the Safeguard Player to replay the session as part of the review process.

The following topics explain the entire end-to-end session access process from request to approval to review (and play back if sessions recording is enabled).

### About sessions and recordings

One Identity Safeguard proxies all sessions to target resources. Users do not have direct access to resources, therefore, the enterprise is protected against viruses, malware or other dangerous items on the user’s system. One Identity Safeguard for Privileged Sessions can proxy and record Unix/Linux, Windows, network devices, firewalls, routers and more.

### Important notes

- The Safeguard Desktop Player, used to play back recorded sessions, is installed with the Windows desktop client.
- Safeguard PuTTY is installed with the Windows desktop client and is used to launch the SSH client if PuTTY is not available on the machine.
- For some systems (SUSE and some Debian systems) that use SSH, you must enable password authentication in the package generated configuration file (sshd_config). For example, in the debian sshd_config file, set the following parameter: PasswordAuthentication yes.
- Sessions requests are enabled by default. However, if authorized users cannot request sessions, check the **Session Requests Enabled** setting (Administrative Tools | Settings | Access Request | Enable or Disable Services).

  **NOTE**: You must have Appliance Administrator permissions to manage the service settings.

- All session activity - every packet sent and action that takes place on the screen, including mouse movements, clicks and keystrokes - is recorded and available for play back.
- If Safeguard detects no activity for 10 minutes during a privileged session, the session is terminated.
- It is highly recommended to assign an archive server for each Safeguard appliance’s session recordings to avoid filling up the appliance’s disk space. For more information, see Session Recordings Storage Management on page 363.

- Both SSH and RDP session recordings use the Timestamping Certificate Authority. For more information, see Sessions Certificates on page 302. Recordings are signed and timestamped every 30 seconds so that partial recordings may be verified as authentic.

- During an RDP session, the Privileged Sessions module proxies the connection to the target asset.
  
  When an RDP connection is established, the Safeguard Privileged Sessions module will generate a certificate on the fly and sign it using the RDP Connection Signing Certificate. Therefore the RDP client trusts the RDP Connection Signing Certificate and the generated certificate that is signed by the RDP Connection Signing Certificate. This allows the client to verify that the connection is trusted.

- During an SSH session, the Privileged Sessions module proxies the connection to the target asset. Therefore, Safeguard’s SSH host Key (Settings | Sessions | SSH Host Key) must be trusted by the client. This SSH host key is unique and produced during manufacturing. This key can be trusted by the client or replaced with a different key if desired.

### Requesting session access

If you are designated as an authorized “user” of an entitlement, you can request access for a specific period (or session) to any account or asset in the scope of the entitlement’s policies.

| NOTE: | You can configure One Identity Safeguard to notify you of pending access request workflow events, such as when a session request is pending, denied or revoked, and so forth. For more information, see Configuring alerts on page 72. |

**To request session access**

1. From your 🏡 Home page, click (or tap) New Request to open the New Access Request dialog.
   
   | NOTE: | You can also submit an access request from your Favorites pane, if you previously saved it as a favorite. |

2. On the Asset Selection tab, select the assets to be included in the access request. Limit: 50 assets
   
   The assets available for selection are based on the scope defined in the entitlement’s access request policies.

3. On the Account & Access Type tab, select the accounts to be included in the access request and the type of access being requested for each selected account.
• **Account**: The accounts available appear in the **Account** column. When an asset has multiple accounts available, either **Select Account(s)** or the account name appears as a hyperlink in the **Account** column. Click (or tap) the hyperlink in the **Account** column to display a list of accounts available and select the accounts to be included in the access request.

The accounts available for selection are based on the Asset-Based Session Access setting (Access Config tab) defined for the entitlement's access request policy. That is:

- If **None** is selected in the access request policy, the accounts Safeguard retrieved from the vault will be available for selection. The selected account will then be used when the session is requested.
- If **User Supplied** is selected in the access request policy, you will be required to enter the user credentials as part of the request workflow, prior to launching the SSH or RDP session.
- If **Linked Account** is selected in the access request policy, linked directory accounts will be available for selection. The selected account will then be used when the session is requested.
- If **Directory Account** is selected in the access request policy, only the specified directory accounts will be available for selection. The selected directory account will then be used when the session is requested.

• **Access Type**: The type of access request appears in the **Access Type** column. When multiple access request types are available, this value appears as a hyperlink, which when selected displays an additional dialog allowing you to select the access type. Select one of the following for a session request: **RDP** or **SSH**.

  ![NOTE: The access type options available depend on the type of asset selected on the Asset Selection tab. For example, RDP is only available for Windows sessions.

To remove an asset or account from the list, select the entry in the grid and click (or tap) the **Delete** toolbar button.

4. On the **Request Details** tab, configure the following settings, which will apply to all of the selected assets and accounts:

a. **Normal Access**: Select this option to gain normal access to this password. Normal access ensures the access request goes through the entire end-to-end access release process from request to approval to review as defined in the policy by the Security Policy Administrator.

  ![NOTE: This option is only available if the policy has emergency access enabled.

b. **Emergency Access**: Select this option to gain immediate emergency access to this password. When you use **Emergency Access**, the request requires no approval. For more information, see **Creating an access request policy** on page 214.
c. **Request Immediately**: Clear this option to enter a specific date and time for the request.

   **NOTE**: Enter the time in the user’s local time.

d. **Checkout Duration**: This either displays the checkout duration; or, if the Allow Requester to Change Duration option is enabled in the policy, it allows you to set the days, hours, and minutes that you want the password and overrides the checkout duration set in the access request policy. For more information, see Creating an access request policy on page 214.

e. **Ticket Number**: Enter a valid ticket number for this request.

   **NOTE**: Safeguard does not display the Ticket Number option unless the Security Policy Administrator selected Require Ticket Number for this policy. For more information, see Ticketing on page 338.

   When multiple accounts are specified in the request, if any of the selected accounts require a ticket number, you must specify a valid ticket number. The specified ticket number will be applied to all of the requests associated with this access request.

f. **Reason**: Select an access request reason code for this request.

   Select the Description down arrow to view the description defined for the selected reason.

   **NOTE**: Safeguard does not display the Reason option unless the Security Policy Administrator selected reasons for this policy. For more information, see Reasons on page 249.

   When multiple accounts are specified in the request, if any of the selected accounts require a reason, you must specify a reason. The specified reason will be applied to all of the requests associated with this access request.

g. **Comment**: Enter information about this request.

   Limit: 255 characters

   **NOTE**: When multiple accounts are specified in the request, if any of the selected accounts require a comment, you must enter a comment. The comment will be applied to all of the requests associated with this access request.

5. To save the access request as a favorite, click (or tap) the Add to Favorites button. The Add to Favorites dialog displays allowing you to specify a name and description for the access request. It also allows you to assign a color to the request's icon.
This access request is then added to your Home page Favorites pane. Selecting it from the Favorites pane displays the New Access Request dialog allowing you to edit the request details or enter a required reason or comment before submitting the request.

6. After entering the required information, click (or tap) Submit Request.

The Access Request Result dialog displays showing you the access requests submitted and whether a request was successful.

Taking action on a session request

The actions a user authorized to request access to a privileged session can take depends on the state of the request.

To take action on a session request

1. From your Home page, the Requests widget has these controls:
   a. Select (expand down) to open the list of active requests.
   b. Select Popout to float the Requests pane.

   You can then select and drag the pane to any location on the console and resize the window.

   NOTE: You enable or disable the Home page widgets in the Settings menu.

2. Open the list of requests and select one of these view filters:

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Requests in all states.</td>
</tr>
<tr>
<td>Available</td>
<td>Approved requests that are ready (that is, a session that can be launched).</td>
</tr>
<tr>
<td>Approved</td>
<td>Requests that have been approved, but the checkout time has not arrived.</td>
</tr>
<tr>
<td>Pending</td>
<td>Requests that are waiting for approval.</td>
</tr>
<tr>
<td>Revoked</td>
<td>Approved requests retracted by the approver.</td>
</tr>
</tbody>
</table>

   NOTE: The approver can revoke a request between the time the requester launches the session and checks it back in.

   NOTE: When a user with Security Policy administrator permissions revokes a "live" session, the active session is terminated.
<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expired</td>
<td>Requests for which the checkout duration has elapsed.</td>
</tr>
<tr>
<td>Denied</td>
<td>Requests denied by the approver.</td>
</tr>
</tbody>
</table>

**NOTE:** The number indicates how many requests are in that state.

3. Select an account to see the details of the session request.
4. You can take the following actions on session requests, depending on the state:

<table>
<thead>
<tr>
<th>State</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>Click (or tap) <strong>Launch</strong> to launch the SSH client or Remote Desktop Connection. For more information, see <a href="#">Launching the SSH client</a> or <a href="#">Launching an RDP session</a>. Click (or tap) <strong>Check-In</strong> to complete the checkout process once you have ended your session. In addition, you can use the following buttons to view or copy information into the configuration dialog that contains the credentials needed to launch the session:</td>
</tr>
<tr>
<td></td>
<td>· <strong>View</strong>: Click (or tap) this button to view the password or connection string, which is required to launch the session.</td>
</tr>
<tr>
<td></td>
<td>· <strong>Copy</strong>: Click (or tap) this button to copy a value to the copy buffer.</td>
</tr>
<tr>
<td></td>
<td>· <strong>Help</strong>: Click (or tap) this button to copy the value into the appropriate field of the configuration dialog.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: The configuration dialogs are populated with the required information; these actions are available if the fields are not populated for some reason.</td>
</tr>
<tr>
<td>Approved</td>
<td>Click (or tap) <strong>Cancel</strong> to remove the request.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: A sessions request changes from &quot;Approved&quot; to &quot;Available&quot; when the requested time is reached. It stays available until you either cancel the request or it reaches the end of the duration period.</td>
</tr>
<tr>
<td>Pending</td>
<td>Click (or tap) <strong>Cancel</strong> to remove the request.</td>
</tr>
<tr>
<td>Revoked</td>
<td>Click (or tap) <strong>Resubmit Request</strong> to request the session again. Click (or tap) <strong>Remove</strong> to delete the request from the list.</td>
</tr>
</tbody>
</table>
### Approving a session request

Depending on how the Security Policy Administrator configured the policy, a sessions request will either require approval by one or more Safeguard users, or be auto-approved.

- **NOTE:** You can configure Safeguard to notify you of an access request that requires your approval. For more information, see Configuring alerts on page 72.

#### To approve or deny a sessions request

1. From your Home page, the Approvals widget has these controls:
   - a. Select ▼ (expand down) to open the list of approvals.
   - b. Select Popout to float the Approvals pane.
     - You can then select and drag the pane to any location on the console and resize the window.

- **NOTE:** You enable or disable the Home page widgets in the Settings menu.

2. Open the list of approvals and select one of these view filters:

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Requests in all states.</td>
</tr>
<tr>
<td>Pending</td>
<td>Requests that are waiting for approval.</td>
</tr>
<tr>
<td>Approved</td>
<td>Requests that have been approved, but not yet available to the requester.</td>
</tr>
</tbody>
</table>

- **NOTE:** The number indicates how many requests are in that state.

3. Once you open the list, select the requester's name to see the details of the sessions request.

4. Take the following actions on sessions requests:

<table>
<thead>
<tr>
<th>State</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending</td>
<td>Select <strong>Approve</strong> or <strong>Deny</strong> a sessions request. Optionally, enter a comment of up to 255 characters.</td>
</tr>
<tr>
<td>Pending Additional Approvers</td>
<td>Select <strong>Deny</strong> a sessions request. Optionally, enter a comment of up to 255 characters.</td>
</tr>
<tr>
<td>Approved</td>
<td>Select <strong>Deny</strong> or <strong>Revoke</strong> an approved request.</td>
</tr>
</tbody>
</table>

- **NOTE:** You can revoke a request between the time the requester views it and checks it in. Any eligible approver can deny an access request after it has already been approved or auto-approved. Once disallowed, the requester will no longer be able to access the requested session, but he is given another opportunity to request that session again. The requester receives an email notifying him that the request was denied. For more information, see Configuring alerts on page 72.

## Launching the SSH client

Once an SSH session request becomes available, the requester can launch the SSH client to start the session.

**To launch the SSH client to begin your session**

1. If the **User Supplied** option is selected in the policy, you will be prompted to enter your user credentials. After entering the requested credentials, click **Apply**. This will retrieve the information (for example, Hostname Connection String) required to launch the SSH client.

2. Click (or tap) the **Launch** button to the right of the asset name. Clicking this button displays the PuTTY Configuration dialog. The required information is populated, click **Open** to launch the SSH client.
NOTE: If the required information is not populated in the PuTTY Configuration dialog, use the following buttons to copy and paste the information into the dialog:

a. Use the buttons to the right of the Hostname Connection String to perform the following tasks:
   - 🔍 View: To view the hostname connection string.
   - ☁ Copy: To copy the value to your copy buffer, which can then be pasted into the Hostname field of the PuTTY Configuration dialog.
   - 🔄 Help: To copy the value into the Hostname field of the PuTTY Configuration dialog.

b. Use the buttons to the right of the Password to perform the following tasks:
   - 🔍 View: To view the password.
   - ☁ Copy: To copy the password to your copy buffer, which can then be pasted into the Password field of the PuTTY Configuration dialog.
   - 🔄 Help: To copy the value into the Password field of the PuTTY Configuration dialog.

NOTE: The Password field only appears if the Include password release with session requests option (Access Config tab) is selected in the entitlement's access request policy.

3. In the SSH client, run the commands or programs on the target host.

   NOTE: If there is no activity in an open session for about 10 minutes, the session will be terminated. However, as long as the request is in an Available state, you can launch the session again to resume your tasks.

4. Once you are completed, log out of the target host and select ✅ Check in to complete the session request process.

   This makes the session request available to reviewers. If the Record Sessions option is enabled in the policy, the reviewer can play back the recording as part of the review process. In addition, if the Enable Command Detection option is selected in the policy, the reviewer can view a list of the commands and programs run during the session.

Launching an RDP session

Once an RDP session request becomes available, the requester can launch the remote desktop connection to start the session.
**To launch a remote desktop connection to begin your RDP session**

1. If the **User Supplied** option is selected in the policy, you will be prompted to enter your user credentials. After entering the requested credentials, click **Apply**. This will retrieve the information (for example, Username Connection String) required to launch the remote desktop session.

2. Click (or tap) the **Launch** button to the right of the asset name. Clicking this button displays the **Remote Desktop Connection** dialog. Click **Connect** to launch the remote desktop session.

   **NOTE:** If the required information is not populated in the **Remote Desktop Connection** dialog, use the following buttons to copy and paste the information into the dialog:
   a. Use the buttons to the right of the **Username Connection String** to perform the following tasks:
      - **View**: To view the username connection string.
      - **Copy**: To copy the value to your copy buffer, which can then be pasted into the Username field of the **Remote Desktop Connection** dialog.
      - **Help**: To copy the value into the Username field of the **Remote Desktop Connection** dialog.
   b. Use the buttons to the right of the **Password** to perform the following tasks:
      - **View**: To view the password.
      - **Copy**: To copy the password to your copy buffer, which can then be pasted into the Password field of the **Remote Desktop Connection** dialog.
      - **Help**: To copy the value into the Password field of the **Remote Desktop Connection** dialog.

   **NOTE:** The Password field only appears if the **Include password release with session requests** option (Access Config tab) is selected in the entitlement’s access request policy.

3. In the remote desktop session, run the commands or programs on the target host.

   **NOTE:** If there is no activity in an open session for about 10 minutes, the session will be terminated. However, as long as the request is in an **Available** state, you can launch the session again to resume your tasks.

4. Once you are completed, log out of the target host and select **✓ Check in** to complete the session request process.

   This makes the session request available to reviewers. If the **Record Sessions** option is enabled in the policy, the reviewer can playback the recording as part of the review process. In addition, if the **Enable Window Title Detection** option is selected in the policy, the reviewer can view a list of the windows opened on the desktop during the session.
Reviewing a session request

The Security Policy Administrator can configure an access request policy to require a review of completed session requests for assets or accounts in the scope of the policy.

NOTE: You can configure Safeguard to notify you of an access request that requires your review. For more information, see Configuring alerts on page 72.

To review a completed sessions request

1. From your Home page, the Reviews widget has these controls:
   a. Click (or tap) ⬇️ (expand down) to open the list of pending reviews.
   b. Click (or tap) Popout to float the Reviews pane.

   You can then select and drag the pane to any location on the console and resize the window.

   NOTE: You enable or disable the Home page widgets in the Settings menu.

2. Open the list of pending reviews and select an account name to see the details of the sessions request.

3. Take the following action on sessions requests:
   a. Select Workflows to review the transactions that took place in the selected request.
      - If Record Sessions is enabled in the policy, click (or tap) ➤ Play on the Initialize Session event to play back the session.

      NOTE: A (green dot) indicates the session is "live". A user with Security Policy administrator permissions can click this icon to follow an active session.

      NOTE: If the session recording has been archived and removed from the local Safeguard file system, you will see a ✗ Download button instead of a ➤ Play button. Click (or tap) ✗ Download to download the recording and then click (or tap) ➤ Play.

      - If Enable Command Detection is enabled in the policy, expand to show the details and click the events link on the Initialize Session event to view a list of the commands and programs run during the session.

      NOTE: For an RDP session, the setting is Enable Windows Title Detection. When enabled, you can view a list of windows that were opened during the privileged session.

   b. Select Review to complete the review process.

      Optionally, enter a comment of up to 255 characters.

      Once the review is complete, it no longer appears on the Reviews pane.
Replaying a session

You can play back a recorded session from the Request Workflow dialog, which can be accessed by clicking the □ Workflow button that appears to reviewers for completed session requests and in the Activity Center view when an access request event is selected in an activity audit log report. In addition, you can play back a recorded session by clicking (or tapping) the icon displayed to the left of an access request session event on the activity audit log report in the Activity Center view.

NOTE: This feature is only available for session requests that have Record Session enabled in the access request policy (Access Config tab).

To play back a session (Request Workflow dialog)

1. Open the Request Workflow dialog using the □ Workflow button.

   NOTE: If accessing the Request Workflow dialog from the Activity Center, select an Access Request Session event from the activity audit log report.

2. Locate an Initialize Session event and click (or tap) ▶ Play to launch the Safeguard Desktop Player.

   NOTE: A (green dot) indicates the session is "live". A user with Security Policy administrator permissions can click this icon to follow an active session.

   NOTE: If the session recording has been archived and removed from the local Safeguard file system, you will see a ▼ Download button instead of a ▶ Play button. Click (or tap) ▼ Download to download the recording and then click (or tap) ▶ Play.

3. Accept the certificate to continue.

   NOTE: In the Certificate error message, click (or tap) Continue to use the default Session Recording Signing certificate shipped with Safeguard. To use a different SSL certificate, click (or tap) Abort and then import the appropriate certificates including the root CA.

4. Use one of the following methods to play back the session recording:
   - Click ▶ Play Channel from the toolbar at the top of the player.
   - Click ▶ in the thumbnail in the upper right corner of the Information page.
   - Click ▶ Play Channel next to a channel in the Channels pane.

For more information about the Safeguard Desktop Player and navigating through a recording, see Recording navigation.

For more information on archiving session recordings, see Session Recordings Storage Management.
Following and terminating a "live" session

An access request session event that contains a 🟢 (green dot) in the left-most column of the activity audit log report or Request Workflow dialog indicates that a "live" session is taking place. Clicking this button launches the Safeguard Desktop Player allowing you to follow what is happening in the active session. Safeguard also allows you to terminate an active session directly from the desktop player.

**NOTE:** You must have Security Policy administrator permissions to follow an active session.

**To watch or terminate a "live" session**

1. From the Request Workflow dialog or Activity Center activity audit log report click (or tap) the 🟢 (green dot) next to an access request session event.

   **NOTE:** Security Policy Administrators can also launch the Safeguard Desktop Player from the Access Requests view. Select an access request session in the request grid and click (or tap) the View Live Session toolbar button.

   The Safeguard Desktop Player launches allowing you to watch the active session. On the Information page, the thumbnail (upper right) displays a blinking red recording button when a session is "live".

2. Use one of the following methods to follow the session:
   - Click ➤ Play Channel from the toolbar at the top of the player.
   - Click ➤ in the thumbnail in the upper right corner of the Information page.
   - Click ➤ Play Channel next to a channel in the Channels pane.

3. In the playback window, you will see a **Terminate** button and a **Live** indicator in the lower right corner.

4. Click **Terminate** to stop the active session.

   **NOTE:** You can also terminate an active session by revoking the session through the Windows desktop client.
Toolbox

When you select the **Administrative Tools** link from the **Home** page navigation pane, the **Toolbox** view appears. This view gives you quick-start links to the tasks you can perform.

NOTE: The display is tailored to your Administrator permissions.

Each numbered tile gives you quick access to its Administrative Tool. Clicking displays the dialog allowing you to add an object.

In addition, the Toolbox allows you to view the status of running tasks.

- Viewing task status
- Stopping a task

**Viewing task status**

Safeguard displays a number on your **Toolbox** navigation link to notify you when you have any tasks running.

**To view task status**

1. Navigate to the **Toolbox**.
2. Click (or tap) **Popout** to float the **Tasks** pane.
   
   You can then select and drag the pane to any location on the console and resize the window.
3. Click (or tap) **Remove** to delete a task from the pane.
4. Click (or tap) **Cancel** next to a running task to stop a task.
5. Click (or tap) **Clear** to remove all items from the **Tasks** pane.
Stopping a task

To stop a task

1. In the Toolbox, open the Tasks pane.
2. Click (or tap) ☑ Cancel next to a running task.
Accounts

A Safeguard account is a unique identifier that Safeguard uses to control access to assets. Managed user, group, or service accounts exist on the asset. Each account has an associated asset; if you delete an asset, Safeguard permanently deletes all the accounts associated with it.

The Auditor and the Asset Administrator have permission to access Accounts.

**NOTE:** On Unix assets, the accounts are stored in `etc/passwd`; however, each platform implements this concept differently.

The Accounts view displays the following information about the selected account:

**NOTE:** Safeguard designates a service account with a Service Account icon. For more information, see About service accounts on page 140.

**Table 28: Accounts: Tabs**

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td>Displays general information about the selected account.</td>
</tr>
<tr>
<td>Access Request Policies tab</td>
<td>Displays the entitlements and access request policies associated with the selected account.</td>
</tr>
<tr>
<td>Account Groups tab</td>
<td>Displays the account groups that contain the selected account.</td>
</tr>
<tr>
<td>Check and Change Log tab</td>
<td>Displays the password validation and reset history for the selected account.</td>
</tr>
<tr>
<td>History tab</td>
<td>Displays the details of each operation that has affected the selected account.</td>
</tr>
</tbody>
</table>

For information about configuring account discovery in Safeguard, see Account discovery job workflow.
Use these toolbar buttons to manage accounts.

### Table 29: Accounts: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Add Account</td>
<td>Add accounts to Safeguard. For more information, see Adding an account on page 102.</td>
</tr>
<tr>
<td>Delete Selected</td>
<td>Remove the selected account. For more information, see Deleting an account on page 107.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of accounts.</td>
</tr>
<tr>
<td>Import Accounts</td>
<td>Add accounts to Safeguard. For more information, see Importing objects on page 388.</td>
</tr>
<tr>
<td>Account Security</td>
<td>Menu options include: Check Password, Change Password, and Set Password. For more information, see Checking, changing, or setting an account password on page 110.</td>
</tr>
<tr>
<td>Password Archive</td>
<td>Display the password history for the selected account. For more information, see Viewing password archive on page 112.</td>
</tr>
<tr>
<td>Access Requests</td>
<td>Allows you to enable or disable access request services for the selected account. Menu options include: Enable Password Request, Disable Password Request, Enable Session Request, Disable Session Request.</td>
</tr>
</tbody>
</table>

**NOTE:** Access request services are enabled by default for all accounts added directly to Safeguard, except for service accounts. Access request services are disabled by default for all discovered accounts.

### General tab

The **General** tab lists information about the selected account. Large tiles at the top of the tab display the number of Access Request Policies and Account Groups associated with the selected account. Clicking a tile heading opens the corresponding tab.

**NOTE:** These tiles are only visible to the Auditor.
NOTE: The time stamps for the password and SSH Key check and change transactions are based on the user’s local time.

**Table 30: Accounts General tab: General properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the selected account.</td>
</tr>
<tr>
<td>Asset</td>
<td>The display name of the managed system associated with this account. The time stamps for the password and SSH Key check and change transactions are based on the user’s local time.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> Accounts are only associated with one asset.</td>
<td></td>
</tr>
<tr>
<td>Partition</td>
<td>The name of the partition where the selected account resides.</td>
</tr>
<tr>
<td>Profile</td>
<td>The name of the profile that governs the accounts assigned to a partition.</td>
</tr>
<tr>
<td>Enable Password Request</td>
<td>True or False, indicating whether password release requests are enabled for this account.</td>
</tr>
<tr>
<td>Enable Session Request</td>
<td>True or False, indicating whether session access requests are enabled for this account.</td>
</tr>
<tr>
<td>Last Successful Password Check</td>
<td>The date and time of the last successful password validation. For more information, see Adding check password settings on page 347.</td>
</tr>
<tr>
<td>Next Password Check</td>
<td>The date and time of the next automated password check as set in the Check Password schedule of the partition profile. For more information, see Adding check password settings on page 347.</td>
</tr>
<tr>
<td>Last Successful Password Change</td>
<td>The date and time of the last successful password change.</td>
</tr>
<tr>
<td>Next Password Change</td>
<td>The date and time of the next automated password change as set in the Change Password schedule of the partition profile. For more information, see Adding change password settings on page 344.</td>
</tr>
<tr>
<td>Last Successful SSH Key Change</td>
<td>The date and time of the last successful SSH Key change.</td>
</tr>
<tr>
<td>Next SSH Key Change</td>
<td>The date and time of the next SSH Key change.</td>
</tr>
</tbody>
</table>

**Tags:** Tag assignments for the selected account.

The tiles displayed in the Tags pane include both the dynamic tags added through tagging rules and static tags that were added manually. In addition to viewing tag assignments, Asset Administrators can add and remove statically assigned tags.

**NOTE:** Dynamically assigned tags contain a lightening bolt icon and cannot be deleted; whereas, static tags which can be removed contain an X icon.

**Description:** Information about selected account.
Related Topics
Modifying an account

Access Request Policies tab

The **Access Request Policies** tab displays the entitlements and access request policies, including password release policies and session request policies, associated with the selected account.

Click (or tap) **Add to Policy** from the details toolbar to add the selected account to the scope of an access request policy.

### Table 31: Accounts: Access Request Policies tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entitlement</td>
<td>The name of the access request policy's entitlement.</td>
</tr>
<tr>
<td>Access Request Policy</td>
<td>The name of the policy that governs the selected account.</td>
</tr>
<tr>
<td>Accounts</td>
<td>The number of unique accounts in the account groups that are associated with the access request policy.</td>
</tr>
<tr>
<td># Account Groups</td>
<td>The number of unique account groups in the access request policy.</td>
</tr>
<tr>
<td>Account Groups</td>
<td>The names of the account groups that associate the selected account with the policy.</td>
</tr>
</tbody>
</table>

Use these buttons on the details toolbar to manage your access request policies associated with the selected account.

### Table 32: Accounts: Access Request Policies tab toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📦 Add to Policy</td>
<td>Add the selected account to the scope of an access request policy.</td>
</tr>
<tr>
<td>❌ Remove Selected</td>
<td>Remove the selected policy.</td>
</tr>
<tr>
<td>⚫ Refresh</td>
<td>Update the list of access request policies.</td>
</tr>
<tr>
<td>☰ Details</td>
<td>View additional details about the selected policy. For more information, see Viewing policy details on page 226.</td>
</tr>
<tr>
<td>🔍 Search</td>
<td>To locate a specific policy or set of policies in this list, enter the character string to be used to search for a match. For more information, see Search box on page 65.</td>
</tr>
</tbody>
</table>
Account Groups tab

The Account Groups tab displays the account groups that contain the selected account. **NOTE:** The Account Groups tab is only available to a user with Auditor permissions.

Click (or tap) + Add Account Group from the details toolbar to add the selected account to one or more account groups.

Table 33: Accounts: Account Groups tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The account group name.</td>
</tr>
<tr>
<td>Dynamic</td>
<td>A check mark in this column indicates that the group is a dynamic account group.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the account group.</td>
</tr>
</tbody>
</table>

Related Topics

Adding an account to account groups

Check and Change Log tab

The Check and Change Log tab displays the password validation and reset history for the selected account.

**Time Frame:** By default the check and change log entries displayed are for the last 24 hours. Click (or tap) one of the time intervals at the top of the grid to display log entries for a different time frame. If the display does not refresh after selecting a different time interval, click (or tap) the Refresh.

Table 34: Accounts: Check and Change Log tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The display name of the user that triggered the event.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the transaction:</td>
</tr>
<tr>
<td></td>
<td>• Failure</td>
</tr>
<tr>
<td></td>
<td>• Success</td>
</tr>
<tr>
<td></td>
<td>• Queued</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Reason</td>
<td>A system message pertaining to the password validation and reset activity, such as the password matches the asset, or was changed successfully, or does not match the asset.</td>
</tr>
</tbody>
</table>
| Type     | The type of transaction:  
- Check Password  
- Change Password |

**NOTE:** Check and Change Log only displays events that the appliance performs; that is, it only displays Check Password and Change Password transactions. It does not display Set Password transactions. For more information, see Checking, changing, or setting an account password on page 110.

<table>
<thead>
<tr>
<th>Date</th>
<th>The date of the transaction.</th>
</tr>
</thead>
</table>

**NOTE:** The time stamps for transactions are based on the user's local time.

<table>
<thead>
<tr>
<th>Time</th>
<th>The time of the transaction.</th>
</tr>
</thead>
</table>

**NOTE:** The time stamps for transactions are based on the user's local time.

| Duration | The amount of time the transaction took to complete. |

**History tab**

The History tab allows you to view or export the details of each operation that has affected the selected account.

The History tab contains the following information:

- **Items:** Total number of entries in the history log.
- **Search:** For more information, see Search box on page 65.
- **Time Frame:** By default the history details are displayed for the last 24 hours. Click (or tap) one of the time intervals at the top of the grid to display history details for a different time frame. If the display does not refresh after selecting a different time interval, click (or tap) **Refresh**.
Table 35: Accounts: History tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>The date and time of the event.</td>
</tr>
<tr>
<td>User</td>
<td>The display name of the user that triggered the event.</td>
</tr>
<tr>
<td>Source IP</td>
<td>The network DNS name or IP address of the managed system that triggered the event.</td>
</tr>
<tr>
<td>Object Name</td>
<td>The name of the selected account.</td>
</tr>
<tr>
<td>Event</td>
<td>The type of operation made to the selected account:</td>
</tr>
<tr>
<td></td>
<td>• Create</td>
</tr>
<tr>
<td></td>
<td>• Delete</td>
</tr>
<tr>
<td></td>
<td>• Update</td>
</tr>
<tr>
<td></td>
<td>• Add Membership</td>
</tr>
<tr>
<td></td>
<td>• Remove Membership</td>
</tr>
</tbody>
</table>

NOTE: A membership operation indicates a "relationship" change with a related or parent object such as the selected account was added or removed from the membership of an account group.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related Object</td>
<td>The name of the related object.</td>
</tr>
<tr>
<td>Related Object Type</td>
<td>The type of the related object.</td>
</tr>
<tr>
<td>Parent</td>
<td>The name of the object to which the selected account is a child.</td>
</tr>
<tr>
<td>Parent Object Type</td>
<td>The parent object type.</td>
</tr>
</tbody>
</table>

Select an event to display this additional information for some types of events (for example, create and update events).

Table 36: Additional History tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>The property that was updated.</td>
</tr>
<tr>
<td>Old Value</td>
<td>The value of the property before it was updated.</td>
</tr>
<tr>
<td>New Value</td>
<td>The new value of the property.</td>
</tr>
</tbody>
</table>

Exporting data

You can export history, activity log, or access request data to a file.
To export data

1. Click (or tap) **Export** to create a file in a location of your choice of all data in the results grid.
   - When you export historical information from a History tab or License history, Safeguard creates a .csv file.
   - When you export activity log data from the Activity Center and Reports, Safeguard creates a .json file.
   - When you export access request data from the Access Requests view, Safeguard creates a .csv file.
2. Open a .csv file in a spreadsheet program such as Microsoft Excel where you can perform data searches.
3. JSON is a language-independent data format. Code for parsing and generating JSON data is readily available in many programming languages.

Managing accounts

Use the controls and tabbed pages on the Accounts page to perform the following tasks to manage Safeguard accounts:

- Adding an account
- Adding a cloud platform account
- Manually adding a tag to an account
- Adding an account to account groups
- Modifying an account
- Deleting an account
- Importing objects
- Checking, changing, or setting an account password
- Viewing password archive

Adding an account

It is the responsibility of the Asset Administrator to add assets and accounts to Safeguard.

**NOTE:** Safeguard allows you to set up account discovery jobs that run automatically. For more information, see *Account discovery job workflow* on page 491.
To add an account

1. Navigate to Administrative Tools | Accounts.
2. Click (or tap) Add Account from the toolbar.
3. In the Account dialog, supply the following information:

   - **Asset Name**: Browse to select an asset to associate with this account.
     - **NOTE**: While an asset can have multiple accounts, you can only associate an account with one asset.
   - **Name**: Enter the login user name for this account.
     Limit: 100 characters
   - **Description**: (Optional) Enter information about this managed account.
     Limit: 255 characters
   - **Profile**: Browse to select a profile to govern this account.
     - **NOTE**: By default an account inherits the profile of its associated asset, but you can assign it to a different profile for this partition. For more information, see Assigning assets or accounts to a partition profile on page 242.
   - **Enable Password Request**: This check box is selected by default indicating that password release requests are enabled for this account. Clear this option to prevent someone from requesting the password for this account.
     - **NOTE**: By default a user can request the password for any account in the scope of the entitlements in which he or she is an authorized "user".
   - **Enable Session Request**: This check box is selected by default indicating that session access requests are enabled for this account. Clear this option to prevent someone from requesting session access using this account.
     - **NOTE**: By default a user can make an access request for any account in the scope of the entitlements in which he or she is an authorized "user".

   - **NOTE**: When you add an account to Safeguard you are not adding it to the asset, you are simply adding an existing account to the Safeguard database. The new account displays on the Accounts list.

Related Topics

Checking, changing, or setting an account password
Assigning assets or accounts to a partition profile
Account discovery job workflow
Adding a cloud platform account
Adding a cloud platform account

One Identity Safeguard can manage cloud platform accounts such as Facebook, Twitter, Amazon Web Services (AWS), etc.

Before you add cloud platform accounts to Safeguard, you must first add an asset with which to associate the accounts.

- For more information, see Prepare Amazon Web Services platforms on page 436.
- For more information, see Prepare Facebook hosts on page 437.

To add a cloud platform to Safeguard

1. Log into Safeguard and navigate to Administrative Tools.
2. In Assets, click (or tap) + Add Asset from the toolbar.
3. In the General tab,
   - **Name**: Enter an asset name that is meaningful to you, such as "Cloud Account Server" which you can use to manage all cloud platform accounts. (You might add separate assets for Facebook accounts and Twitter accounts.)
   - **Description**: (Optional) Enter a description for the asset.
   - **Partition**: Select the partition you want Safeguard to use to manage the cloud platform account passwords.
   - **Profile**: Select the profile you want Safeguard to use to manage the cloud platform account passwords.
4. In the Management tab,
   - **Product**: Select the appropriate product, such as Amazon Web Services, Facebook, or Twitter.
   - **Version**: For Amazon Web Services, select the version.
   - **Network Address**: For Amazon Web Services, enter the AWS Account Id or Alias.
5. For Amazon Web Services, in the Connection tab, select:
   - **Access Key** to authenticate to the asset using an access key. Enter the following information:
     - **Service Account Name**: Enter the configured IAM service account.
     - **Access Key ID**: Enter the Access Key ID created for the IAM service account.
     - **Secret Key**: Enter the Secret Key created for the IAM service account.
   - **OR**-
   - **None** to not authenticate to the asset and manually manage the asset.
6. For Facebook and Twitter, in the Connection tab, select **Account Password** to authenticate using the current account password.

Once you add the cloud platform asset, you can associate accounts with it.
To add an account to the cloud platform

1. In Assets, select the cloud platform asset and switch to the Accounts tab.
2. Click (or tap) ✪ Add Account from the details toolbar.
3. In the User Name field, enter the cloud platform account username, email address, or phone number. For example, for a Twitter account, enter the "@User" account name.
4. In the Password field, enter the account password for the user name you provided.
5. Click (or tap) Test Connection to verify that Safeguard can communicate with this cloud platform using the credentials that you have provided.
6. Optionally enter a Description.
7. Browse to select a profile to govern this account
8. Ensure the Enable Password Request option is checked and click (or tap) Add Account.

Now you can manually check, change, or set the cloud platform account password; and, Safeguard can automatically manage the password according to the Check and Change settings in the profile governing the account.

To resolve a Twitter requirement for additional verification

Twitter may prompt for additional verification on the next login if suspicious activity is detected (for example, the login originated from a new device or there were too many failed logins from a device). The additional verification may require entry of the email address associated with the Twitter account or entry of a temporary password sent via email. Safeguard detects the Twitter prompt and displays the login requirement in a status message when the password change fails. The Activity Center Event may display Password Change Failed with the following Checking detail: Additional account verification requested: 'RetypeEmail'.

To resolve the request for verification so that Twitter trusts the Safeguard appliance:

1. Open a browser on the same network as the Safeguard appliance.
2. Log into Twitter as the account.
3. Enter the additional verification requested.

To checkout the cloud platform account

1. Add a cloud platform Account Group and add the accounts to the group.
2. Add an entitlement for the cloud platform accounts.
3. Add users to the entitlements.
4. Add a password release policy to the entitlement.
5. Add the cloud platform Account Group to the scope of the policy.
Manually adding a tag to an account

Asset Administrators can manually add and remove tags to an account using the Tags pane, which is located at the bottom of the General tab when an account is selected on the Accounts view.

**To manually add a tag to an account**

1. Navigate to Administrative Tools | Accounts.
2. In Accounts, select an account from the object list (left-pane).
3. Open the General tab and scroll down to view the Tags pane.
4. Click (or tap) next to the Tags title.
5. Place your cursor in the edit box and enter the tag to be assigned to the selected account.
   - As you type, existing tags that start with the letters entered will appear allowing you to select a tag from the list.
   - To add additional tags, press Enter before entering the next tag.
6. Click (or tap) OK.
   - If you do not see the new tag, click the Refresh toolbar button.
7. To remove a manually assigned tag, click (or tap) next to the Tags title and click the X inside the tag box to be removed.

   **NOTE:** You cannot manually remove dynamically assigned tags which are indicated by a lightening bolt icon. You must modify the rule associated with the dynamic tag if you want to remove it. For more information, see Modifying an asset or asset account tag on page 284.

Adding an account to account groups

From the Accounts view you can add an account to one or more account groups.

**To add an account to account groups**

1. Navigate to Administrative Tools | Accounts.
2. In Accounts, select an account from the object list and open the Account Groups tab.
3. Click (or tap) Add Account Group from the details toolbar.
4. Select one or more account groups from the list in the Account Groups dialog and click (or tap) OK.
   - **NOTE:** You can also double-click (or double-tap) an account group name to add it.
If you do not see the account group you are looking for, depending on your Administrator permissions, you can create it in the Account Groups selection dialog. (You must have Security Policy Administrator permissions to create account groups.)

To create a new account group from the Account Groups selection dialog

1. Click (or tap) + Create New.
   For more information about creating account groups, see Adding an account group.
2. Create additional account groups, as required.
3. Click (or tap) OK in the Account Groups selection dialog to add the new account to the selected account group.

Related Topics
Adding accounts to an account group

Modifying an account

To modify an account’s information

1. Navigate to Administrative Tools | Accounts.
2. In Accounts, select an account from the object list.
3. Double-click (or double-tap) the General information box or click (or tap) the Edit icon.
   - NOTE: You can also double-click (or double-tap) an account name to open the General settings edit window.
   - NOTE: Once you add an account, you cannot modify an account’s associated asset or its name.
4. To view the selected account’s password validation and reset history, switch to the Check and Change Log tab.
5. To view or export the details of each operation that has affected the selected account, switch to the History tab.
6. To reset an account’s password, right-click (or press and hold) the account name and navigate to Change Password or Set Password from the context menu. For more information, see Checking, changing, or setting an account password on page 110.

Deleting an account

- NOTE: When you delete an account, Safeguard does not delete it from its associated asset, it simply removes it from Safeguard.
To delete an account

1. Navigate to Administrative Tools | Accounts.
2. In Accounts, select an account from the object list
3. Click (or tap) Delete Selected.

   **NOTE:** If you delete a service account, Safeguard changes the asset’s authentication type to None which disables automatic password management for all accounts that are associated with this asset. All assets must have a service account in order to check and change the passwords for the accounts associated with it. For more information, see About service accounts on page 140.

4. Confirm your request.

Importing objects

Safeguard allows you to import a .csv file containing a set of accounts, assets, or users.

To import a set of objects

1. Click (or tap) Import from the toolbar.
2. In the Import dialog, Browse to select an existing .csv file containing a list of objects to import.

   **NOTE:** For assistance in creating an import file, click (or tap) CSV Template Assistant. For more information, see Creating an import file on page 109.

3. When importing assets, the Discover SSH Host Keys option is selected by default indicating that Safeguard will retrieve the required SSH host key for the assets specified in the CSV file.
4. Click (or tap) OK.

   Safeguard imports the objects into its database.
NOTE: Safeguard does not add an object if any column contains invalid data in the .csv file with the follow exceptions:

- **Assets PlatformDisplayName** property.
  a. If Safeguard does not find an exact match, it looks for a partial match. If it finds a partial match it supplies the `<platform> Other` platform, such as "Other Linux".
  b. If it does not find a partial match, it supplies the Other platform type.

- **Users TimeZoneId** property.
  a. If Safeguard does not find a valid TimeZoneId property (that is, does not find an exact match or no timezone was provided), it uses the local workstation's current timezone.

  NOTE: Do not enter numbers or abbreviations for the TimeZoneId.

- **Users Password** property.
  a. Safeguard adds a user without validating the password you provide.

5. Navigate to the **Tasks** pane in the **Toolbox** for details about the import process and invalid data messages. For more information, see Viewing task status on page 93.

**Creating an import file**

When importing objects, such as accounts, assets, or users, Safeguard expects the import file to be a Comma Separated Values (CSV) file.

A CSV file is a text file used to store database entries where each line is a unique record and each record consists of fields of data separated by commas. The easiest way to create a CSV file is by using a spreadsheet program such as Microsoft Excel; however, you can use any text editor, such as Notepad, to create a comma-delineated file, as long as you save the file with a .csv file type extension.

The order of the columns is not important, but the title of the column must match the property name.

**IMPORTANT:** You must not add any trailing spaces in the properties you define in the CSV file.

**To create a customized .csv file template**

1. In the **Import** dialog, click (or tap) **CSV Template Assistant**.
2. Select specific template properties from the template properties table, or select the "select all" check box in the heading.
NOTE: Safeguard preselects the required properties; you can select any additional properties you desire.

3. Select **Download Template** to save a copy of the template properties table to a location of your choice.

   TIP: Click (or tap) the View icon in the Values column to display a list of allowable values. Click (or tap) Copy to copy the selected value to your copy buffer which can then be pasted into your CSV file.

   NOTE: Click (or tap) **Export Full Table**, in upper the right corner above the properties table, to save a copy of the properties table.

4. Locate the downloaded template and add your specific information to the template.

   TIP: Users **AdminRoles** property: The value for the Authorizer Administrator is "GlobalAdmin".

   NOTE: Safeguard does not add an object if any column contains invalid data in the .csv file with the follow exceptions:
   - Assets **PlatformDisplayName** property.
     a. If Safeguard does not find an exact match, it looks for a partial match. If it finds a partial match it supplies the `<platform>` **Other** platform, such as "Other Linux".
     b. If it does not find a partial match, it supplies the **Other** platform type.
   - Users **TimeZoneId** property.
     a. If Safeguard does not find a valid TimeZoneId property (that is, does not find an exact match or no timezone was provided), it uses the local workstation's current timezone.

      NOTE: Do not enter numbers or abbreviations for **TimeZoneId**.
   - Users **Password** property.
     a. Safeguard adds a user without validating the password you provide.

5. Use the customized .csv file to import the objects.

### Checking, changing, or setting an account password

The Asset Administrator can manually check, change, or set an account password from the **Account Security** menu.
To manually check, change, or set an account password

1. Navigate to Administrative Tools | Accounts.
2. In Accounts, select an account from the object list.
3. Click (or tap) Account Security from the toolbar.
   
   **NOTE:** You can also right-click (or press and hold) the account name to open the context menu.

Select one of these options:

- **Check Password** to verify the account password is in sync with the Safeguard database. If the password verification fails, you can change it.
- **Change Password** to reset and synchronize the account password with the Safeguard database.
- **Set Password** to set the account password in the Safeguard database.
   
   **NOTE:** The "Set" option does not change the account password on the asset.

**NOTE:** See the progress and results of the "Check" and "Change" options in the Toolbox | Tasks pane. For more information, see Viewing task status on page 93.

4. The **Set Password** option provides two options:

   a. **Generate Password** - select this option to have Safeguard generate a new random password, that complies with the password rule that is set in the account's profile.
      
      - Click (or tap) Generate Password to display the Generate Password dialog.
      - Click (or tap) Show Password to reveal the new password.
      - Click (or tap) Copy to put it into your copy buffer.
      - Log into your device, using the old password, and change it to the password in your copy buffer.
      - Click (or tap) OK to change the password in the Safeguard database or click (or tap) Cancel to close the dialog without changing the current password in Safeguard.

   b. **Manual Password** - select this option to manually set the account password in the Safeguard database.
      
      - Click (or tap) Manual Password to display the Set Password dialog.
      - In the Set Password dialog, enter the password and click (or tap) OK.
      - Clicking OK updates the Safeguard database.
      - Set the account password on the physical device to synchronize it with the Safeguard database.
Viewing password archive

The Asset Administrator and Auditor can access a previous password for an account for a specific date.

NOTE: The Password Archive dialog only displays previously assigned passwords for the selected asset based on the date specified. This dialog does not display the current password for the asset.

To access an account's previous password

1. Navigate to Administrative Tools | Accounts.
2. In Accounts, right-click (or press and hold) an account name and choose Password Archive.
   Or, click (or tap) Password Archive from the toolbar.
3. In the Password Archive dialog, select a date.
   TIP: If you select today's date (or a previous date) and no entries are returned, this indicates that the asset is still using the current password.
4. In the View column, click (or tap) to display the password that was assigned to the asset at that given date and time.
5. In the details dialog, click (or tap) Copy to copy the password to your copy buffer, or click (or tap) OK to close the dialog.

NOTE: You view an account's password validation and reset history on the Check and Change Log tab.
Account Groups

A Safeguard account group is a set of accounts which you can add to the scope of an access request policy. For more information, see Creating an access request policy on page 214.

The Auditor and the Security Policy Administrator have permission to access Account Groups.

The Account Groups view displays the following information about the selected account group.

Table 37: Account Groups: Tabs

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td>Displays general information about the selected account group.</td>
</tr>
<tr>
<td>Accounts tab</td>
<td>Displays the accounts associated with the selected account group.</td>
</tr>
<tr>
<td>Access Request Policies tab</td>
<td>Displays the entitlements and access request policies associated with the selected account group.</td>
</tr>
<tr>
<td>History tab</td>
<td>Displays the details of each operation that has affected the selected account group.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage account groups.

Table 38: Account Groups: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Account Group</td>
</tr>
<tr>
<td>Add</td>
<td>Dynamic Account Group</td>
</tr>
<tr>
<td>Delete Selected</td>
<td>Remove the selected account group from Safeguard. For more information, see Deleting an account group on page 125.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of account groups.</td>
</tr>
</tbody>
</table>
General tab

The General tab lists information about the selected Account Group.

Large tiles at the top of the tab display the number of Accounts and Access Request Policies associated with the selected account group. Clicking a tile heading opens the corresponding tab.

Table 39: Account Groups General tab: General properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The selected account group's name.</td>
</tr>
</tbody>
</table>

Description: Information about the selected account group.

Asset Account Rules: For dynamic account groups, a summary of the asset account rules defined.

Directory Account Rules: For dynamic account groups, a summary of the directory account rules defined.

Related Topics

Modifying an account group

Accounts tab

The Accounts tab displays the accounts associated with the selected account group.

Click (or tap) + Add Account from the details toolbar to add one or more accounts to the selected account group.

Search: For more information, see Search box on page 65.

Table 40: Account Groups: Accounts tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the account belonging to the selected account group.</td>
</tr>
<tr>
<td>Parent</td>
<td>The asset or directory to which the account belongs.</td>
</tr>
<tr>
<td>Domain</td>
<td>For directory accounts, the name of the domain the account is associated with.</td>
</tr>
<tr>
<td>Service Account</td>
<td>A check in this column indicates that the account is a service account.</td>
</tr>
</tbody>
</table>
### Access Request Policies tab

The **Access Request Policies** tab displays the entitlements and policies, including password release and session request policies, associated with the selected account group.

Click (or tap) **+ Add to Policy** from the details toolbar to add the selected account group to the scope of one or more access request policies.

#### Table 41: Account Groups: Access Request Policies tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entitlement</td>
<td>The name of the access request policy's entitlement.</td>
</tr>
<tr>
<td>Access Request</td>
<td>The name of the policy that governs the accounts in the selected account group.</td>
</tr>
<tr>
<td>Policy</td>
<td></td>
</tr>
<tr>
<td>Account Groups</td>
<td>The number of unique account groups in the access request policy.</td>
</tr>
<tr>
<td>Accounts</td>
<td>The number of unique accounts in the account groups that are associated with the access request policy.</td>
</tr>
</tbody>
</table>

Use these buttons on the details toolbar to manage your access request policies associated with the selected account group.

#### Table 42: Account Groups: Access Request Policies tab toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Add to Policy</td>
<td>Add the selected account group to the scope of an access request</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Remove Selected</td>
<td>Remove the selected account group from the scope of the selected access policy.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of access request policies.</td>
</tr>
<tr>
<td>Details</td>
<td>View additional details about the selected policy. For more information, see Viewing policy details on page 226.</td>
</tr>
<tr>
<td>Search</td>
<td>To locate a specific policy or set of policies in this list, enter the character string to be used to search for a match. For more information, see Search box on page 65.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Adding accounts to an access request policy
- Modifying an account group

**History tab**

The **History** tab allows you to view or export the details of each operation that has affected the selected account group.

The **History** tab contains the following information:

- **Items**: Total number of entries in the history log.
- **Search**: For more information, see Search box on page 65.
- **Time Frame**: By default the history details are displayed for the last 24 hours. Click (or tap) one of the time intervals at the top of the grid to display history details for a different time frame. If the display does not refresh after selecting a different time interval, click (or tap) **Refresh**.

**Table 43: Account Groups: History tab properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>The date and time of the event.</td>
</tr>
<tr>
<td>User</td>
<td>The display name of the user that triggered the event.</td>
</tr>
<tr>
<td>Source IP</td>
<td>The network DNS name or IP address of the managed system that triggered the event.</td>
</tr>
<tr>
<td>Object Name</td>
<td>The name of the selected account group.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event</td>
<td>The type of operation made to the selected account group:</td>
</tr>
<tr>
<td></td>
<td>• Create</td>
</tr>
<tr>
<td></td>
<td>• Delete</td>
</tr>
<tr>
<td></td>
<td>• Update</td>
</tr>
<tr>
<td></td>
<td>• Add Membership</td>
</tr>
<tr>
<td></td>
<td>• Remove Membership</td>
</tr>
</tbody>
</table>

**NOTE:** A membership operation indicates a "relationship" change with a related or parent object such as the selected account group was added or removed from the membership of a policy, or an account was added or removed from the membership of the selected account group.

<table>
<thead>
<tr>
<th>Related Object</th>
<th>The name of the related object.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related Object Type</td>
<td>The type of the related object.</td>
</tr>
<tr>
<td>Parent</td>
<td>The name of the object to which the selected account group is a child.</td>
</tr>
<tr>
<td>Parent Object Type</td>
<td>The parent object type.</td>
</tr>
</tbody>
</table>

Select an event to display this additional information for some types of events (for example, create and update events).

**Table 44: Additional History tab properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>The property that was updated.</td>
</tr>
<tr>
<td>Old Value</td>
<td>The value of the property before it was updated.</td>
</tr>
<tr>
<td>New Value</td>
<td>The new value of the property.</td>
</tr>
</tbody>
</table>

**Managing account groups**

Use the controls and tabbed pages in the Account Groups view to perform the following tasks to manage Safeguard account groups:

- Adding an account group
- Adding a dynamic account group
- Adding accounts to an account group
- Adding accounts to an access request policy
- Modifying an account group
- Deleting an account group

**Adding an account group**

It is the responsibility of the Security Policy Administrator to add account groups to Safeguard.

**To add an account group**

1. Navigate to **Administrative Tools | Account Groups**.
2. Click (or tap) **+ Add | Add Account Group** from the toolbar.
3. In the **Account Group** dialog, enter the following information:
   - **Name**: Enter a unique name for the account group.  
     Limit: 50 characters
   - **Description**: (Optional) Enter information about this account group.  
     Limit: 255 characters

**Adding a dynamic account group**

It is the responsibility of the Security Policy Administrator to add account groups to Safeguard.

**To add a dynamic account group**

1. Navigate to **Administrative Tools | Account Groups**.
2. Click (or tap) **+ Add | Add Dynamic Account Group** from the toolbar.
3. In the **Dynamic Account Group** dialog, provide information in each of the tabs:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td>Where you add general information about the dynamic account group.</td>
</tr>
<tr>
<td>Asset Account Rules tab</td>
<td>Where you define the rules to be used to identify the accounts to be included in a dynamic account group.</td>
</tr>
<tr>
<td>Directory Account Rules tab</td>
<td>Where you define the rules to be used to identify the directory accounts to be included in a dynamic account group.</td>
</tr>
<tr>
<td>Summary tab</td>
<td>Where you review the rules defined for adding accounts to a dynamic account group, and where you save your selections, and add the dynamic account group.</td>
</tr>
</tbody>
</table>
Related Topics
When does the rules engine run for dynamic grouping and tagging

General tab

On the General tab of the Dynamic Account Group dialog, supply general information about the dynamic account group.

Table 45: Dynamic Account Group: General tab

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the dynamic account group.</td>
</tr>
<tr>
<td></td>
<td>Limit: 50 characters</td>
</tr>
<tr>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>Description</td>
<td>Enter information about this dynamic account group.</td>
</tr>
<tr>
<td></td>
<td>Limit: 255 characters</td>
</tr>
</tbody>
</table>

Asset Account Rules tab

Use the controls on the Asset Account Rules tab of the Dynamic Account Group dialog to define the accounts that are to be included in the dynamic account group.

Table 46: Dynamic Account Group: Asset Account Rules tab

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don't include an asset account rule for this group</td>
<td>Select this check box if you do not want to include an asset account rule for this dynamic account group. Selecting this check box disables the rule editor controls. Proceed to the next tab in the dialog to define the conditions for a directory account rule.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> You can create a dynamic account group without any rules; however, no accounts will be added to this dynamic account group until you have added a rule.</td>
</tr>
<tr>
<td>AND</td>
<td>OR</td>
</tr>
<tr>
<td></td>
<td>Click (or tap) <strong>OR</strong> to &quot;or&quot; multiple search criteria together; where at least one of the criteria must be met in order to be included.</td>
</tr>
<tr>
<td>Attribute</td>
<td>In the first query clause box, select the attribute to be searched.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Valid attributes</td>
<td>include:</td>
</tr>
<tr>
<td>Name (Default)</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Platform</td>
<td></td>
</tr>
<tr>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Tag</td>
<td></td>
</tr>
<tr>
<td>Service Account</td>
<td></td>
</tr>
<tr>
<td>Partition Name</td>
<td></td>
</tr>
<tr>
<td>Asset Tag</td>
<td></td>
</tr>
<tr>
<td>Operator</td>
<td>In the middle clause query box, select the operator to be used in the search. The operators available depend upon the data type of the attribute selected. For string attributes, the operators may include:</td>
</tr>
<tr>
<td>Contains (Default)</td>
<td></td>
</tr>
<tr>
<td>Does not contain</td>
<td></td>
</tr>
<tr>
<td>Starts with</td>
<td></td>
</tr>
<tr>
<td>Ends with</td>
<td></td>
</tr>
<tr>
<td>Equals</td>
<td></td>
</tr>
<tr>
<td>Not equal</td>
<td></td>
</tr>
<tr>
<td>For boolean attributes, the operators may include:</td>
<td></td>
</tr>
<tr>
<td>Is True</td>
<td></td>
</tr>
<tr>
<td>Is False</td>
<td></td>
</tr>
<tr>
<td>Search string</td>
<td>In the last clause query box, enter the search string or value to be used to find a match.</td>
</tr>
<tr>
<td>Click (or tap) +</td>
<td>to the left of a search clause to add an additional clause to the search criteria.</td>
</tr>
<tr>
<td>Click (or tap) −</td>
<td>to remove the search clause from the search criteria.</td>
</tr>
<tr>
<td>Add Grouping</td>
<td>Click (or tap) the  <strong>Add Grouping</strong> button to add an additional set of conditions to be met.</td>
</tr>
<tr>
<td>Remove</td>
<td>A new grouping is added under the last query clause in a group and appears in a bordered pane showing that it is subordinate to the higher level query conditions. Click (or tap) the <strong>Remove</strong> button to remove a grouping from the</td>
</tr>
</tbody>
</table>
Directory Account Rules tab

Use the controls on the Directory Account Rules tab of the Dynamic Account Group dialog to define the directory accounts that are to be included in the dynamic account group.

Table 47: Dynamic Account Group: Directory Account Rules tab

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don't include a directory account rule for this group</td>
<td>Select this check box if you do not want to include a directory account rule for this dynamic account group. Selecting this check box disables the rule editor controls. Proceed to the next tab to review the conditions defined for this dynamic account group.</td>
</tr>
<tr>
<td>AND</td>
<td>OR</td>
</tr>
</tbody>
</table>
| Attribute                                     | In the first query clause box, select the attribute to be included. Valid attributes include:  
  - Name (Default)  
  - Description  
  - Platform  
  - Disabled  
  - Tag  
  - Service Account  
  - Domain Name  
  - NETBIOS Name  
  - Distinguished Name  
  - SID
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator</td>
<td>In the middle clause query box, select the operator to be used in the search. The operators available depend upon the data type of the attribute selected. For string attributes, the operators may include:</td>
</tr>
</tbody>
</table>
|                | • Contains (Default)  
|                | • Does not contain  
|                | • Starts with  
|                | • Ends with  
|                | • Equals  
|                | • Not equal  
| Search string  | In the last clause query box, enter the search string or value to be used to find a match.                                                                                                                   |
| + / —          | Click (or tap) + to the left of a search clause to add an additional clause to the search criteria. Click (or tap) — to remove the search clause from the search criteria.                                             |
| Add Grouping   | Click (or tap) the + Add Grouping button to add an additional set of conditions to be met. A new grouping is added under the last query clause in a group and appears in a bordered pane showing that it is subordinate to the higher level query conditions.|
| Remove         | Click (or tap) the Remove button to remove a grouping from the search criteria.                                                                                                                              |
| Preview        | Click (or tap) Preview to run the query in order to review the results of the query before adding the dynamic group.                                                                                             |

**Summary tab**

On the Summary tab of the Dynamic Account Group dialog, review the rules defined for adding accounts to the dynamic account group, save your selections, and add the dynamic account group to Safeguard.
1. Review the rules defined for this dynamic account group.
   Open the Account Rules tab to review the asset account rules. Open the Directory Rules tab to review the directory account rules.

2. Return to the Asset Account Rules tab or Directory Account Rules tab to modify any of the rules if necessary.

3. Click (or tap) Add Account Group to create the dynamic account group.

## Adding accounts to an account group

From the Account Groups view, you can add one or more accounts to an account group.

### To add accounts to an account group

1. Navigate to Administrative Tools | Account Groups.
2. In Account Groups, select an account group from the object list and open the Accounts tab.
3. Click (or tap) + Add Account from the details toolbar.
4. Select one or more accounts from the list in the Accounts selection dialog and click (or tap) OK.

   | NOTE: You can also double-click (or double-tap) an account name to add it.

If you do not see the account you are looking for, depending on your Administrator permissions, you can create it in the Accounts selection dialog. (You must have Asset Administrator permissions to create accounts.)

### To create a new account from the Accounts selection dialog

1. Click (or tap) + Create New.
   For more information about creating accounts, see Adding an account.
2. Create additional accounts, as required.
3. Click (or tap) OK in the Accounts selection dialog to add the accounts to the selected account group.

## Related Topics

Adding an account to account groups
Adding accounts to an access request policy

To add accounts to an access request policy

1. Navigate to Administrative Tools | Account Groups.
2. In Account Groups, select an account group from the object list and open the Access Request Policies tab.
3. Click (or tap) Add to Policy from the details toolbar.
4. Select a policy from the list in the Access Request Policy selection dialog and click (or tap) OK.
   
   NOTE: You can also double-click (or double-tap) the access request policy to which the account group is to be added.

Modifying an account group

To modify an account group’s information

1. Navigate to Administrative Tools | Account Groups.
2. In Account Groups, select an account group from the object list.
3. Select the view of the account group's information you want to modify (General, Accounts, or Access Request Policies).
   
   For example:
   
   - To change an account group’s name or description, double-click (or double-tap) the General information box in the General tab or click (or tap) the Edit icon.
     
     NOTE: You can also double-click (or double-tap) an account group name to open the General settings edit window.
   
   - To add (or remove) accounts to the selected account group, switch to the Accounts tab.
     
     NOTE: You can multi-select members to add or remove more than one from an account group.
   
   - To add (or remove) the selected account group to the scope of a policy, switch to the Access Request Policies tab.

4. To view or export the details of each operation that has affected the selected account group, switch to the History tab.
Deleting an account group

**NOTE:** When you delete an account group, Safeguard does not delete the associated accounts.

To delete an account group

1. Navigate to **Administrative Tools | Account Groups**.
2. In **Account Groups**, select an account group.
3. Click (or tap) **Delete Selected**.
4. Confirm your request.
Assets

A Safeguard asset is a computer, server, network device, or application managed by a Safeguard appliance.

The Auditor and the Asset Administrator have permission to access Assets.

**NOTE:** Before adding systems to Safeguard, you must ensure they are properly configured. For more information, see Preparing systems for management on page 434.

**NOTE:** For information about configuring asset discovery in Safeguard, see Asset discovery job workflow.

The Assets view displays the following information about the selected system,

**Table 48: Assets: Tabs**

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td>Displays general, management and connection settings for the selected asset.</td>
</tr>
<tr>
<td>Accounts tab</td>
<td>Displays the accounts associated with this asset.</td>
</tr>
<tr>
<td>Account Dependencies tab</td>
<td>Displays the directory accounts that the selected Windows server depends on to perform services and tasks.</td>
</tr>
<tr>
<td>Access Request Policies tab</td>
<td>Displays the entitlements and access request policies associated with the selected asset.</td>
</tr>
<tr>
<td>Asset Groups tab</td>
<td>Displays the asset groups that contain the selected asset.</td>
</tr>
<tr>
<td>History tab</td>
<td>Displays the details of each operation that has affected the selected asset.</td>
</tr>
</tbody>
</table>
Use these toolbar buttons to manage assets.

Table 49: Assets: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Add</td>
<td>Add Asset</td>
</tr>
<tr>
<td>Delete Selected</td>
<td>Delete the selected asset. For more information, see <a href="#">Deleting an asset</a> on page 155.</td>
</tr>
<tr>
<td>IMPORTANT: When you delete an asset, you also permanently delete all the Safeguard accounts associated with the asset.</td>
<td></td>
</tr>
<tr>
<td>Refresh</td>
<td>Refresh</td>
</tr>
<tr>
<td>Import Assets</td>
<td>Add assets to Safeguard. For more information, see <a href="#">Importing objects</a> on page 388.</td>
</tr>
<tr>
<td>Discovery</td>
<td>Add or manage asset discovery jobs. For more information, see <a href="#">Discovery</a> on page 156.</td>
</tr>
<tr>
<td>Download SSH Key</td>
<td>Add the SSH key to the selected asset. For more information, see <a href="#">Downloading a public SSH key</a> on page 166.</td>
</tr>
<tr>
<td>Access Request</td>
<td>Allows you to enable or disable access request services for the selected asset. Menu options include:</td>
</tr>
<tr>
<td>⚖ Show Ignored</td>
<td>Display the hidden assets.</td>
</tr>
<tr>
<td>⚖ Hide Ignored</td>
<td>Hide assets marked as &quot;Ignore&quot;.</td>
</tr>
</tbody>
</table>

Use these context menu options to manage assets.

Table 50: Assets context menu options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover SSH Host Key</td>
<td>Retrieves the latest SSH host key for the selected asset. The Discover SSH Host Key dialog also tells you when the SSH host key is up to date.</td>
</tr>
<tr>
<td>IMPORTANT: This option only applies to assets that exchange SSH host keys, such as Unix-based assets and Linux-based assets.</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Discover Accounts</strong></td>
<td>Runs a discovery job to find accounts on the selected asset. From the tasks pane, select <strong>Show Accounts</strong> to open the Partitions view to view the accounts found.</td>
</tr>
<tr>
<td><strong>Download SSH Key</strong></td>
<td>Add the SSH key to the selected asset.</td>
</tr>
<tr>
<td><strong>Manage - Ignore</strong></td>
<td>Select <a href="#">Manage</a> to have Safeguard manage an &quot;ignored&quot; asset. This option is only available for assets that have been ignored.</td>
</tr>
<tr>
<td></td>
<td>Select <a href="#">Ignore</a> to prevent Safeguard from managing the selected asset.</td>
</tr>
<tr>
<td><strong>Check Connection</strong></td>
<td>Select to verify that Safeguard can log into the asset using the current service account credentials. For more information, see <a href="#">Checking an asset's connectivity</a> on page 151.</td>
</tr>
<tr>
<td><strong>Access Requests</strong></td>
<td>Select <strong>Enable Session Request</strong> to allow session requests for the selected asset.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Disable Session Request</strong> to disallow session requests for the selected asset.</td>
</tr>
<tr>
<td><strong>Delete Selected</strong></td>
<td>Remove the selected asset from Safeguard.</td>
</tr>
</tbody>
</table>

### General tab

The **General** tab lists information about the selected asset.

Large tiles at the top of the tab display the number of **Accounts**, **Account Dependencies** (when applicable), **Access Request Policies** and **Asset Groups** associated with the selected asset. Clicking a tile heading opens the corresponding tab.

**NOTE:** If the SSH host key is not discovered on the asset (either via a discovery or import), certain tasks will not be available for accounts associated with the asset, such as Check System, Check Password, Change Password.

**NOTE:** When you ignore an asset, Safeguard disables it and removes all associated accounts. If you choose to **Manage** the asset later, Safeguard re-enables all the associated accounts.

**IMPORTANT:** When you delete an asset, you also permanently delete all the Safeguard accounts associated with the asset.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The asset name.</td>
</tr>
<tr>
<td>Partition</td>
<td>The name of the partition where the selected asset resides.</td>
</tr>
<tr>
<td>Profile</td>
<td>The name of the profile that manages the asset’s accounts.</td>
</tr>
<tr>
<td></td>
<td>NOTE: All assets must be governed by a profile. All new assets are</td>
</tr>
<tr>
<td></td>
<td>automatically governed by the default profile unless otherwise specified.</td>
</tr>
<tr>
<td>License Type</td>
<td>Indicates your license model.</td>
</tr>
<tr>
<td>Last Successful</td>
<td>The date and time of the last successful account discovery job.</td>
</tr>
<tr>
<td>Account Discovery</td>
<td></td>
</tr>
<tr>
<td>Next Account</td>
<td>The date and time of the next automated account discovery job as set in the</td>
</tr>
<tr>
<td>Discovery</td>
<td>Account Discovery schedule of the partition profile.</td>
</tr>
<tr>
<td></td>
<td>(For more information, see Creating a partition profile on page 239.)</td>
</tr>
<tr>
<td>Directory</td>
<td>The name of the directory where the asset was discovered.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This property is only displayed for assets discovered from a directory.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The name of the domain where the asset was discovered.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This property is only displayed for assets discovered from a directory.</td>
</tr>
<tr>
<td>NetBios name</td>
<td>The NetBios name of the asset that was discovered.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This property is only displayed for assets discovered from a directory.</td>
</tr>
<tr>
<td>Distinguished Name</td>
<td>The distinguished name of the asset that was discovered.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This property is only displayed for assets discovered from a directory.</td>
</tr>
</tbody>
</table>

Table 52: Assets General tab: Management properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>The platform of the selected managed system.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Version</td>
<td>The operating system version.</td>
</tr>
<tr>
<td>Architecture</td>
<td>The operating system architecture.</td>
</tr>
<tr>
<td>Network Address</td>
<td>The network DNS name or IP address of the managed system.</td>
</tr>
<tr>
<td>Enable Session Request</td>
<td>True or False, indicating whether session access requests are enabled for the asset.</td>
</tr>
<tr>
<td>RDP Session Port</td>
<td>The access port on the target server used for RDP session access requests.</td>
</tr>
<tr>
<td>SSH Session Port</td>
<td>The access port on the target server used for SSH session access requests.</td>
</tr>
<tr>
<td>Managed Network</td>
<td>The managed network that is assigned for work load balancing. For more information, see Managed Networks on page 314.</td>
</tr>
</tbody>
</table>

**Table 53: Assets General properties: Connection properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Type</td>
<td>How the console connects with the managed system. For more information, see Connection tab on page 139.</td>
</tr>
<tr>
<td>Service Account Name</td>
<td>The account used by Safeguard to securely manage accounts and passwords on the asset.</td>
</tr>
<tr>
<td>Connection Timeout</td>
<td>The session timeout period.</td>
</tr>
<tr>
<td>Privilege Elevation Command</td>
<td>Displays the elevation command (such as sudo) if it is populated on the Connection tab.</td>
</tr>
<tr>
<td>Port</td>
<td>The port used by SSH to log into the managed system.</td>
</tr>
<tr>
<td>SSH Host Key Fingerprint</td>
<td>The fingerprint of the SSH key that Safeguard uses to authenticate to the asset.</td>
</tr>
</tbody>
</table>

**Tags**: Tag assignments for the selected asset.

The tiles listed under in the Tags pane display both the dynamic tags assigned to the asset through tagging rules and static tags that were added manually. In addition to viewing tag assignments, Asset Administrators can add and remove statically assigned tags using this pane.

**Description**: Information about the selected asset.

**Related Topics**

Assigning an asset to a partition
Assigning a profile to an asset
Modifying an asset
Accounts tab

An asset's Accounts tab displays the accounts associated with this asset. Click (or tap) + Add Account from the details toolbar to associate an account with the selected asset.

Table 54: Assets: Accounts tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of an account associated with the selected asset.</td>
</tr>
<tr>
<td></td>
<td>NOTE: While you can associate an account with only one asset, you can log into an asset with more than one account.</td>
</tr>
<tr>
<td>Profile</td>
<td>The name of the profile that manages the account.</td>
</tr>
<tr>
<td>Service Account</td>
<td>A check in this column indicates that the account is a service account.</td>
</tr>
<tr>
<td>Password Request</td>
<td>A check in this column indicates that password release requests are enabled for the account.</td>
</tr>
<tr>
<td></td>
<td>NOTE: Click (or tap) Access Requests from the details toolbar to enable or disable a user's ability to request access to the selected account.</td>
</tr>
<tr>
<td>Session Request</td>
<td>A check in this column indicates that session access requests are enabled for the account.</td>
</tr>
<tr>
<td></td>
<td>NOTE: Click (or tap) Access Requests from the details toolbar to enable or disable a user's ability to request access to the selected account.</td>
</tr>
<tr>
<td>Needs a Password</td>
<td>Displays⚠️ if a password is not set for the account. For more information, see Checking, changing, or setting an account password on page 110.</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive information entered when the account was added.</td>
</tr>
</tbody>
</table>

Use these buttons on the details toolbar to manage your asset accounts.

Table 55: Assets: Accounts tab toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Add Account</td>
<td>Add accounts to the selected asset. For more information, see Adding an account to an asset on page 153.</td>
</tr>
<tr>
<td>Delete Selected</td>
<td>Remove the selected account from the asset.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Refresh</strong></td>
<td>Update the list of asset accounts.</td>
</tr>
<tr>
<td><strong>Account Security</strong></td>
<td>Menu options include: <strong>Check Password</strong>, <strong>Change Password</strong>, and <strong>Set Password</strong>. For more information, see <strong>Checking, changing, or setting an account password</strong> on page 110.</td>
</tr>
<tr>
<td><strong>Password Archive</strong></td>
<td>Display the password history for the selected asset account. For more information, see <strong>Viewing password archive</strong> on page 112.</td>
</tr>
<tr>
<td><strong>Access Requests</strong></td>
<td>Select an option to enable or disable access request services for the selected account. Menu options include: Enable Password Request, Disable Password Request, Enable Session Request, Disable Session Request</td>
</tr>
<tr>
<td><strong>Set Profile</strong></td>
<td>Select a profile to manage the selected asset account.</td>
</tr>
<tr>
<td><strong>Search</strong></td>
<td>To locate a specific asset account or set of accounts in this list, enter the character string to be used to search for a match. For more information, see <strong>Search box</strong> on page 65.</td>
</tr>
</tbody>
</table>

**Account Dependencies tab**

The **Account Dependencies** tab displays the directory accounts that the selected Windows server depends on to perform services and tasks.

*NOTE:* **The Account Dependencies** tab is only applicable for a Windows platform when one or more directories have been added to Safeguard.

Click (or tap) **Add Account** from the details toolbar to associate account dependencies with the selected asset.
### Table 56: Assets: Account Dependencies tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of a directory account.</td>
</tr>
<tr>
<td>Directory</td>
<td>The directory in which the account resides.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The forest root domain name for the directory.</td>
</tr>
<tr>
<td>Distinguished Name</td>
<td>The distinguished name for a directory account.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the dependent account.</td>
</tr>
</tbody>
</table>

### Related Topics

Adding account dependencies

### Access Request Policies tab

The **Access Request Policies** tab displays the entitlements and access request policies associated with the selected asset.

### Table 57: Assets: Access Request Policies tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entitlement</td>
<td>The name of the access request policy's entitlement.</td>
</tr>
<tr>
<td>Access Request Policy</td>
<td>The name of the policy that governs the selected asset.</td>
</tr>
<tr>
<td>Assets</td>
<td>The number of unique assets that are associated with the access request policy.</td>
</tr>
<tr>
<td># Asset Groups</td>
<td>The number of unique asset groups in the access request policy.</td>
</tr>
<tr>
<td>Asset Groups</td>
<td>The names of the asset groups that associate the selected asset with the policy.</td>
</tr>
</tbody>
</table>

Use these buttons on the details toolbar to manage your access request policies associated with the selected asset.

### Table 58: Assets: Access Request Policies tab toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Add to Policy</td>
<td>Add the selected asset to the scope of a session access request policy.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Remove Selected</td>
<td>Remove the selected policy. For more information, see Deleting an access request policy on page 225.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of access request policies.</td>
</tr>
<tr>
<td>Details</td>
<td>View additional details about the selected policy. For more information, see Viewing policy details on page 226.</td>
</tr>
<tr>
<td>Search</td>
<td>To locate a specific policy or set of policies in this list, enter the character string to be used to search for a match. For more information, see Search box on page 65.</td>
</tr>
</tbody>
</table>

**Asset Groups tab**

The **Asset Groups** tab displays the asset groups that contain the selected asset. The Auditor and Security Policy Administrator have permission to access **Asset Groups**. Click (or tap) **Add Asset Groups** from the details toolbar to add the selected asset to one or more asset groups.

**Table 59: Assets: Asset Groups tab properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The asset group name.</td>
</tr>
<tr>
<td>Dynamic</td>
<td>A check mark in this column indicates that the group is a dynamic asset group.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the asset group.</td>
</tr>
</tbody>
</table>

**Related Topics**

Adding an asset to asset groups

**History tab**

The **History** tab allows you to view or export the details of each operation that has affected the selected asset. The **History** tab contains the following information:

**Items**: Total number of entries in the history log.

**Search**: For more information, see Search box on page 65.
Time Frame: By default the history details are displayed for the last 24 hours. Click (or tap) one of the time intervals at the top of the grid to display history details for a different time frame. If the display does not refresh after selecting a different time interval, click (or tap) **Refresh**.

Table 60: Assets History tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>The date and time of the event.</td>
</tr>
<tr>
<td>User</td>
<td>The display name of the user that triggered the event.</td>
</tr>
<tr>
<td>Source IP</td>
<td>The network DNS name or IP address of the managed system that triggered the event.</td>
</tr>
<tr>
<td>Object Name</td>
<td>The name of the selected asset.</td>
</tr>
<tr>
<td>Event</td>
<td>The type of operation made to the selected asset:</td>
</tr>
<tr>
<td></td>
<td>• Create</td>
</tr>
<tr>
<td></td>
<td>• Delete</td>
</tr>
<tr>
<td></td>
<td>• Update</td>
</tr>
<tr>
<td></td>
<td>• Add Membership</td>
</tr>
<tr>
<td></td>
<td>• Remove Membership</td>
</tr>
</tbody>
</table>

| NOTE: A membership operation indicates a "relationship" change with a related or parent object such as an account dependency was added or deleted from the selected asset. |

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related Object</td>
<td>The name of the related object.</td>
</tr>
<tr>
<td>Related Object Type</td>
<td>The type of the related object.</td>
</tr>
<tr>
<td>Parent</td>
<td>The name of the object to which the selected asset is a child.</td>
</tr>
<tr>
<td>Parent Object Type</td>
<td>The parent object type.</td>
</tr>
</tbody>
</table>

Select an event to display this additional information for some types of events (for example, create and update events).

Table 61: Additional History tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>The property that was updated.</td>
</tr>
<tr>
<td>Old Value</td>
<td>The value of the property before it was updated.</td>
</tr>
<tr>
<td>New Value</td>
<td>The new value of the property.</td>
</tr>
</tbody>
</table>
Managing assets

Use the controls and tabbed pages on the Assets page to perform the following tasks to manage Safeguard assets:

- Adding an asset
- Checking an asset’s connectivity
- Assigning an asset to a partition
- Assigning a profile to an asset
- Manually adding a tag to an asset
- Adding an account to an asset
- Adding account dependencies
- Adding an asset to asset groups
- Modifying an asset
- Deleting an asset
- Importing objects
- Discovery
- Downloading a public SSH key

Adding an asset

It is the responsibility of the Asset Administrator to add assets and accounts to Safeguard.

**NOTE:** Safeguard allows you to set up asset discovery jobs that run automatically. For more information, see Asset discovery job workflow on page 490.

**IMPORTANT:** Before you add systems to Safeguard, make sure they are properly configured. For more information, see Preparing systems for management on page 434.

*To add an asset*

1. Navigate to Administrative Tools | Assets.
2. Click (or tap) **Add Asset** from the toolbar.
3. In the **Asset** dialog, provide information in each of the tabs:
   - **General tab** Where you add general information about the asset.
Management tab  Where you add the network address, operating system and version information.

Connection tab  Where you add the authentication type information.

Related Topics
Adding an account to an asset
Assigning an asset to a partition
Assigning a profile to an asset
Assigning assets or accounts to a partition profile

General tab
Use the General tab to specify general information about the asset.

Table 62: Asset: General properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique display name for the asset. Limit: 100 characters Required</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter information about this managed system. Limit: 255 characters</td>
</tr>
</tbody>
</table>
| Partition   | Browse to select a partition for this asset.  

1  NOTE: You can set a specific partition as the default, see Setting a default partition profile. |
| Profile     | Browse to select a profile to manage this asset's accounts.  

1  NOTE: You must assign all assets to a profile. Safeguard assigns all new assets to the default profile unless you specify another. You can set a specific profile as the default. For more information, see Setting a default partition profile on page 241. |

Click (or tap) **Reset** to set the profile to the current default.  

1  NOTE: The **Reset** button only becomes active when the asset has been explicitly assigned to the profile. If the asset is only implicitly assigned to the profile, Safeguard does not activate the **Reset** button. If you do not explicitly assign an asset to a profile, it is always assigned to the current default profile.
Management tab

Use the Management tab to add the network address, operating system and version information for an asset:

Table 63: Asset: Management tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>Select an operating system for this asset.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Safeguard allows you to select a generic operating system of &quot;Other&quot; or &quot;Other Linux&quot;. This allows you to add an asset to Safeguard without designating a specific platform.</td>
</tr>
<tr>
<td></td>
<td>* <strong>Other</strong> - Safeguard cannot manage an asset with an &quot;Other&quot; operating system. You can manually change passwords on accounts associated with an asset with an &quot;Other&quot; operating system, but Safeguard cannot automatically check or change the passwords, test connection, etc. because it cannot connect to the asset.</td>
</tr>
<tr>
<td></td>
<td>* <strong>Other Linux</strong> - Safeguard can manage an asset with &quot;Other Linux&quot; on a best effort basis.</td>
</tr>
<tr>
<td>Version</td>
<td>Select the operating system version. When adding a Linux or Macintosh OS X system, Safeguard allows you to choose an &quot;Other&quot; version.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Safeguard does not manage passwords for accounts on domain controllers. Manage accounts on domain controllers through the directory that hosts the domain controller. For more information, see Adding directory accounts to a directory on page 193.</td>
</tr>
<tr>
<td>Architecture</td>
<td>When applicable, select the operating system architecture.</td>
</tr>
<tr>
<td>Network Address</td>
<td>Enter a network DNS name or the IP address used to connect to the managed system over the network.</td>
</tr>
</tbody>
</table>
### Session Access Properties

Use the following settings to enable session access for this asset.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Session Request</td>
<td>This check box is selected by default indicating that authorized users can request session access for this asset.</td>
</tr>
<tr>
<td></td>
<td>Clear this check box if you do not want to allow session requests for this asset.</td>
</tr>
<tr>
<td>RDP Session Port</td>
<td>Specify the access port on the target server to be used for RDP session requests.</td>
</tr>
<tr>
<td></td>
<td>Default: 3389</td>
</tr>
<tr>
<td>SSH Session Port</td>
<td>Specify the access port on the target server to be used for SSH session requests.</td>
</tr>
<tr>
<td></td>
<td>Default: 22</td>
</tr>
</tbody>
</table>

### Connection tab

On the Connection tab, choose an authentication type and specify the service account credentials. The type of asset specified in the **Product** field on the Management tab determines the authentication types available for the asset.

### Table 64: Asset authentication types

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH Key</td>
<td>To authenticate to the asset using an SSH authentication key.</td>
</tr>
<tr>
<td>Directory Account</td>
<td>To authenticate to the asset using an account from an external identity store such as Microsoft Active Directory.</td>
</tr>
<tr>
<td></td>
<td>☢️ <strong>NOTE:</strong> In order to use this authentication type, you must first add a directory to Safeguard and add domain user accounts. For more information, see <strong>Directories</strong> on page 177.</td>
</tr>
<tr>
<td>Local System Account</td>
<td>To authenticate to the asset using a local system account, which is a Windows user account on the server that is hosting the SQL database.</td>
</tr>
</tbody>
</table>
## Authentication Type

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>To authenticate to the asset using a local service account and password.</td>
</tr>
<tr>
<td>Account Password</td>
<td>To authenticate using the current account password.</td>
</tr>
<tr>
<td>Access Key</td>
<td>To authenticate to the asset using an access key.</td>
</tr>
<tr>
<td>None</td>
<td>To authenticate to the asset manually.</td>
</tr>
</tbody>
</table>

### NOTE:

- This option is only available for SQL Server assets.
- This option is the only option available for Facebook and Twitter assets.
- This option is used by Amazon Web Services assets.

### Client ID:

For SAP assets, enter the client ID.

### About service accounts

Safeguard uses a service account to connect to an asset to securely manage accounts and passwords on that asset. Therefore a service account needs sufficient permissions to edit the passwords of other accounts.

When you add an asset, Safeguard adds its service account to the list of Accounts and designates it with a Service Account icon. By default, Safeguard automatically manages the service account password according to the check and change schedules in the profile that governs its asset. For more information, see Creating a partition profile on page 239.

### TIP:

As a best practice, if you do not want Safeguard to manage a service account password, add the account to a profile that is set to never change passwords.

### NOTE:

When adding a service account, Safeguard automatically disables it from access requests. If you want the password to be available for release, click (or tap) Access Requests and select Enable Password Request. If you want to enable session access, select Enable Session Request.

If you delete a service account, Safeguard changes the asset’s authentication type to None which disables automatic password management for all accounts that are associated with this asset. A user can continue to checkout the passwords, however, if the policy that governs the account requires that it change the password after release, the password can get stuck in a 'pending password reset' state. For more information, see Password is pending a reset on page 462.
Using a directory account as a service account for an asset

To use a directory account as a service account for an asset, you must first add the account to the directory. For more information, see Adding directory accounts to a directory on page 193.

Test connectivity

The most common causes of failure in Safeguard are either connectivity issues between the appliance and the managed system, or problems with service accounts. If you experience issues, first verify that you can access the managed system from another system (independent of Safeguard), using the service account. For more information about troubleshooting connectivity issues, see Test Connection failures and Connectivity failures.

CAUTION: If you restore a backup that is older than the Maximum Password Age set in the Login Control settings, all user accounts (including the bootstrap administrator) will be disabled and you will have to reset all of the user account passwords. If your bootstrap administrator’s password is locked out, you can reset it from the recovery kiosk. For more information, see Admin password reset on page 466.

To restore Safeguard to a backup

1. In Settings, select Backup and Retention | Safeguard Backup and Restore.
2. Select a backup.
   
   ![NOTE: If the backup file is not listed, you can Upload it first.]
3. Click (or tap) Restore.
4. In the Restore dialog, enter the word Restore in the box and click (or tap) OK. Safeguard automatically restarts the appliance, if necessary.
5. Once the appliance is fully operational, it asks you to restart the Windows desktop client.

![NOTE: All modifications to Safeguard objects since the backup was created will be lost.]

CAUTION: After a restore, requesters, approvers, and reviewers will not have access to any access request workflow events that were in process at the time of the backup. The Activity Center displays those workflow events as incomplete.

![NOTE: Safeguard does not restore the appliance IP address, NTP settings or the DNS settings. To verify that these settings are correct after a restore, go to Settings | Appliance Information.]

Safeguard does not restore the appliance IP address, NTP settings or the DNS settings.
About Test Connection

When adding an asset, **Test Connection** verifies that Safeguard can log into the asset using the service account credentials that you have provided.

When adding an asset that requires an SSH host Key, **Test Connection** first discovers the key and presents it to you for acceptance. When you accept it, **Test Connection** then verifies that Safeguard can log into the asset using the service account credentials that you have provided.

Once you save the new asset, Safeguard saves the service account credentials. Safeguard uses these credentials to connect to an asset to securely manage accounts and passwords on that asset. For more information, see About service accounts on page 140.

If you want to verify an existing asset's connectivity, use the **Check Connection** right-click command. For more information, see Checking an asset's connectivity on page 151.

Related Topics

Test Connection failures

**SSH Key**

You can configure Safeguard to authenticate to a managed system using an SSH authentication key.

**NOTE:** This option is not available for all operating systems. But if a Safeguard asset requires an SSH host key and does not have one, Check Password, Change Password, and Test Connection will fail. For more information, see Connectivity failures on page 455.

**Table 65: SSH Key authentication type properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically Generate the SSH Key</td>
<td>Select this option to have Safeguard generate the SSH authentication key.</td>
</tr>
<tr>
<td>Manually Deploy the SSH Key</td>
<td>When you select <strong>Automatically Generate the SSH Key</strong>, Safeguard allows you to select this option so that you can manually append this public key to the authorized keys file on the managed system for the service account. For more information, see Downloading a public SSH key on page 166. The SSH authentication key becomes available after Safeguard creates the asset.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>NOTE:</strong> If you do not select this option, Safeguard automatically installs the SSH authentication key. If you select this option Safeguard creates the key and associates it with the Safeguard asset you are creating, but it does not install it on the managed system for you.</td>
<td></td>
</tr>
<tr>
<td>Import and Manually Deploy the SSH Key</td>
<td>Select this option, then <strong>Browse</strong> to import an SSH authentication key. For more information, see Importing an SSH key on page 144.</td>
</tr>
<tr>
<td>Key Comment</td>
<td><em>(Optional)</em> Enter a description of this SSH key.</td>
</tr>
<tr>
<td>Service Account Name</td>
<td>Enter the service account name that Safeguard is to use for management tasks.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This is the account Safeguard uses to install the SSH authentication key on the asset. For more information, see About service accounts on page 140.</td>
<td></td>
</tr>
<tr>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>Service Account Password</td>
<td>If not importing the SSH authentication key, then you must enter the service account password Safeguard needs to authenticate to this managed system.</td>
</tr>
<tr>
<td>Limit: 255 characters</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Test Connection</strong></td>
<td>Click (or tap) this button to verify that Safeguard can log into this asset using the service account credentials you have provided. For more information, see About Test Connection on page 142.</td>
</tr>
<tr>
<td>Privilege Elevation Command</td>
<td>Enter a privilege elevation command (such as <strong>sudo</strong>), if required. Safeguard uses this as a prefix for commands that require privileged access on the system and to manage accounts on Unix-based systems; that is, to check and change passwords and to discover accounts.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IMPORTANT:</td>
<td>When adding an asset, Safeguard uses this command to perform <strong>Test Connection</strong>. For more information, see <em>About Test Connection</em> on page 142. To enable Safeguard to elevate the privileges of the service account, assign the asset to the scope of a partition profile that has the privilege elevation command defined. For more information, see <em>Creating a partition profile</em> on page 239. The privilege elevation command must run non-interactively, that is, without prompting for a password. For more information, see <em>Prepare Unix-based systems</em> on page 448. Limit: 255 characters</td>
</tr>
<tr>
<td>Auto Accept SSH Host Key</td>
<td>Select this option to have Safeguard automatically accept the SSH host key when it creates the Safeguard asset. When this option is selected, Safeguard displays the thumbprint of the SSH host key that was discovered. <strong>NOTE:</strong> When a managed system requiring an SSH host Key does not have one, <strong>Check Password</strong> will fail. For more information, see <em>Connectivity failures</em> on page 455.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number used by SSH to log into the managed system. Required</td>
</tr>
<tr>
<td>Connection Timeout</td>
<td>Enter the command timeout period. <strong>NOTE:</strong> This option applies only to platforms that use Telnet or SSH. Default: 20 seconds</td>
</tr>
</tbody>
</table>

**NOTE:** Safeguard will not rotate SSH Keys unless you select the **Manage SSH Key** option in the asset's profile change schedule. For more information, see *Adding change password settings* on page 344.

### Importing an SSH key

When you add an asset using the **SSH Key** authentication type, Safeguard gives you the option to **Use an Imported SSH Key**.
To import an SSH Key

1. Click (or tap) **Add Asset** from the toolbar to add an asset.
2. In the Connection tab,
   a. **Authentication type**: Select **SSH Key**.
   b. **SSH Key Generation and Deployment Settings**: Select **Import and Manually Deploy SSH Key**.
   c. **Browse** to select an SSH key.
3. In the **SSH Key** dialog, click (or tap) **Import an SSH Key**.
4. In the **Import an SSH Key** dialog, specify the following information:
   a. **Private Key File**: **Browse** to select a private key file.
   b. **Key Comment**: Enter a comment regarding the key.
   c. Click (or tap) **Import**.

Directory Account

You can configure Safeguard to authenticate to a managed system using an account from an external identity store such as Microsoft Active Directory.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Account</td>
<td>Click (or tap) <strong>Select Account</strong> to choose a domain user account. The accounts available for selection are domain user accounts that are linked to a directory that was previously added to Safeguard. Required</td>
</tr>
<tr>
<td>Test Connection</td>
<td>Click (or tap) this button to verify that Safeguard can log into this asset using the service account credentials you have provided. For more information, see About Test Connection on page 142.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Open to reveal the following settings:</td>
</tr>
<tr>
<td></td>
<td>Į</td>
</tr>
<tr>
<td>Privilege Level Password</td>
<td>Enter the system enable password to allow access to the Cisco configuration.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Privilege Elevation Command</td>
<td>Enter a privilege elevation command (such as sudo), if required. Safeguard uses this as a prefix for commands that require privileged access on the system and to manage accounts on Unix-based systems; that is, to check and change passwords and to discover accounts.</td>
</tr>
<tr>
<td>AUTO Accept SSH Host Key</td>
<td>Select this option to have Safeguard automatically accept an SSH host key.</td>
</tr>
<tr>
<td>Instance</td>
<td>(Optional) Specify the instance name if you have configured multiple instances of a SQL Server on this asset.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number to log into the asset.</td>
</tr>
<tr>
<td>Connection Timeout</td>
<td>Enter the directory connection timeout period. Default: 20 seconds</td>
</tr>
</tbody>
</table>
Local System Account

You can configure Safeguard to authenticate to a managed SQL Server using a local system account and password. The local system account is a Windows user account on the server that is hosting the SQL database.

NOTE: In order to use this authentication type, you must add both a Windows asset and a SQL Server asset to Safeguard.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Account</td>
<td>Click (or tap) <strong>Select Account</strong> to choose the local system account associated with the SQL Server for Safeguard to use for management tasks. Required</td>
</tr>
</tbody>
</table>

**Test Connection**

Click (or tap) this button to verify that Safeguard can log into this asset using the local system account credentials you have provided. For more information, see About Test Connection on page 142.

**Advanced**

Open to reveal the following settings:

- **Instance**
  - (Optional) Specify the instance name if you have configured multiple instances of a SQL Server on this asset.
  
  NOTE: If you have configured a default (unnamed) instance of the SQL Server on the host, you need to provide the IP address and port number.

- **Port**
  - Enter the port number to log into the asset. Required

- **Connection Timeout**
  - Enter the SQL server connection timeout period. Default: 20 seconds

Password

You can configure Safeguard to authenticate to a managed system using a local service account and password.

NOTE: Some options are not available for all operating systems.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distinguished Name</td>
<td>For LDAP platforms, enter the fully qualified distinguished name (FQDN) for the service account. For example: cn=dev-sa,ou=people,dc=example,dc=com</td>
</tr>
<tr>
<td>Service Account Name</td>
<td><strong>Browse</strong> to select the service account for Safeguard to use for management tasks. When you add the asset, Safeguard automatically adds the service account to <strong>Accounts</strong>. For more information, see About service accounts on page 140. Required except for LDAP platforms, which use the Distinguished Name.</td>
</tr>
<tr>
<td>Service Account Password</td>
<td>Enter the service account password used to authenticate to this asset. Limit: 255 characters Required</td>
</tr>
<tr>
<td>Test Connection</td>
<td>Click (or tap) this button to verify that Safeguard can log into this asset using the service account credentials you have provided. For more information, see About Test Connection on page 142.</td>
</tr>
<tr>
<td>Privilege Level Password</td>
<td>Enter the Enable password to allow access to the Cisco configuration.</td>
</tr>
<tr>
<td>Privilege Elevation Command</td>
<td>Enter a privilege elevation command (such as <code>sudo</code>), if required. Safeguard uses this as a prefix for commands that require privileged access on the system and to manage accounts on Unix-based systems; that is, to check and change passwords and to discover accounts.</td>
</tr>
</tbody>
</table>

**IMPORTANT:** When adding an asset, Safeguard uses this command to perform **Test Connection**. For more information, see About Test Connection on page 142.

To enable Safeguard to elevate the privileges of the service account, assign the asset to the scope of a partition profile that has the privilege elevation command defined. For more information, see Creating a partition profile on page 239.

The privilege elevation command must run non-interactively, that is, without prompting for a password. For more information, see Prepare Unix-based systems on page 448.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit: 255 characters</td>
<td></td>
</tr>
<tr>
<td>Auto Accept SSH Host Key</td>
<td>This option is selected by default indicating that Safeguard automatically accepts an SSH host key. Once the SSH host key is discovered, the SSH host key fingerprint is displayed.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> When an asset requiring an SSH host Key does not have one, <strong>Check Password</strong> will fail. For more information, see Connectivity failures on page 455.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This option is not available for all platforms.</td>
</tr>
<tr>
<td>Use SSL Encryption</td>
<td>Select this option to enable Safeguard to encrypt communication with this asset.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If you do not select this option for a Microsoft SQL Server that is configured to Force Encryption, <strong>Test Connection</strong> will use untrusted encryption and succeed with valid credentials. For more information about how Safeguard database servers use SSL, see How do Safeguard database servers use SSL</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>Use this option to enable or disable SSL Certificate verification on the asset.</td>
</tr>
<tr>
<td></td>
<td>When enabled, Safeguard compares the signing authority of the certificate presented by the asset to the certificates in the Trusted Certificates store every time Safeguard connects to the asset. Trust must be established for Safeguard to manage the asset.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> For Safeguard to verify an SSL certificate, you must add the asset's signing authority certificate to the Trusted Certificates store.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Only clear the <strong>Verify SSL Certificate</strong> option if you do not want to establish trust with the asset’s certificate in Safeguard's Trusted Certificates store. One Identity does not recommend disabling this option in production environments.</td>
</tr>
<tr>
<td>Instance</td>
<td>(Optional) Specify the instance name if you have configured multiple instances of a SQL server on this asset.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If you have configured a default (unnamed) instance of the SQL Server on the host, you need to only provide the IP address and port number.</td>
</tr>
</tbody>
</table>
### Property Description

**Workstation ID**
- Specify the configured workstation ID, if applicable.

**NOTE:** This option is only available for IBM i systems.

**Port**
- Enter the port number on which the asset will be listening for connections.
- Default: 22; 1433 for SQL server; 8443 for SonicWALL SMA or CMS appliance.
- Required

**Connection Timeout**
- Enter the connection timeout period.
- Default: 20 seconds

### Access Key

You can configure Safeguard to authenticate to a managed system using an access key.

**Table 69: Access Key authentication type properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Account</td>
<td>Enter an account for Safeguard to use for management tasks. For more information, see <a href="#">About service accounts</a> on page 140.</td>
</tr>
<tr>
<td>Access Key ID</td>
<td>Enter the unique identifier that is associated with the secret key. The access key ID and secret key are used together to sign programmatic AWS requests cryptographically. Limit: 32 alphanumeric characters</td>
</tr>
<tr>
<td>Secret Key</td>
<td>Enter a secret access key used to cryptographically sign programmatic Amazon Web Services (AWS) requests. Limit: 40 alphanumeric characters; the + and the / characters are also allowed.</td>
</tr>
<tr>
<td>Test Connection</td>
<td>Click (or tap) this button to verify that Safeguard can log into this asset using the service account credentials you have provided. For more information, see <a href="#">About Test Connection</a> on page 142.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number to log into the asset.</td>
</tr>
<tr>
<td>Connection Timeout</td>
<td>Enter the connection timeout period. Default: 20 seconds</td>
</tr>
</tbody>
</table>
None

Choose the **None** option if you are planning to manually authenticate to this managed system.

Safeguard cannot manage any accounts associated with an asset set to **None**. All assets must have a service account in order to check and change the passwords for the accounts associated with it.

Checking an asset's connectivity

After you add an asset you can verify that Safeguard can log into it using the **Check Connection** option.

**NOTE:** When you run **Test Connection** from the asset's **Connection** tab (such as when you add the asset initially), you must enter the service account credentials. Once you add the asset to Safeguard it saves these credentials.

The **Check Asset** option does not require that you enter the service account credentials because it uses the saved credentials to verify that it can log into that asset.

**To check an asset's connectivity**

1. Navigate to **Administrative Tools | Assets**.
2. From **Assets**, right-click an asset in the object list to open the asset's context menu.
3. Choose the **Check Connection** option.

   Safeguard displays a Toolbox task pane that shows the results.

Related Topics

About Test Connection
About service accounts

Assigning an asset to a partition

Use the **Assets** view to assign an asset to a partition.

**NOTE:** An asset can only be in one partition at a time. When you add an asset to a partition, all accounts associated with that asset are automatically added to that partition, as well.

You cannot remove an asset from a partition. However, you can add the asset to another partition either from the scope of the other partition or from an asset's **General** properties.
To assign an asset to a partition

1. Navigate to Administrative Tools | Assets.
2. In Assets, double-click (or double-tap) an asset to open the general properties, or click (or tap) the Edit icon next to the General title on the General tab.
3. On the Asset dialog, Browse to select a partition.
4. Click (or tap) OK.

Related Topics
Adding assets to a partition

Assigning a profile to an asset

Use the Assets view to assign a profile to an asset.

To assign a profile to an asset

1. Navigate to Administrative Tools | Assets.
2. In Assets, double-click (or double-tap) an asset to open the general properties, or click (or tap) the Edit icon next to the General title on the General tab.
3. Browse to select a profile, and click (or tap) OK.
   
   NOTE: You can only choose profiles that are in the selected asset's partition.
4. Click (or tap) Reset to set the profile to the current default.

Related Topics
Assigning assets or accounts to a partition profile

Manually adding a tag to an asset

Asset Administrators can manually add and remove tags to an asset using the Tags pane, which is located at the bottom of the General tab when an asset is selected on the Assets view.

To manually add a tag to an asset

1. Navigate to Administrative Tools | Assets.
2. Select an asset from the object list (left-pane).
3. Open the General tab and scroll down to view the Tags pane.
4. Click (or tap) next to the Tags title.
5. Place your cursor in the edit box and enter the tag to be assigned to the selected asset.
   As you type, existing tags that start with the letters entered will appear allowing you to select a tag from the list.
   To add additional tags, press Enter before entering the next tag.
6. Click (or tap) OK.
   If you do not see the new tag, click (or tap)-refresh.
7. To remove a manually assigned tag, click (or tap) the X inside the tag box.

   NOTE: You cannot manually remove dynamically assigned tags which are indicated by a lightening bolt icon. You must modify the rule associated with the dynamic tag if you want to remove it. For more information, see Modifying an asset or asset account tag on page 284.

Adding an account to an asset

Use the Accounts tab on the Assets view to add an account to an asset.

To add an account to an asset

1. Navigate to Administrative Tools | Assets.
2. In Assets, select an asset from the object list and open the Accounts tab.
3. Click (or tap) Add Account from the details toolbar.
4. Enter the account information and click (or tap) Add Account.

For more information about an account's details, see Adding an account.

Adding account dependencies

When one or more Windows servers use a directory account (such as an Active Directory account) to run hosted services and/or tasks, an Asset Administrator can configure a dependency relationship between the directory account and the Windows servers. Safeguard performs dependent system updates to maintain the passwords for dependent accounts on all the systems that use them. For example, when Safeguard changes the directory account password, it updates the credentials on all the Windows server's dependent accounts so that the services or tasks using this account are not interrupted.

NOTE: You must add directory accounts to Safeguard before you can set up account dependency relationships. For more information, see Adding directory accounts to a directory on page 193.
To add account dependencies to Windows servers

1. Navigate to Administrative Tools | Assets.
2. In Assets, select a Windows server from the object list and open the Account Dependencies tab.
3. Click (or tap) + Add Account from the details toolbar and select one or more directory accounts.

**NOTE:** Safeguard only allows you to select directory accounts.

Adding an asset to asset groups

Use the Asset Groups tab on the Assets view to add an asset to one or more asset groups.

**To add an asset to asset groups**

1. Navigate to Administrative Tools | Assets.
2. In Assets, select an asset from the object list and open the Asset Groups tab.
3. Click (or tap) + Add Asset Group from the details toolbar.
4. Select one or more asset groups from the list in the Asset Groups selection dialog and click (or tap) OK.

If you do not see the asset group you are looking for, depending on your Administrator permissions, you can create it in the Asset Groups selection dialog. (You must have Security Policy Administrator permissions to create asset groups.

**To create a new asset group from the Asset Groups selection dialog**

1. Click (or tap) + Create New.
   
   For more information on creating asset groups, see Adding an asset group.
2. Create additional asset groups, as required.
3. Click (or tap) OK in the Asset Groups selection dialog to add the new asset to the selected asset group.

Modifying an asset

**To modify an asset**

1. Navigate to Administrative Tools | Assets.
2. In Assets, select an asset from the object list.
3. Select the view of the asset's information you want to modify (General, Accounts,
or Account Dependencies).

For example:

- To change an asset's connection information, for example connection timeout, double-click (or double-tap) the Connection information in the General tab or click (or tap) the Edit icon.
  
  NOTE: You can also double-click (or double-tap) an asset name to open the General settings edit window.

- To add (or remove) an account to this asset, switch to the Accounts tab.

- To add (or remove) a directory account to a Windows server as an account dependency, switch to the Account Dependencies tab. For more information, see Adding account dependencies on page 153.

4. To view or export the details of each operation that has affected the selected asset, switch to the History tab.

  NOTE: If you add an asset with a generic operating system, you can change an "Other" operating system to any other platform or an "Other Linux" operating system to any type of Linux, such as AIX, HP-UX, Solaris, etc. However, once you save an asset with a specific operating system, you cannot modify the platform type.

## Deleting an asset

- IMPORTANT: When you delete an asset, you also permanently delete all the Safeguard accounts associated with the asset.

- NOTE: The Asset Administrator can delete an asset that has active access requests.

**To delete an asset**

1. Navigate to Administrative Tools | Assets.
2. In Assets, select an asset from the object list.
3. Click (or tap) Delete Selected.
4. Confirm your request.

## Importing objects

Safeguard allows you to import a .csv file containing a set of accounts, assets, or users.
To import a set of objects

1. Click (or tap) **Import** from the toolbar.

2. In the **Import** dialog, **Browse** to select an existing `.csv` file containing a list of objects to import.

   **NOTE:** For assistance in creating an import file, click (or tap) **CSV Template Assistant**. For more information, see Creating an import file on page 109.

3. When importing assets, the **Discover SSH Host Keys** option is selected by default indicating that Safeguard will retrieve the required SSH host key for the assets specified in the CSV file.

4. Click (or tap) **OK**.

   Safeguard imports the objects into its database.

   **NOTE:** Safeguard does not add an object if any column contains invalid data in the `.csv` file with the follow exceptions:

   - **Assets PlatformDisplayName** property.
     a. If Safeguard does not find an exact match, it looks for a partial match. If it finds a partial match it supplies the `<platform>` Other platform, such as "Other Linux".
     b. If it does not find a partial match, it supplies the Other platform type.

   - **Users TimeZoneId** property.
     a. If Safeguard does not find a valid TimeZoneId property (that is, does not find an exact match or no timezone was provided), it uses the local workstation's current timezone.

       **NOTE:** Do not enter numbers or abbreviations for the TimeZoneId.

   - **Users Password** property.
     a. Safeguard adds a user without validating the password you provide.

5. Navigate to the **Tasks** pane in the **Toolbox** for details about the import process and invalid data messages. For more information, see Viewing task status on page 93.

Discovery

One Identity Safeguard allows you to set up asset discovery jobs to run automatically against the directories you have added to Safeguard. For more information, see **Asset discovery job workflow** on page 490.

The **Discovery** menu in **Assets** has these options.
Table 70: Asset Discovery menu options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Where you add a new asset discovery job. For more information, see Creating an asset discovery job on page 157.</td>
</tr>
<tr>
<td>Manage</td>
<td>Where you can add, modify or run asset discovery jobs. For more information, see Managing asset discovery jobs on page 165.</td>
</tr>
</tbody>
</table>

When an asset discovery job runs, Safeguard adds the assets it finds to Assets. If Safeguard cannot detect the operating system, it applies the "Other" or "Other Linux" operating system which you can modify later. For more information, see Modifying an asset on page 154.

Once Safeguard adds an asset, you can press and hold (or right-click) it and choose one of these context menu options.

Table 71: Asset Discovery context menu options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑️ Manage</td>
<td>Select to have Safeguard manage an &quot;ignored&quot; asset. This option is only available for assets that have been ignored.</td>
</tr>
<tr>
<td>☢️ Ignore</td>
<td>Select to prevent Safeguard from managing the selected asset.</td>
</tr>
</tbody>
</table>

NOTE: When you Ignore an asset, Safeguard disables it and removes all associated accounts. If you choose to Manage the asset later, Safeguard re-enables all the associated accounts.

Creating an asset discovery job

To create a new asset discovery job

1. Navigate to Administrative Tools | Assets.
2. From Assets, click (or tap) the ☰️ Discovery toolbar button.
3. On the Asset Discovery Jobs dialog, click (or tap) + to create a new asset discovery job.
4. In the Discovery dialog, provide information for the discovery job on the following tabs:
General tab

Where you add general information about the discovery job and identify which partition you want Safeguard to add the assets it discovers.

Information tab

Where you select the directory and set the search location.

Rules tab

Where you define the search constraints and conditions and choose the profile you want to govern the discovered assets.

Schedule tab

Where you configure the schedule for the discovery job.

Summary tab

Where you review the asset discovery job parameters and save it.

After you save the discovery job, you can modify or run it using the toolbar buttons on the Asset Discovery Jobs dialog. For more information, see Managing asset discovery jobs on page 165.

General tab

On the General tab, supply general information about the asset discovery job and identify the partition where you want Safeguard to add the assets it discovers.

Table 72: Discovery: General properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the asset discovery job. Limit: 50 characters Required</td>
</tr>
<tr>
<td>Description</td>
<td>Enter information about this asset discovery job. Limit: 255 characters</td>
</tr>
</tbody>
</table>
| Partition  | **Browse** to select the partition in which to manage the discovered assets.  
**IMPORTANT:** You cannot change the partition after you save this discovery job. Required |
| Method     | Choose a type of discovery:  
- Directory  
- Network Scan  
Required |
Information tab

On the Information tab define the directory or network information for the discovery job.

Table 73: Discovery: Information properties for Directory scans

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory</td>
<td>Select the Directory on which to run the asset discovery job. Required</td>
</tr>
</tbody>
</table>

Table 74: Discovery: Information properties for Network scans

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable OS Detection</td>
<td>This check box is selected by default indicating that OS fingerprinting is to be used to detect the operation system being used. Clear this check box if you do not want to use the OS fingerprinting process.</td>
</tr>
<tr>
<td>IPv4 Range</td>
<td>Enter a range of IPv4 addresses to scan:</td>
</tr>
<tr>
<td></td>
<td>• Starting IP Address</td>
</tr>
<tr>
<td></td>
<td>• Ending IP Address</td>
</tr>
<tr>
<td></td>
<td>Click (or tap) + Add or − Delete to add or remove IPv4 address range sets. Required</td>
</tr>
<tr>
<td>Advanced</td>
<td>Open to reveal the following setting for each IPv4 address range set:</td>
</tr>
<tr>
<td>Exclude IP</td>
<td>Safeguard allows you to exclude an IP address within a specified IPv4 range from the scan.</td>
</tr>
<tr>
<td></td>
<td>Click (or tap) + Add to exclude an IP address from the scan.</td>
</tr>
<tr>
<td></td>
<td>Click (or tap) − Delete to remove the corresponding excluded IPv4 address and include that IP address in the scan.</td>
</tr>
</tbody>
</table>

Rules tab

On the Rules tab define the search constraints and conditions, and choose the profile you want to govern the discovered assets.

**NOTE:** You can configure multiple rules for an asset discovery job. Safeguard considers each rule separately and combines the results.
**To add a new asset discovery rule**

1. On the **Rules** tab, click (or tap) **Add**.
2. In the **Rule** dialog, enter a name for the new asset discovery rule of up to 50 characters.
3. Under **Settings**:
   a. Select **Add Condition** to add one or more constraints or an advanced LDAP filter.
   b. Select **Add Connection** to configure the authentication parameters.
      
      **NOTE:** Connection defaults to NONE.
   c. Select **Add Profile** to select a profile to govern the discovered assets.
      
      **NOTE:** Profile defaults to the partition default profile.

      **NOTE:** You must specify at least one condition, the connection and a profile for each rule. The **OK** button in the **Rules** dialog will be disabled until all of these settings are defined.
4. Click (or tap) **OK** to save the asset discovery rule.

**IMPORTANT**: A discovery job can have more than one rule. When Safeguard runs the discovery job, if it finds an asset with more than one rule, it applies the connection and profile settings of the first rule that discovers the asset. Once Safeguard creates an asset, it will not attempt to re-create it or modify it if rediscovered by a different job.

**Add Condition**

**Conditions** allow you to add one or more search conditions.

**To add a condition (Constraint)**

1. In the **Rule** dialog, select **Add Condition**.
2. In the **Condition** dialog,
   a. **Find By**: Choose **Constraints** and enter the search criteria to be used:
3. To apply constraints,
   a. Select a property:
      
      - **Name**
      - **Description**
      - **Network Address**
      - **Operating System**
      - **Operating System Version**
NOTE: For Network Scan, you can only apply constraints on the information the network finds, which is **Name** and **Operating System**.

b. Select an operation:
   - Equals
   - Not Equals
   - Starts With
   - Ends With
   - Contains

c. Type a value of up to 255 characters.

   **NOTE:** The search is case sensitive and does not allow wild cards.

4. Click (or tap) **Preview** to test the conditions you have configured.

   **Preview** displays a list of assets Safeguard will find in the directory or network you specified in the **Information** tab based on these conditions.

   **NOTE:** While a discovery rule can have more than one condition; each condition can have one or more constraints. When you select **Preview**, Safeguard considers all the search constraints in the current condition and returns the assets it finds based only on that condition. When Safeguard runs the discovery job, it finds all assets that meet all of the search conditions.

5. Click (or tap) **+ Add** to additional constraints to your search criteria.

6. Click (or tap) **– Delete** to remove the corresponding constraint from your search criteria.

7. Click (or tap) **OK** to save your selections.

**To add a condition (Filter Search Base)**

Search base limits the search to the defined branch of the specified directory, including sub containers if that option is selected.

   **NOTE:** This condition is only available for a **Directory** discovery job (LDAP or Active Directory directories).

1. In the **Rule** dialog, select **Add Condition**.

2. In the **Condition** dialog,
   a. **Find By**: Choose **LDAP Filter** and enter the search criteria to be used:
   b. **Filter Search Location**: **Browse** to select a container within the directory to search for assets.

      **TIP:** Do not select the Directory Root for asset discovery jobs.

c. **Include objects from sub containers**: Optionally select this check box to search for assets in sub-containers.
3. Click (or tap) **Preview** to test the conditions you have configured.
4. Click (or tap) **OK** to save your selections.

**To add a condition (Group)**

| NOTE: This condition is only available for a **Directory** discovery job. |

1. In the **Rule** dialog, select **Add Condition**.
2. In the **Condition** dialog,
   a. **Find By**: Choose **Group**.
   b. Click (or tap) + **Add** to launch the **Group** dialog.
   c. **Contains**: Enter a full or partial group name and click **Search**.
      | NOTE: You can only enter a single string (full or partial group name) at a time.
   d. **Filter Search Location**: **Browse** to select a container to search within the directory.
   e. **Include objects from sub containers**: Select this check box to include child objects.
   f. **Select the group to add**: The results of the search displays in this grid. Select one or more groups to add to the discovery job.
3. Click (or tap) **Preview** to test the conditions you have configured.
   **Preview** displays a list of assets Safeguard will find in the directory or network you specified in the **Information** tab based on these conditions.
4. Click (or tap) **OK** to save your selections.

**To add a condition (Find All)**

1. In the **Rule** dialog, select **Add Condition**.
2. In the **Condition** dialog,
   a. **Find By**: Choose **Find All**.
   b. **Filter Search Location**: **Browse** to select a container within the directory to search for assets.
      | NOTE: The Filter Search Location is only available for **Directory** discovery jobs.
3. Click (or tap) **Preview** to test the conditions you have configured.
   **Preview** displays a list of assets Safeguard will find in the directory or network you specified in the **Information** tab based on these conditions.
4. Click (or tap) **OK** to save your selections.
Add Connection

You must configure how you want Safeguard to connect to and communicate with the discovered assets.

IMPORTANT: A discovery job can have more than one rule. When Safeguard runs the discovery job, if it finds an asset with more than one rule, it applies the connection and profile settings of the first rule that discovers the asset. Once Safeguard creates an asset, it will not attempt to re-create it or modify it if rediscovered by a different job.

To add connection information

1. In the Rule dialog, click (or tap) Edit next to Connection.
2. In the Connection dialog, select an Authentication Type:
   - SSH Key: To authenticate to the asset using an SSH authentication key.
     Browse to select an SSH Key and provide an account name.
   - Directory Account: To authenticate to the assets using an account from an external identity store such as Microsoft Active Directory, select the service account.
     Click (or tap) Select Account to choose the directory account.
   - Password: To authenticate to the assets using a local service account and password.
     Enter the account name and password.
   - None: To authenticate to the assets manually.
3. To verify the connection setting, click (or tap) Test Connection.
   Test Connection returns a list of assets Safeguard will find in the directory you set in the Information tab.
4. Choose an asset and click (or tap) OK.
5. If asked to Verify Host Authenticity, click (or tap) Yes to accept the SSH Key for the host.
6. You can click (or tap) Test Connection again to verify the connection setting on another asset or OK to return to the Rule dialog to continue configuring the discovery rule.

NOTE: Assets that fail the test connection during the asset discovery are created with a authentication type of NONE.

Add Profile

During discovery, Safeguard automatically adds the assets that it finds and begins to manage them according to the settings in the profile you set on the Rules tab.
**To add the profile information**

1. In the Rule dialog, click (or tap) Edit next to Profile.
2. Browse to select a profile to govern the discovered assets.
   - **NOTE:** You can only choose a profile that is associated with the partition selected in the General tab.
3. Click (or tap) OK to save your selection.

   - **IMPORTANT:** A discovery job can have more than one rule. When Safeguard runs the discovery job, if it finds an asset with more than one rule, it applies the connection and profile settings of the first rule that discovers the asset. Once Safeguard creates an asset, it will not attempt to re-create it or modify it if rediscovered by a different job.

**Schedule tab**

On the Schedule tab configure when you want to run the asset discovery job.

**To schedule an asset discovery job**

1. On the Schedule tab,
   a. **Interval:** Choose Never, Minute, Hour, Day, Week, or Month.
      - **NOTE:** Best Practice: Do not use the Minute interval.
      - **NOTE:** If you selected Never, click (or tap) Next to proceed to the Summary tab. For all other intervals, proceed with step 1b.
   b. **Time of day:** Set the start time.
   c. **Repeat interval:** Select the interval you would like to repeat the asset discovery job.
      - If Weekly, select which days of the week to run the asset discovery job.
      - If Monthly, set the task recurrence pattern: Day of month or week of month and day of week.
   d. **Time Zone:** Select the time zone.

**Summary tab**

On the Summary tab review the asset discovery job parameters and save it.

1. Review the following settings:
   - Method
   - Information
2. Modify the asset discovery job settings, if necessary.
3. Click (or tap) Add Discovery to save the discovery job.

Managing asset discovery jobs

To add, modify, or run asset discovery jobs
1. Navigate to Administrative Tools | Assets.
2. From Assets, click (or tap) the Discovery toolbar button.
3. Use these buttons on the Asset Discovery Jobs dialog to manage discovery jobs.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add an asset discovery job. For more information, see Creating an asset discovery job on page 157.</td>
</tr>
<tr>
<td>Delete Selected</td>
<td>Remove the selected asset discovery job.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of asset discovery jobs.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modify the selected asset discovery job.</td>
</tr>
<tr>
<td>Run Now</td>
<td>Run the selected asset discovery job.</td>
</tr>
<tr>
<td>Cancel Running Job</td>
<td>Stop the running asset discovery job.</td>
</tr>
</tbody>
</table>

4. After a discovery job runs, the right pane allows you to view:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td># Assets Found</td>
<td>The number of asset found during the discovery job.</td>
</tr>
<tr>
<td>Last Run Date</td>
<td>The date the selected discovery job ran.</td>
</tr>
<tr>
<td>Last Run Time</td>
<td>The time the selected discovery job ran.</td>
</tr>
<tr>
<td>Started By</td>
<td>The user or process that initiated the discovery job.</td>
</tr>
<tr>
<td>Schedule</td>
<td>The frequency and time the selected discovery job is configured to run.</td>
</tr>
<tr>
<td>Next Run Date</td>
<td>The date when the discovery job is scheduled to run next.</td>
</tr>
<tr>
<td>Next Run Time</td>
<td>The time when the discovery job is scheduled to run next.</td>
</tr>
<tr>
<td>Details</td>
<td>Click (or tap) Details to view the name and network address of the assets the selected discovery job found.</td>
</tr>
</tbody>
</table>
History Click (or tap) **History** to view the results of a previous run of the selected job. Double-click (or double-tap) a job to open the details for it.

**NOTE:** You can also search the **Activity Center** for information about discovery jobs that have run. Safeguard lists the asset discovery events in the **Asset Discovery Activity** category.

---

**Downloading a public SSH key**

When you add an asset and select the **Automatically Generate the SSH Key** (SSH Key Generation and Deployment setting on the Connection page in the **Asset** dialog), Safeguard allows you to download the SSH key so that you can manually install it on the asset.

**To download a public SSH key**

1. Navigate to **Administrative Tools | Assets**.
2. In **Assets**, select an asset that has an SSH key authentication type.
3. Click (or tap) the **Download SSH Key** from the toolbar or the context menu.
   - **OR**-
   Open the asset’s **Connection** settings and select **Download SSH Key**.
4. In the **Save As** dialog, specify the drive, directory, and name of the file to save.

You can manually install this public key to an asset.
Asset Groups

A Safeguard asset group is a set of assets which you can add to the scope of an access request policy. For more information, see Creating an access request policy on page 214.

The Auditor and the Security Policy Administrator have permission to access Asset Groups.

The Asset Groups view displays the following information about the selected asset group.

**Table 75: Asset Groups: Tabs**

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td>Displays general information about the selected asset group.</td>
</tr>
<tr>
<td>Assets tab</td>
<td>Displays the assets associated with the selected asset group.</td>
</tr>
<tr>
<td>Access Request Policies tab</td>
<td>Displays the entitlements and access request policies associated with the selected asset group.</td>
</tr>
<tr>
<td>History tab</td>
<td>Displays the details of each operation that has affected the selected asset group.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage asset groups.

**Table 76: Asset Groups: Toolbar**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✚ Add</td>
<td>Asset Group</td>
</tr>
<tr>
<td>✚ Add</td>
<td>Dynamic Asset Group</td>
</tr>
<tr>
<td>✖ Delete Selected</td>
<td>Remove the selected asset group from Safeguard. For more information, see Deleting an asset group on page 175.</td>
</tr>
<tr>
<td>☐ Refresh</td>
<td>Update the list of asset groups.</td>
</tr>
</tbody>
</table>
General tab

The General tab lists information about the selected asset group. The large tile at the top of the tab displays the number of Assets and Access Request Policies associated with the selected asset group. Clicking a tile heading opens the corresponding tab.

Table 77: Asset Groups General tab: General properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The selected asset group's name.</td>
</tr>
</tbody>
</table>

Description: Information about the selected asset group.
Asset Rules: For dynamic asset groups, a summary of the asset rules defined.

Related Topics
Modifying an asset group

Assets tab

The Assets tab displays the assets associated with the selected asset group.
Click (or tap) + Add Asset from the details toolbar to add one or more assets to the selected asset group.

Search: For more information, see Search box on page 65.

Table 78: Asset Groups: Assets tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The asset name assigned to the managed system.</td>
</tr>
<tr>
<td>Platform Type</td>
<td>The platform of the managed system.</td>
</tr>
<tr>
<td>Session Request</td>
<td>A check in this column indicates that session access requests are enabled for the asset.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the asset.</td>
</tr>
</tbody>
</table>

Related Topics
Adding assets to an asset group
Modifying an asset group
Access Request Policies tab

The Access Request Policies tab displays the entitlements and access request policies, associated with the selected asset group.

Click (or tap) + Add to Policy from the details toolbar to add the selected asset group to the scope of one or more access request policies.

Table 79: Asset Groups: Access Request Policies tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entitlement</td>
<td>The name of the access request policy's entitlement.</td>
</tr>
<tr>
<td>Access Request Policy</td>
<td>The name of the policy that governs the assets in the selected asset group.</td>
</tr>
<tr>
<td>Asset Groups</td>
<td>The number of unique asset groups in the access request policy.</td>
</tr>
<tr>
<td>Assets</td>
<td>The number of unique assets in the asset groups that are associated with the access request policy.</td>
</tr>
</tbody>
</table>

Use these buttons on the details toolbar to manage your access request policies associated with the selected asset group.

Table 80: Asset Groups: Access Request Policies tab toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Add to Policy</td>
<td>Add the selected asset group to the scope of an access request policy.</td>
</tr>
<tr>
<td>— Remove Selected</td>
<td>Remove the selected policy. For more information, see Deleting an access request policy on page 225.</td>
</tr>
<tr>
<td>C Refresh</td>
<td>Update the list of access request policies.</td>
</tr>
<tr>
<td>☰ Details</td>
<td>View additional details about the selected policy. For more information, see Viewing policy details on page 226.</td>
</tr>
<tr>
<td>🕵 Search</td>
<td>To locate a specific policy or set of policies in this list, enter the character string to be used to search for a match. For more information, see Search box on page 65.</td>
</tr>
</tbody>
</table>

History tab

The History tab allows you to view or export the details of each operation that has affected the selected asset group.

The History tab contains the following information:
Items: Total number of entries in the history log.

Search: For more information, see Search box on page 65.

Time Frame: By default the history details are displayed for the last 24 hours. Click (or tap) one of the time intervals at the top of the grid to display history details for a different time frame. If the display does not refresh after selecting a different time interval, click (or tap) Refresh.

Table 81: Asset Groups: History tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>The date and time of the event.</td>
</tr>
<tr>
<td>User</td>
<td>The display name of the user that triggered the event.</td>
</tr>
<tr>
<td>Source IP</td>
<td>The network DNS name or IP address of the managed system that triggered the event.</td>
</tr>
<tr>
<td>Object Name</td>
<td>The name of the selected asset group.</td>
</tr>
<tr>
<td>Event</td>
<td>The type of operation made to the selected account group:</td>
</tr>
<tr>
<td></td>
<td>• Create</td>
</tr>
<tr>
<td></td>
<td>• Delete</td>
</tr>
<tr>
<td></td>
<td>• Update</td>
</tr>
<tr>
<td></td>
<td>• Add Membership</td>
</tr>
<tr>
<td></td>
<td>• Remove Membership</td>
</tr>
<tr>
<td>NOTE:</td>
<td>A membership operation indicates a &quot;relationship&quot; change with a related or parent object such as the selected asset group was added or removed from the membership of a policy, or an asset was added or removed from the membership of the selected asset group.</td>
</tr>
<tr>
<td>Related Object</td>
<td>The name of the related object.</td>
</tr>
<tr>
<td>Related Object Type</td>
<td>The type of the related object.</td>
</tr>
<tr>
<td>Parent</td>
<td>The name of the object to which the selected asset group is a child.</td>
</tr>
<tr>
<td>Parent Object Type</td>
<td>The parent object type.</td>
</tr>
</tbody>
</table>

Select an event to display this additional information for some types of events (for example, create and update events).
Table 82: Additional History tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>The property that was updated.</td>
</tr>
<tr>
<td>Old Value</td>
<td>The value of the property before it was updated.</td>
</tr>
<tr>
<td>New Value</td>
<td>The new value of the property.</td>
</tr>
</tbody>
</table>

Managing asset groups

Use the controls and tabbed pages in the Asset Groups view to perform the following tasks to manage Safeguard asset groups:

- Adding an asset group
- Adding a dynamic asset group
- Adding assets to an asset group
- Modifying an asset group
- Deleting an asset group

Adding an asset group

It is the responsibility of the Security Policy Administrator to add asset groups to Safeguard.

Use the Asset Groups view to add new asset groups to Safeguard.

To add an asset group

1. Navigate to Administrative Tools | Asset Groups.
2. Click (or tap) + Add Asset Group from the toolbar.
3. In the Asset Group dialog, enter the following information:
   a. Name: Enter a unique name for the asset group.
      Limit: 50 characters
   b. Description: (Optional) Enter descriptive text about this asset group.
      Limit: 255 characters
4. Click (or tap) Add Asset Group.
Adding a dynamic asset group

It is the responsibility of the Security Policy Administrator to add asset groups to Safeguard.

To add a dynamic asset group

1. Navigate to Administrative Tools | Asset Groups.
2. From Asset Groups, click (or tap) + Add | Add Dynamic Asset Group from the toolbar.
3. In the Dynamic Asset Group dialog, provide information in each of the tabs:

   **General tab** | Where you add general information about the dynamic asset group.
   **Asset Account Rules tab** | Where you define the rules to be used to identify what assets are to be included in the dynamic asset group.
   **Summary tab** | Where you review the rules defined for adding assets to this dynamic asset group, and where you save your selections and create the dynamic asset group.

Related Topics

When does the rules engine run for dynamic grouping and tagging

**General tab**

On the General tab of the Dynamic Asset Group dialog, supply general information about the dynamic asset group.

**Table 83: Dynamic Asset Group: General tab**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the dynamic asset group. Limit: 50 characters Required</td>
</tr>
<tr>
<td>Description</td>
<td>Enter information about this dynamic asset group. Limit: 255 characters</td>
</tr>
</tbody>
</table>
Asset Rules tab

Use the rule editor controls on the Asset Rules tab of the Dynamic Asset Group dialog to define what assets are to be included in the dynamic asset group.

### Table 84: Dynamic Asset Group: Asset Rules tab

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>**AND</td>
<td>OR**</td>
</tr>
<tr>
<td><strong>Attribute</strong></td>
<td>In the first query clause box, select the attribute to be searched. Valid attributes include:</td>
</tr>
<tr>
<td></td>
<td>• Name (default)</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Platform</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
</tr>
<tr>
<td></td>
<td>• Tag</td>
</tr>
<tr>
<td></td>
<td>• Discovery Job Name</td>
</tr>
<tr>
<td></td>
<td>• Partition Name</td>
</tr>
<tr>
<td></td>
<td>• Profile</td>
</tr>
<tr>
<td></td>
<td>• Network Address</td>
</tr>
<tr>
<td><strong>Operator</strong></td>
<td>In the middle clause query box, select the operator to be used in the search. The operators available depend upon the data type of the attribute selected. For string attributes, the operators may include:</td>
</tr>
<tr>
<td></td>
<td>• Contains (Default)</td>
</tr>
<tr>
<td></td>
<td>• Does not contain</td>
</tr>
<tr>
<td></td>
<td>• Starts with</td>
</tr>
<tr>
<td></td>
<td>• Ends with</td>
</tr>
<tr>
<td></td>
<td>• Equals</td>
</tr>
<tr>
<td></td>
<td>• Not equal</td>
</tr>
<tr>
<td></td>
<td>For boolean attributes, the operators may include:</td>
</tr>
<tr>
<td></td>
<td>• Is True</td>
</tr>
</tbody>
</table>
## Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search string</td>
<td>In the last clause query box, enter the search string or value to be used to find a match.</td>
</tr>
<tr>
<td>+</td>
<td>−</td>
</tr>
<tr>
<td>Add Grouping</td>
<td>Click (or tap) the Add Grouping button to add an additional set of conditions to be met. A new grouping is added under the last query clause in a group and appears in a bordered pane showing that it is subordinate to the higher level query conditions. Click (or tap) the Remove button to remove a grouping from the search criteria.</td>
</tr>
<tr>
<td>Preview</td>
<td>Click (or tap) Preview to run the query in order to review the results of the query before adding the dynamic group.</td>
</tr>
</tbody>
</table>

### Summary tab

On the Summary tab of the Dynamic Asset Group dialog, review the rules defined for adding assets to the dynamic asset group, save your selections, and add the dynamic asset group to Safeguard.

1. Review the rules defined for this dynamic asset group.
2. Return to the Asset Rules tab to modify any of the rules if necessary.
3. Click (or tap) Add Asset Group to create the dynamic asset group.

### Adding assets to an asset group

From the Assets tab on the Asset Groups view, you can add one or more assets to an asset group.

**To add assets to an asset group**

1. Navigate to Administrative Tools | Assets Groups.
2. In Asset Groups, select an asset group from the object list and open the Assets tab.
3. Click (or tap) + Add Asset from the details toolbar.
4. Select one or more assets from the list in the **Assets** selection dialog and click (or tap) **OK**.

   **NOTE:** You can also double-click (or double-tap) an asset name to add it.

If you do not see the asset you are looking for, depending on your **Administrator permissions**, you can create it in the Assets selection dialog. (You must have Asset Administrator permissions to create assets.)

**To create a new asset from the Assets selection dialog**

1. Click (or tap) **Create New**.
   
   For more information on creating assets, see Adding an asset.
2. Create additional assets, as required.
3. Click (or tap) **OK** in the Assets selection dialog to add the assets to the selected asset group.

## Modifying an asset group

**To modify an asset group’s information**

1. Navigate to **Administrative Tools | Asset Groups**.
2. In **Asset Groups**, select an asset group from the object list.
3. Select the view of the asset group’s information you want to modify (**General** or **Assets**).

   **For example:**
   
   - To change an asset group’s name or description, double-click (or double-tap) the **General** information in the **General** tab or click (or tap) the ☑ **Edit** icon.

     **NOTE:** You can also double-click (or double-tap) an asset group name to open the **General** settings edit window.

   - To add (or remove) assets to the selected asset group, open the **Assets** tab.
4. To view or export the details of each operation that has affected the selected asset group, open the **History** tab.

## Deleting an asset group

**NOTE:** When you delete an asset group, Safeguard does not delete the associated assets.
To delete an asset group

1. Navigate to Administrative Tools | Asset Groups.
2. In Asset Groups, select an asset group from the object list.
3. Click (or tap) Delete Selected.
4. Confirm your request.
Directories

You can leverage your existing directory infrastructure (such as Microsoft Active Directory) in One Identity Safeguard. Once you import directory users and directory groups, Safeguard automatically synchronizes the objects in its database with the directory schema attributes. User and group membership changes in the directory are reflected in Safeguard. Directory users authenticate to Safeguard with their directory credentials.

Safeguard supports the RBAC model of separation of duties. With directory integration there are three distinct roles in play: the Directory Administrator, the User Administrator, and the Security Policy Administrator.

- The Directory Administrator integrates the directory with Safeguard by specifying the credentials Safeguard should use to read from the directory. They also add the directory accounts to make them available for use in access request policies.
- The User Administrator adds directory users and directory groups to Safeguard.
- The Security Policy Administrator assigns directory users and groups to access request policies to get access to privileged passwords.

The Auditor and the Directory Administrator have permission to access Directories.

The Directories view displays the following information about the selected directory.

Table 85: Directories: Tabs

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td>Displays general and attribute settings information.</td>
</tr>
<tr>
<td>Accounts tab</td>
<td>Displays the user accounts associated with the selected directory.</td>
</tr>
<tr>
<td>Profiles tab</td>
<td>Displays the profiles associated with the selected directory.</td>
</tr>
<tr>
<td>Discovered Accounts tab</td>
<td>Displays the accounts Safeguard discovers when it runs a directory account discovery job. For more information, see Directory account discovery job workflow on page 492.</td>
</tr>
<tr>
<td>History tab</td>
<td>Displays the details of each operation that has affected the selected directory.</td>
</tr>
</tbody>
</table>
Use these toolbar buttons to manage directories.

### Table 86: Directories: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Directory</td>
<td>Add an external identity provider, such as Active Directory, to Safeguard. For more information, see Adding a directory on page 188.</td>
</tr>
<tr>
<td>Delete Selected</td>
<td>Remove the selected directory. For more information, see Deleting a directory on page 203.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of directories.</td>
</tr>
<tr>
<td>Sync Now</td>
<td>Click (or tap) Sync Now to:</td>
</tr>
<tr>
<td></td>
<td>• Run the directory account discovery jobs currently set up. For more information, see Managing directory account discovery jobs on page 195.</td>
</tr>
<tr>
<td></td>
<td>• AND-</td>
</tr>
<tr>
<td></td>
<td>• Synchronize the Safeguard database with the properties of any objects imported into Safeguard from the selected directory. For more information, see General tab on page 189.</td>
</tr>
</tbody>
</table>

Use these context menu options to manage directories:

### Table 87: Directories context menu options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Connection</td>
<td>Select to verify that Safeguard can log into the directory using the current service account credentials. For more information, see Checking a directory's connectivity on page 193.</td>
</tr>
<tr>
<td>Delete Selected</td>
<td>Remove the selected directory from Safeguard. For more information, see Deleting a directory on page 203.</td>
</tr>
</tbody>
</table>
### General tab

The **General** tab lists information about the selected directory.

Large tiles at the top of the tab display the number of directory *Accounts*, *Profiles*, and *Discovered Accounts* associated with the selected directory.

**Table 88: Directories General tab: General properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forest Root Domain Name</td>
<td>The forest root domain name.</td>
</tr>
<tr>
<td>Domains</td>
<td>A list of domain names in the forest.</td>
</tr>
<tr>
<td>Service Account Domain Name</td>
<td>The service account's fully qualified directory domain name.</td>
</tr>
<tr>
<td>Service Account Name</td>
<td>An account Safeguard uses for management tasks.</td>
</tr>
<tr>
<td>Sync additions every</td>
<td>The interval for synchronizing additions to the directory object (group membership and user account attributes) properties.</td>
</tr>
<tr>
<td>Sync deletions every</td>
<td>The interval for synchronizing deletions from the directory object properties.</td>
</tr>
<tr>
<td>Last Sync</td>
<td>The last date and time Safeguard synchronized its database with the selected directory object properties.</td>
</tr>
<tr>
<td>Last Delete Sync</td>
<td>The last date and time Safeguard synchronized deletions from the directory object properties.</td>
</tr>
<tr>
<td>Last Failure Sync</td>
<td>The last date and time Safeguard failed to synchronize its database with the selected directory.</td>
</tr>
<tr>
<td>Last Success Sync</td>
<td>The last date and time Safeguard successfully synchronized its database with the selected directory.</td>
</tr>
<tr>
<td>Last Failure Delete Sync</td>
<td>The last date and time Safeguard failed to synchronize deletions from the directory object properties.</td>
</tr>
<tr>
<td>Last Success Delete Sync</td>
<td>The last date and time Safeguard successfully synchronized deletions from the directory object properties.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last Failure Account Discovery</td>
<td>The date and time of the last failed account discovery job.</td>
</tr>
<tr>
<td>Last Success Account Discovery</td>
<td>The date and time of the last successful account discovery job.</td>
</tr>
</tbody>
</table>

**Table 89: Directories General tab: Attribute properties**

<table>
<thead>
<tr>
<th>Safeguard Attribute</th>
<th>Directory Attribute</th>
</tr>
</thead>
</table>

**User Attributes**

- **Object Class**: `inetOrgPerson`, the default user object class.
- **User Name**: `cn`, the user's common name.
- **Password**: `userPassword`, the user's password.
- **First Name**: `givenName`, the user's given name.
- **Last Name**: `sn`, the user's last name.
- **Work Phone**: `telephoneNumber`, the user's work telephone number.
- **Mobile Phone**: `mobile`, the user's primary mobile telephone number.
- **Email Address**: `mail`, the user's email address.
- **Description**: `description`, the description of the user.

**Computer Attributes**

- **Object Class**: `ipHost`, the default computer object class.
- **Name**: `cn`, the computer's common name.
- **Network Address**: `ipHostNumber`, the network DNS name or IP address of the LDAP server.
- **Operating System**: `operatingSystem`, the default operating system.
- **Operating System Version**: `operatingSystemVersion`, the default operating system version.
- **Description**: `description`, the description of the computer.

**Group Attributes**

- **Object Class**: `groupOfNames`, the default group object class.
- **Name**: `cn`, the group's common name.
### Safeguard Attribute Directory Attribute

<table>
<thead>
<tr>
<th>Safeguard Attribute</th>
<th>Directory Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
<td><em>member</em>, the group's member name.</td>
</tr>
<tr>
<td>Description</td>
<td><em>description</em>, the description of the group.</td>
</tr>
</tbody>
</table>

**NOTE:** For more information about how to synchronize the objects in Safeguard to directory schema attributes, see Adding a directory.

**Description:** Information about the selected directory.

#### Related Topics

Modifying a directory

---

## Accounts tab

The **Accounts** tab displays the user accounts associated with the selected directory.

### Table 90: Directories: Accounts tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of a user account you can use to log into the selected directory.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The forest root domain name for the selected directory.</td>
</tr>
<tr>
<td>Profile</td>
<td>The name of the profile that manages the selected directory account.</td>
</tr>
<tr>
<td>Service Account</td>
<td>A check in this column indicates that the selected account is a service account.</td>
</tr>
<tr>
<td>Password Request</td>
<td>A check in this column indicates that password release requests are enabled for this account.</td>
</tr>
<tr>
<td>Session Request</td>
<td>A check in this column indicates that session access requests are enabled for this account.</td>
</tr>
</tbody>
</table>

**NOTE:** Click (or tap) **Access Requests** from the details toolbar to enable or disable a user's ability to request access to the selected directory account.

**NOTE:** Click (or tap) **Access Requests** from the details toolbar to enable or disable a user's ability to request access to the selected directory account.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Needs a Password</td>
<td>Displays a if a password is not set for the selected directory account. For more information, see Setting directory account passwords on page 198.</td>
</tr>
<tr>
<td>Distinguished Name</td>
<td>The distinguished name for the selected directory.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the selected account.</td>
</tr>
</tbody>
</table>

**NOTE:** Safeguard may truncate the description when it imports the directory account if the description contains more than 255 characters.

When you add a directory, Safeguard adds its service account to the list of accounts in the **Accounts** tab. By default, Safeguard automatically manages the service account password according to the Check and Change settings in the profile that governs the directory. For more information, see Creating a directory profile on page 199. If you do not want Safeguard to manage the service account password, add the account to a profile that is set to never change passwords.

**NOTE:** When you add the directory, Safeguard automatically adds the service account to the directory’s **Accounts** tab and disables it for access requests. If you want the password to be available for release, click (or tap) **Access Requests** and select **Enable Password Request** from the details toolbar. If you want to enable session access, select **Enable Session Request**.

Use these buttons on the details toolbar to manage your directory accounts.

### Table 91: Directories: Accounts tab toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✉️ Add Account</td>
<td>Add directory accounts to the selected directory. For more information, see Adding directory accounts to a directory on page 193.</td>
</tr>
<tr>
<td>✗ Delete Selected</td>
<td>Remove the selected directory account. For more information, see Deleting a directory on page 203.</td>
</tr>
<tr>
<td>⚡ Refresh</td>
<td>Update the list of directory accounts.</td>
</tr>
<tr>
<td>🔍 Manage Discovery</td>
<td>Add or modify directory account discovery jobs. For more information, see Managing directory account discovery jobs on page 195.</td>
</tr>
<tr>
<td>🔒 Account Security</td>
<td>Menu options include: Check Password, Change Password, and Set Password. For more information, see Checking, changing, or setting an account password on page 110.</td>
</tr>
<tr>
<td>🔒 Password Archive</td>
<td>Display the password history for the selected directory</td>
</tr>
</tbody>
</table>
### Description

**Option**

- **Access Requests**: Select an option to enable or disable a user's ability to request the selected directory account's password or session access. Menu options include:
  - Enable Password Request
  - Disable Password Request
  - Enable Session Request
  - Disable Session Request

**Set Profile**: Select a profile to manage the selected directory account.

**Add to Account Groups**: Add the selected account to one or more account groups.

**Details**: View the general details and tags associated with the selected account.

**Search**: To locate a specific directory account or set of accounts in this list, enter the character string to be used to search for a match. For more information, see Search box on page 65.

### Profiles tab

The **Profiles** tab displays the profiles associated with the selected directory. For more information, see About profiles on page 233.

Click (or tap) **Create Profile** from the details toolbar to add a profile to the selected directory.

#### Table 92: Directories: Profiles tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Password management profile name.</td>
</tr>
<tr>
<td>Default</td>
<td>&quot;Default&quot; displays in this column for the default profile. For more information, see Setting a default directory profile on page 201.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the profile.</td>
</tr>
</tbody>
</table>

Use these buttons on the details toolbar to manage your directory profiles.
Table 93: Directories: Profiles tab toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Create Profile</td>
<td>Add a profile to the selected directory. For more information, see Creating a directory profile on page 199.</td>
</tr>
<tr>
<td>⌚️ Delete Selected</td>
<td>Remove the selected directory profile. For more information, see Deleting a directory on page 203.</td>
</tr>
<tr>
<td>⌚️ Refresh</td>
<td>Update the list of directory profiles.</td>
</tr>
<tr>
<td>✎ Edit Profile</td>
<td>Modify the selected directory profile. For more information, see Modifying a directory profile on page 200.</td>
</tr>
<tr>
<td>⚖️ Set as Default</td>
<td>Set the selected profile as the default directory profile. For more information, see Setting a default directory profile on page 201.</td>
</tr>
<tr>
<td>🕵️ Details</td>
<td>View additional details about the selected directory profile.</td>
</tr>
<tr>
<td>🔍 Search</td>
<td>To locate a specific directory profile or set of profiles in this list, enter the character string to be used to search for a match. For more information, see Search box on page 65.</td>
</tr>
</tbody>
</table>

Related Topics

Adding accounts to a directory profile
How do I see which assets and/or accounts are governed by a profile

About profiles

A profile is a set of configuration settings for a set of accounts in a partition or directory.

When you create a new partition or directory, Safeguard creates a corresponding default profile with default schedules and rules. You can create multiple profiles to govern the accounts assigned to a partition or directory. Both assets and accounts are assigned to the scope of a profile.

For example, suppose you have an asset with 12 accounts and you configure the profile to check and change passwords every 60 days. If you want the password managed for one of those accounts every 7 days, you can create another profile and add the individual account to the new profile. Now, Safeguard will check and change all the passwords on this asset every 60 days except for this account, which will change every 7 days.

Implicit and explicit association

It is important to understand the difference between implicit and explicit assignments to a profile.
Implicit associations

Safeguard makes implicit assignments. For example, when you add an asset to Safeguard, it automatically adds the asset to the default partition and assigns it to the scope of the default profile. This is called implicit association. Assets implicitly inherit the partition's default profile. Similarly, accounts inherit their parent asset’s profile. That means when you add an account to an asset, Safeguard implicitly adds that account to its asset’s profile. Later if you reassign the asset to another profile, Safeguard automatically reassigns all of the asset’s associated accounts to the new profile.

Explicit associations

Safeguard allows you to explicitly add an asset or an account to a specific profile. When you explicitly assign an asset to a profile, it overrides the implicit inheritance from the partition so the asset’s profile is no longer determined by its partition. Similarly, when you explicitly assign an account to a profile, Safeguard overrides the implicit inheritance from the asset and the account’s profile is no longer determined by its asset. Now if you reassign the asset to another profile, Safeguard will not reassign the asset’s associated accounts that were explicitly assigned to the old profile.

Resetting the default profile

If you set another profile as the default, Safeguard implicitly reassigns all assets and their associated accounts to that new default, but it will not reassign any assets or accounts that you have explicitly assigned to a profile. Once the implicit inheritance is broken, changing a partition’s (or directory's) default profile has no effect on the scope of a profile. For more information, see Setting a default partition profile or Setting a default directory profile.

Related Topics

Assigning assets or accounts to a partition profile
Adding accounts to a directory profile
Assigning a profile to an asset
Account Password Rules
How do I manage accounts on unsupported platforms
How do I see which assets and/or accounts are governed by a profile

Discovered Accounts tab

The Directories | Discovered Accounts tab allows you to add directory accounts to Safeguard as a result of any directory account discovery jobs that have run against the selected directory. For more information, see Directory account discovery job workflow on page 492.

The Discovered Accounts tab displays the following for the selected directory.
Table 94: Directories: Discovered Accounts tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Indicates Ignored or Managed or is blank for any directory account that you have not previously tagged as Ignore or Manage.</td>
</tr>
<tr>
<td>Account Name</td>
<td>The name of the discovered directory account.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The name of the domain where the discovered account resides.</td>
</tr>
<tr>
<td>Profile</td>
<td>The name of the profile that manages the account.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>The date and time when the account was discovered.</td>
</tr>
</tbody>
</table>

Use these buttons on the details toolbar to manage your discovered directory accounts.

Table 95: Directories: Discovered Accounts tab toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage</td>
<td>Select to add the selected account to the selected directory, and assign it to the scope of the default profile. For more information, see Setting a default directory profile on page 201.</td>
</tr>
<tr>
<td>Ignore</td>
<td>Select to prevent Safeguard from managing the selected directory account.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of discovered accounts.</td>
</tr>
<tr>
<td>Search</td>
<td>To locate a specific account or set of accounts in this list, enter the character string to be used to search for a match. For more information, see Search box on page 65.</td>
</tr>
</tbody>
</table>

**History tab**

The **History** tab allows you to view or export the details of each operation that has affected the selected directory.

The **History** tab contains the following information:

- **Items**: Total number of entries in the history log.
- **Search**: For more information, see Search box on page 65.
- **Time Frame**: By default the history details are displayed for the last 24 hours. Click (or tap) one of the time intervals at the top of the grid to display history details for a different time frame. If the display does not refresh after selecting a different time interval, click (or tap) **Refresh**.
Table 96: Directories: History tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>The date and time of the event.</td>
</tr>
<tr>
<td>User</td>
<td>The display name of the user that triggered the event.</td>
</tr>
<tr>
<td>Source IP</td>
<td>The network DNS name or IP address of the managed system that triggered the event.</td>
</tr>
<tr>
<td>Object Name</td>
<td>The name of the selected directory.</td>
</tr>
<tr>
<td>Event</td>
<td>The type of operation made to the selected directory:</td>
</tr>
<tr>
<td></td>
<td>- Create</td>
</tr>
<tr>
<td></td>
<td>- Delete</td>
</tr>
<tr>
<td></td>
<td>- Update</td>
</tr>
<tr>
<td></td>
<td>- Add Membership</td>
</tr>
<tr>
<td></td>
<td>- Remove Membership</td>
</tr>
</tbody>
</table>

**NOTE:** A membership operation indicates a "relationship" change with a related or parent object such as when you add or delete an account dependency. For more information, see Adding account dependencies on page 153.

<table>
<thead>
<tr>
<th>Related Object</th>
<th>The name of the related object.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related Object Type</td>
<td>The type of the related object.</td>
</tr>
<tr>
<td>Parent</td>
<td>The name of the object to which the selected directory is a child.</td>
</tr>
<tr>
<td>Parent Object Type</td>
<td>The parent object type.</td>
</tr>
</tbody>
</table>

Select an event to display this additional information for some types of events (for example, create and update events).

Table 97: Additional History tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>The property that was updated.</td>
</tr>
<tr>
<td>Old Value</td>
<td>The value of the property before it was updated.</td>
</tr>
<tr>
<td>New Value</td>
<td>The new value of the property.</td>
</tr>
</tbody>
</table>
Managing directories

Use the controls and tabbed pages on the Directories page to perform the following tasks to manage directories:

- Adding a directory
- Checking a directory's connectivity
- Adding directory accounts to a directory
- Managing directory account discovery jobs
- Setting directory account passwords
- Creating a directory profile
- Modifying a directory profile
- Setting a default directory profile
- Adding accounts to a directory profile
- Modifying a directory
- Deleting a directory

Adding a directory

It is the responsibility of the Directory Administrator to add directories to Safeguard.

Use the Directories view to add new directories to Safeguard.

To add a directory

1. Navigate to Administrative Tools | Directories.
2. Click (or tap) ✦ Add Directory from the toolbar.
3. In the Directory dialog, provide information in each of the tabs:

   | General tab                | Where you select the type of directory and add its service account information. |
   | Attributes tab             | Where you synchronize the attributes in Safeguard to the directory schema attributes. |

When you create a new directory, Safeguard creates a corresponding default profile with default schedules and rules.

- Select the profile and click (or tap) ✂ Edit Profile to add additional schedules and rules. For more information, see Creating a directory profile on page 199.
  -OR-
Modify the values of the default schedules and rules in **Settings**. See **Safeguard Access settings** and **Asset Management settings**.

**Related Topics**

- Adding directory accounts to a directory
- Adding accounts to a directory profile
- Modifying a directory

**General tab**

Use the **General** tab to specify the type of directory to be searched and add the required service account information.

**Table 98: Directory: General tab properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>Select a type of directory:</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Active Directory</td>
</tr>
<tr>
<td></td>
<td>- OpenLDAP 2.4</td>
</tr>
<tr>
<td><strong>Required</strong></td>
<td></td>
</tr>
<tr>
<td>Service Account</td>
<td>For Active Directory, enter the fully qualified Active Directory domain name, such as example.com.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Do not enter the domain controller hostname, such as server.example.com; the domain controller's IP address, such as 10.10.10.10; or the NETBIOS domain name, such as EXAMPLE.</td>
</tr>
<tr>
<td><strong>IMPORTANT</strong>: The service account domain name is the name of the domain where the service account resides. Safeguard uses DNS-SRV to resolve domain names to actual domain controllers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Limit: 255 characters</td>
</tr>
<tr>
<td></td>
<td><strong>Required</strong></td>
</tr>
<tr>
<td>Network Address</td>
<td>For OpenLDAP, enter a network DNS name or the IP address of the LDAP server for Safeguard to use to connect to the managed system over the network.</td>
</tr>
<tr>
<td></td>
<td>Limit: 255 characters</td>
</tr>
<tr>
<td></td>
<td><strong>Required</strong></td>
</tr>
<tr>
<td>Service Account</td>
<td>For Active Directory, enter an account for Safeguard to use for management tasks.</td>
</tr>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>When you add the directory, Safeguard automatically adds the service account to the directory’s <a href="#">Accounts</a> tab and disables it for access requests. If you want the password to be available for release, click (or tap) <a href="#">Access Requests</a> and select <a href="#">Enable Password Request</a> from the details toolbar. To enable session access, select <a href="#">Enable Session Request</a>.</td>
</tr>
<tr>
<td><strong>IMPORTANT:</strong></td>
<td>Add an account that has permission to read all of the domains and accounts that you want to manage with Safeguard. Safeguard is forest-aware. Using the service account you specify, Safeguard automatically locates all of the domains in the forest and creates a directory object which represents the entire forest. The directory object will have the same name as the forest-root domain regardless of which account you specify.</td>
</tr>
<tr>
<td>Required</td>
<td>For more information, see <a href="#">About service accounts</a> on page 140.</td>
</tr>
</tbody>
</table>

**Service Account Distinguished Name**

For OpenLDAP, enter a fully qualified distinguished name (FQDN) for Safeguard to use for management tasks. For example: `cn=dev-sa,ou=people,dc=example,dc=com`

- Required
- Limit: 255 characters

**Service Account Password**

Enter the password Safeguard uses to authenticate to this directory.

- Limit: 255 characters
- Required

**Description**

Enter information about this external identity provider.

- Limit: 255 characters

**Connect**

Click (or tap) Connect to verify the credentials and load the schema attributes for this directory.

**Advanced**

Open to reveal the following synchronization settings:

**Port**

For OpenLDAP, enter the port used for communication with the LDAP directory.

- LDAP uses port 389 for unencrypted connections and LDAPS uses port 636 for encrypted connections.
**Property** | **Description**
---|---

**IMPORTANT:** Safeguard must be able to communicate with the global catalog for directory management tasks including the addition of a directory account, a directory user account, or a directory user group. Standard global catalog ports are 3268 (LDAP) and 3269 (LDAPS).

**Use SSL Encryption** | For OpenLDAP, select to enable Safeguard to encrypt communication with an LDAP directory.

**Verify SSL Certificate** | For OpenLDAP, select to verify the SSL certificate.

**Sync additions every** | Enter or select how often you want Safeguard to synchronize directory additions (in minutes). This updates Safeguard with any additions, or modifications that have been made to the directory objects, including group membership and user account attributes mapped to Safeguard.

  - Default: 15 minutes
  - Range: Between 1 and 2147483647

**Sync deletions every** | Enter or select how often you want Safeguard to synchronize directory deletions (in minutes). This updates Safeguard with any deletions that have been made to the directory objects, including group membership and user account attributes mapped to Safeguard.

  - Default: 15 minutes
  - Range: Between 1 and 2147483647

---

**Attributes tab**

On the Attributes tab, synchronize the attributes in Safeguard to the directory schema attributes.

The Attributes tab displays the default directory attributes that are mapped to the Safeguard properties, such as the user’s first name.

**To map the Safeguard properties to different directory attributes**

1. **Browse** to select one or more object classes for the users, computers, and groups categories.

  **NOTE:** You can use or remove the default object class.
2. If you do not want to use the default property, begin typing in the property box. Safeguard’s auto-complete feature immediately displays a list of attributes to choose. Safeguard only allows you to choose attributes that are valid for the object classes you have selected for users, groups, and computers.

3. Once you have set all the properties, click (or tap) **Add Directory**.

The following tables list the default directory attributes.

**Table 99: Default directory attributes**

<table>
<thead>
<tr>
<th>Safeguard Attribute</th>
<th>Directory Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Users</strong></td>
<td></td>
</tr>
<tr>
<td>Object Class</td>
<td><strong>Browse</strong> to select a class definition that defines the valid attributes for the user object class. Default: <em>user</em> for Active Directory, <em>inetOrgPerson</em> for LDAP</td>
</tr>
<tr>
<td>User Name</td>
<td><em>sAMAccountName</em> for Active Directory, <em>cn</em> for LDAP</td>
</tr>
<tr>
<td>Password</td>
<td><em>userPassword</em> for LDAP</td>
</tr>
<tr>
<td>First Name</td>
<td><em>givenName</em></td>
</tr>
<tr>
<td>Last Name</td>
<td><em>sn</em></td>
</tr>
<tr>
<td>Work Phone</td>
<td><em>telephoneNumber</em></td>
</tr>
<tr>
<td>Mobile Phone</td>
<td><em>mobile</em></td>
</tr>
<tr>
<td>Email</td>
<td><em>mail</em></td>
</tr>
<tr>
<td>Description</td>
<td><em>description</em></td>
</tr>
<tr>
<td><strong>Computers</strong></td>
<td></td>
</tr>
<tr>
<td>Object Class</td>
<td><strong>Browse</strong> to select a class definition that defines the valid attributes for the computer object class. Default: <em>computer</em> for Active Directory, <em>ipHost</em> for LDAP</td>
</tr>
<tr>
<td>Name</td>
<td><em>cn</em></td>
</tr>
<tr>
<td>Network Address</td>
<td><em>dNSHostName</em> for Active Directory, <em>ipHostNumber</em> for LDAP</td>
</tr>
<tr>
<td>Operating System</td>
<td><em>operatingSystem</em> for Active Directory</td>
</tr>
<tr>
<td>Operating System Version</td>
<td><em>operatingSystemVersion</em> for Active Directory</td>
</tr>
<tr>
<td>Description</td>
<td><em>description</em></td>
</tr>
<tr>
<td><strong>Groups</strong></td>
<td></td>
</tr>
<tr>
<td>Object Class</td>
<td><strong>Browse</strong> to select a class definition that defines the valid attributes for the group object class.</td>
</tr>
<tr>
<td>Safeguard Attribute</td>
<td>Directory Attribute</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Default: group for Active Directory, groupOfNames for LDAP</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>sAMAccountName for Active Directory, cn for LDAP</td>
</tr>
<tr>
<td>Member</td>
<td>member</td>
</tr>
<tr>
<td>Description</td>
<td>description</td>
</tr>
</tbody>
</table>

### Checking a directory's connectivity

After you add a directory you can verify that Safeguard can log into it using the **Check Connection** option.

1. **NOTE:** When you run **Connect** from the directory's **General** tab (such as when you add the directory initially), you must enter the service account credentials. Once you add the directory to Safeguard it saves these credentials.
   
The **Check Connection** option does not require that you enter the service account credentials because it uses the saved credentials to verify that it can log into that asset.

   **To check a directory's connectivity**
   1. Navigate to **Administrative Tools** | **Directories**.
   2. From **Directories**, right-click a directory to open its context menu.
   3. Choose the **Check Connection** option.
      
      Safeguard displays a Toolbox task pane that shows the results.

### Related Topics

- About Test Connection
- About service accounts

### Adding directory accounts to a directory

This topic explains how to add a directory account to a directory. Safeguard also allows you to set up directory account discovery jobs that run automatically each time it synchronizes the directory. For more information, see **Directory account discovery job workflow** on page 492.

1. **NOTE:** You must add a directory to Safeguard before you can add directory accounts.
IMPORTANT: Ensure that you add accounts that you want Safeguard to manage. If you add directory user accounts to a directory, Safeguard will automatically change the user passwords according to the directory profile schedule you set which could prevent a directory user from logging into Safeguard. For information about how to set up directory users as Safeguard users, see Adding a directory user account.

IMPORTANT: Safeguard must be able to communicate with the global catalog for directory management tasks including the addition of a directory account, a directory user account, or a directory user group. Standard global catalog ports are 3268 (LDAP) and 3269 (LDAPS).

To add directory accounts to a directory

1. Navigate to Administrative Tools | Directories.
2. In Directories, select a directory from the object list and open the Accounts tab.
3. Click (or tap) + Add Account from the details toolbar.
4. In the Find Accounts dialog, Browse to select a container within the directory as the Filter Search Location.
5. The Include objects from sub containers check box is selected by default indicating that child objects will be included in your search. Clear this check box to exclude child objects from your search.
6. In the Contains field, enter a full or partial account name and click (or tap) Search.
   To search for a directory account, you must enter text into the search box. Safeguard searches the entire forest root using the global catalog. You can search on partial strings. For example, if you enter "ad" in the Contains box, it will find any user Name or Distinguished Name that contains "ad".
   
   NOTE: The text search is not case sensitive and does not allow wild cards.
7. The results of the search displays in the Select the Account(s) to Add grid. Select one or more accounts to add to Safeguard.
8. Browse to select the Directory Profile you want to govern the accounts you added to Safeguard.
9. Click (or tap),
   a. OK to add the selected accounts to Safeguard.
   -OR-
   b. Reoccur to configure a directory account discovery job using the search criteria. For more information, see Managing directory account discovery jobs on page 195.

Related Topics

Adding account dependencies
Adding a directory
Adding accounts to a directory profile
Managing directory account discovery jobs

Safeguard allows you to set up directory account discovery jobs that run automatically each time it synchronizes the directory. For more information, see Directory account discovery job workflow on page 492.

To setup a directory account discovery job

1. Navigate to Administrative Tools | Directories.
2. From Directories select a directory from the object list and open the Accounts tab.
3. Click (or tap) ⚙ Manage Discovery from the details toolbar.
4. In the Manage Discovery dialog, click (or tap) + Add to open the Directory Account Discovery dialog.

   NOTE: This dialog also opens when you select Reoccur in the Find Accounts dialog. For more information, see Adding directory accounts to a directory on page 193.

5. Add information to these tabs:

   General tab
   Where you enter the directory account discovery job name and designate the directory profile to govern the accounts the discovery job adds to Safeguard.

   Rules tab
   Where you configure the search criteria for the discovery job.

General tab

Use the Directory Account Discovery General tab to specify the following details about the discovery job.

Table 100: Directory Account Discovery: General tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the directory account discovery job.</td>
</tr>
<tr>
<td></td>
<td>Limit: 50 characters</td>
</tr>
<tr>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the directory account discovery job.</td>
</tr>
<tr>
<td></td>
<td>Limit: 255 characters</td>
</tr>
<tr>
<td>Directory Profile</td>
<td>Browse to select the Directory Profile you want to govern the accounts the discovery job adds to Safeguard.</td>
</tr>
</tbody>
</table>
Rules tab

Use the Directory Account Discovery Rules tab to define the search criteria to be used to discover directory accounts.

NOTE: When using the Property Constraint search option, if multiple values are entered for an individual property (for example, GID), Safeguard uses the ‘OR’ operator and returns accounts that match any of the specified values.

However, when search values are entered for multiple properties (for example, RID and GID), Safeguard first evaluates the search criteria for each individual property and then chains the results of each individual search using the ‘AND’ operator, returning only those accounts that meet all of the search properties specified.

To define a new directory account discovery rule

1. Click (or tap) + Add from the details toolbar.
2. Provide the following in the Rule dialog:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the directory account discovery rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Limit: 50 characters; cannot contain special characters such as an apostrophe.</td>
</tr>
<tr>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>Find By</td>
<td>Choose one of these search options and enter the search criteria to be used:</td>
</tr>
<tr>
<td>a. Name</td>
<td>Select this option to search by account name.</td>
</tr>
<tr>
<td></td>
<td>· Filter Search Location: Browse to select a container to search within the directory.</td>
</tr>
<tr>
<td></td>
<td>· Contains: Type a full or partial account name.</td>
</tr>
<tr>
<td></td>
<td>NOTE: You can only enter a single string (full or partial account name) at a time. For example, entering &quot;t&quot; will return all account names that begin with the letter &quot;t&quot;: Timothy, Tom, Ted, and so on. But entering &quot;Tim, Tom, Ted&quot; will return no results.</td>
</tr>
<tr>
<td>b. Group</td>
<td>Select this option to search by group name.</td>
</tr>
<tr>
<td></td>
<td>· Click (or tap) + Add to launch the Group dialog.</td>
</tr>
<tr>
<td></td>
<td>· Contains: Enter a full or partial group name and click (or tap) Search.</td>
</tr>
</tbody>
</table>
NOTE: You can only enter a single string (full or partial group name) at a time.

- **Filter Search Location**: Browse to select a container to search within the directory.
- **Include objects from sub containers**: Select this check box to include child objects.
- **Select the group to add**: The results of the search displays in this grid. Select one or more groups to add to the discovery job.

c. **Property Constraint**

Select this option to search for accounts based on an account’s property.

- **Filter Search Location**: Browse to select a container to search within the directory.
- **RID**: Enter one or more Relative Identifier numbers. To enter multiple IDs or ID ranges, you must enter each element of the list separately. For example: enter 1000, enter 5000-7000, then enter 10000.

  NOTE: Spaces and commas are not allowed.

  Limit: 255 numeric characters

  NOTE: RID property only applies to Microsoft Active Directory.

- **GID**: Enter one or more Group Identifier numbers. To enter multiple IDs or ID ranges, you must enter each element of the list separately. For example: enter 8, enter 10-12, then enter 15.

  NOTE: Spaces and commas are not allowed.

  Limit: 255 numeric characters

- **UID**: Enter one or more User Identifier numbers. To enter multiple IDs or ID ranges, you must enter each element of the list separately. For example: enter 1, enter 5-7, then enter 10.

  NOTE: Spaces and commas are not allowed.

  Limit: 255 numeric characters
• **Name:** Enter a single regular expression pattern.

  ![NOTE: For more information, see Regular Expression Language - Quick Reference.]

  Limit: 255 alphanumeric characters

• **Group:** Enter a single regular expression pattern.

  ![NOTE: For more information, see Regular Expression Language - Quick Reference.]

  Limit: 255 alphanumeric characters

d. **LDAP Filter**

   Select this option to search for accounts using an LDAP query.

   • **Filter Search Location:** Browse to select a container to search within the directory.

   • **LDAP Filter:** Type an LDAP query into the field.

e. **Find All**

   This option is selected by default and will find all accounts in the selected directory.

   • **Filter Search Location:** Browse to select a container to search within the directory.

| Preview | Click (or tap) Preview, to verify the rule. The Preview button displays a list of directory accounts Safeguard will find based on the criteria you set in this rule. |

3. Optionally select the **Automatically Manage Found Accounts** option to automatically add the discovered accounts to Safeguard.

4. Click (or tap) **Add Discovery** to save the discovery rule.

Safeguard runs the directory account discovery job according to the directory’s **Synchronization Interval**, and displays the accounts it finds in the directory’s **Discovered Accounts tab**.

![NOTE: You can view or modify the Synchronization Interval on the directory’s General tab.]

### Setting directory account passwords

When you set an account password you are manually setting the account password in the Safeguard database so Safeguard can synchronize it with the password in the external identity provider, such as Microsoft Active Directory.

It is the responsibility of the Directory Administrator to set directory account passwords.
To set directory account passwords

1. Navigate to Administrative Tools | Directories.
2. In Directories, select a directory from the object list and open the Accounts tab.
3. Select one or more accounts that require a password, indicated by the symbol in the Needs a Password column.
4. Click (or tap) Account Security from the details toolbar and select Set Password.
5. The Set Password option provides two options:
   a. Generate Password - select this option to have Safeguard generate a new random password, that complies with the password rule that is set in the account's profile.
      - Click (or tap) Generate Password to display the Generate Password dialog.
      - Click (or tap) Show Password to reveal the new password.
      - Click (or tap) Copy to put it into your copy buffer.
      - Log into your device, using the old password, and change it to the password in your copy buffer.
      - Click (or tap) OK to change the password in the Safeguard database or click (or tap) Cancel to close the dialog without changing the current password in Safeguard.
   b. Manual Password - select this option to manually set the account password in the Safeguard database.
      - Click (or tap) Manual Password to display the Set Password dialog.
      - In the Set Password dialog, enter the password and click (or tap) OK. Clicking OK updates the Safeguard database.
      - Set the account password on the physical device to synchronize it with the Safeguard database.

Creating a directory profile

A directory profile is similar to a partition profile, only it governs the accounts assigned to a directory. For more information, see About profiles on page 233.

It is the responsibility of the Directory Administrator to add profiles to directories.

To add a profile to a directory

1. Navigate to Administrative Tools | Directories.
2. In Directories, select a directory from the object list and open the Profiles tab.
3. Click (or tap) + Create Profile from the details toolbar.
4. On the **General** tab, enter the following information:
   a. **Name**: Enter a unique name for the profile.  
      Limit: 50 characters
      Required
   b. **Description**: Enter information about this profile.  
      Limit: 255 characters

   **NOTE**: The options on the following tabs are read-only. You change the options in Settings at the links provided below.

5. On the **Check Password** tab, select a check password setting or click (or tap) + to create one. For more information, see Adding directory check password settings on page 353.

   *Directory Check Password Settings* are the rules Safeguard uses to verify directory account passwords.

6. On the **Change Password** tab, select a change password setting or click (or tap) + to create one. For more information, see Adding directory change password settings on page 351.

   *Directory Change Password Settings* are the rules Safeguard uses to reset directory account passwords.

7. On the **Account Password Rules** tab, select a directory account password rule or click (or tap) + to create one. For more information, see Adding a directory account password rule on page 348.

   This is a complexity rule that governs the construction of the new password created by Safeguard during an automatic password change.

   **NOTE**: You can expand the **Description** to see information about the account password rule.

**Related Topics**

Adding accounts to a directory profile
Setting a default directory profile
Account Password Rules

**Modifying a directory profile**

**NOTE**: Any modifications that you make to a directory profile affects all the accounts governed by that profile.
**To modify a directory profile**

1. Navigate to Administrative Tools | Directories.
2. In Directories, select a directory from the object list and open the Profiles tab.
3. Select a profile:
   a. To modify the settings or rules, either double-click (or double-tap) the profile or click (or tap) the Edit Profile icon.
   b. To add accounts to the profile, click (or tap) the Details icon and switch to the Accounts tab of the details window.

**Related Topics**

Adding a directory
Adding directory accounts to a directory

**Setting a default directory profile**

When you create a new directory, Safeguard creates a corresponding default profile with default schedules and rules.

**NOTE:** Safeguard sets the default schedules to "Never" verify or reset passwords. To change the settings, see Modifying a directory profile.

**To set another profile as the default**

1. Navigate to Administrative Tools | Directories.
2. In Directories, select a directory from the object list and open the Profiles tab.
3. Select a profile and click (or tap) Set as Default from the details toolbar or context menu.

**NOTE:** All accounts that are not explicitly assigned to the default profile are automatically reassigned to the new default profile.

**Adding accounts to a directory profile**

This topic explains how to add an account to a directory profile. You can also configure Safeguard to run automatic account discovery jobs. For more information, see Directory account discovery job workflow on page 492.

**IMPORTANT:** Ensure that you add accounts to a directory profile that you want Safeguard to manage. If you add directory user accounts to a directory profile, Safeguard will automatically change the user passwords according to the change password schedule you set in the directory profile which could prevent a directory user from logging into Safeguard.
To add accounts to a directory profile

1. Navigate to Administrative Tools | Directories.
2. In Directories, select a directory from the object list and open the Profile tab.
3. Select a profile and click (or tap) Details from the details toolbar.
4. On the Accounts tab, click (or tap) Assign Account to Profile
5. On the Account dialog, choose one or more accounts.

**NOTE:** A directory profile's Accounts tab only displays accounts that have been added to the selected directory.

**NOTE:** If you delete a profile, Safeguard reassigns all assets and accounts to the default profile.

Related Topics

Adding a directory
Setting a default directory profile

Modifying a directory

To modify a directory

1. Navigate to Administrative Tools | Directories.
2. In Directories, select a directory from the object list.
3. Select the view of the directory's information you want to modify (General, Accounts, or Profiles).

For example

- To change a directory's description, double-click (or double-tap) the General information on the General tab or click (or tap) the Edit icon.

  **NOTE:** You can also double-click (or double-tap) a directory name to open the General settings edit window.

- To add accounts to the directory, switch to the Accounts tab. For more information, see Adding directory accounts to a directory on page 193.

- To modify the password validation and reset settings, switch to the Profiles tab, select a profile and click (or tap) the Edit icon. For more information, see Creating a directory profile on page 199.

4. To view or export the details of each operation that has affected the selected directory, switch to the History tab.
Deleting a directory

**NOTE:** The Directory Administrator cannot delete a directory that has active access requests. However, it is the responsibility of the Security Policy Administrator to manage access requests.

**To delete a directory**

1. Navigate to *Administrative Tools | Directories*.
2. In *Directories*, select a directory from the object list.
3. Click (or tap) **Delete Selected**.
4. Confirm your request.
Entitlements

A Safeguard entitlement is a set of access request policies that restrict system access to authorized users. Typically you create entitlements for various job functions; that is, you assign permissions to perform certain operations to specific roles such as Help desk, Unix administrator, or Oracle administrator, and so forth. Password release entitlements consist of users, user groups, and access request policies. Session request entitlements consist of users, user groups, assets, asset groups, and access request policies.

The Auditor and the Security Policy Administrator have permission to access Entitlements.

NOTE: To search for a particular entitlement, see Search box on page 65.

The Entitlements view displays the following information about the selected entitlement:

NOTE: Safeguard displays a ▲ next to an entitlement name when it expires or when the entitlement contains at least one expired policy. You can configure Safeguard to notify you of an impending entitlement or policy expiration by sending an event notification to a syslog server, in an email message, or a SNMP trap. For more information, see External Integration settings on page 317.

Table 101: Entitlements: Tabs

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td>Displays the general and time restriction settings information for the selected entitlement.</td>
</tr>
<tr>
<td>Users tab</td>
<td>Displays the users and user groups who are authorized to request access to the accounts or assets in the scope of the selected entitlement's policies.</td>
</tr>
<tr>
<td>Access Request Policies tab</td>
<td>Displays the access request policies that govern the accounts or assets in the selected entitlement.</td>
</tr>
<tr>
<td>History tab</td>
<td>Displays the details of each operation that has affected the selected entitlement.</td>
</tr>
</tbody>
</table>
Use these toolbar buttons to manage entitlements.

**Table 102: Entitlements: Toolbar**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Entitlement</td>
<td>Add entitlements to Safeguard. For more information, see Adding an entitlement on page 210.</td>
</tr>
<tr>
<td>Delete Selected</td>
<td>Remove the selected entitlement. For more information, see Deleting an entitlement on page 227.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of entitlements.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Modifying an entitlement
- Creating an access request policy
- Modifying an access request policy
- Deleting an access request policy

**General tab**

The **General** tab lists information about the selected entitlement.

Large tiles at the top of the tab display the number of **Users, Accounts** and **Assets** associated with the selected entitlement. Clicking a tile heading opens the corresponding tab.

**Table 103: Entitlements General tab: General properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The entitlement name.</td>
</tr>
<tr>
<td>Priority</td>
<td>A unique number that determines the processing order of the entitlement in relation to other entitlements. For more information, see About priority precedence on page 211.</td>
</tr>
</tbody>
</table>

**Table 104: Entitlements General tab: Time restrictions properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Restrictions</td>
<td>The days and times this entitlement is in effect. For more information, see About time restrictions on page 212.</td>
</tr>
<tr>
<td>Expires</td>
<td>The day and time this entitlement expires.</td>
</tr>
</tbody>
</table>

**Description:** Information about the selected entitlement.
Related Topics

Modifying an entitlement

Users tab

The **Users** tab displays the users and user groups who are authorized to request access for the accounts and assets in the scope of the selected entitlement's policies.

Click (or tap) **Add User or User Group** from the details toolbar to add one or more "requester" users or user groups to the selected entitlement.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Type of member:</td>
</tr>
<tr>
<td></td>
<td>• Group</td>
</tr>
<tr>
<td></td>
<td>• User</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Name of the user or user group included in the selected entitlement.</td>
</tr>
<tr>
<td><strong>Provider</strong></td>
<td>The name of the authentication provider:</td>
</tr>
<tr>
<td></td>
<td>• Local</td>
</tr>
<tr>
<td></td>
<td>• Certificate</td>
</tr>
<tr>
<td></td>
<td>• The name of an external provider such as a Microsoft Active Directory domain name.</td>
</tr>
</tbody>
</table>

Use these buttons on the details toolbar to manage the "requester" users associated with the selected entitlement.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add User or User Group</strong></td>
<td>Add a &quot;requester&quot; user or user group to the entitlement. For more information, see Adding users or user groups to an entitlement on page 213.</td>
</tr>
<tr>
<td><strong>Remove Selected</strong></td>
<td>Remove the selected user or user group from the entitlement.</td>
</tr>
<tr>
<td><strong>Refresh</strong></td>
<td>Update the list of &quot;requester&quot; users or user groups.</td>
</tr>
<tr>
<td><strong>Details</strong></td>
<td>View additional details about the selected user or user group.</td>
</tr>
</tbody>
</table>
### Access Request Policies tab

The **Policies** tab displays the password release policies that govern the accounts in the selected entitlement.

Click (or tap) **Create Access Policy** from the details toolbar to add a policy to the selected entitlement.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>A unique number that determines the processing order of the policy. For more information, see About priority precedence on page 211.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the access request policy.</td>
</tr>
<tr>
<td>Access Type</td>
<td>Indicates the type of access requested:</td>
</tr>
<tr>
<td></td>
<td>- Password Release</td>
</tr>
<tr>
<td></td>
<td>- RDP</td>
</tr>
<tr>
<td></td>
<td>- SSH</td>
</tr>
<tr>
<td>Scope</td>
<td>The number of unique account groups, accounts (including the number of accounts in the specified account groups), asset groups, and assets (including the number of assets in the specified asset groups) governed by the selected policy.</td>
</tr>
<tr>
<td>Expired</td>
<td>&quot;Expired&quot; displays in this column for an expired policy.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the selected policy.</td>
</tr>
</tbody>
</table>

**NOTE:** Safeguard displays a ▲ next to an entitlement name when it contains at least one expired policy.
Use these buttons on the details toolbar to manage your access request policies.

### Table 108: Entitlements: Access Request Policies tab toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>➕ Create Access Policy</td>
<td>Add an access request policy to the selected entitlement. For more information, see Creating an access request policy on page 214.</td>
</tr>
<tr>
<td>остоя Delete Selected</td>
<td>Remove the selected policy from the selected entitlement. For more information, see Deleting an access request policy on page 225.</td>
</tr>
<tr>
<td>⇌ Refresh</td>
<td>Update the list of access request policies.</td>
</tr>
<tr>
<td>📝 Edit Access Policy</td>
<td>Modify the selected policy. For more information, see Modifying an access request policy on page 226.</td>
</tr>
<tr>
<td>🔗 Copy Access Policy</td>
<td>Make a copy of the selected policy. For more information, see Copying an access request policy on page 226.</td>
</tr>
<tr>
<td>🔍 Details</td>
<td>View additional details about the selected policy. For more information, see Viewing policy details on page 226.</td>
</tr>
<tr>
<td>🔍 Search</td>
<td>To locate a specific policy or set of policies in this list, enter the character string to be used to search for a match. For more information, see Search box on page 65.</td>
</tr>
</tbody>
</table>

### History tab

The **History** tab allows you to view or export the details of each operation that has affected the selected entitlement.

The **History** tab contains the following information:

**Items**: Total number of entries in the history log.

**Search**: For more information, see Search box on page 65.

**Time Frame**: By default the history details are displayed for the last 24 hours. Click (or tap) one of the time intervals at the top of the grid to display history details for a different time frame. If the display does not refresh after selecting a different time interval, click (or tap) **Refresh**.

### Table 109: Entitlements: History tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>The date and time of the event.</td>
</tr>
<tr>
<td>User</td>
<td>The display name of the user that triggered the event.</td>
</tr>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th><strong>Property</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>The network DNS name or IP address of the managed system that triggered the event.</td>
</tr>
<tr>
<td>Object Name</td>
<td>The name of the selected entitlement.</td>
</tr>
<tr>
<td>Event</td>
<td>The type of operation made to the selected entitlement:</td>
</tr>
<tr>
<td></td>
<td>- Create</td>
</tr>
<tr>
<td></td>
<td>- Delete</td>
</tr>
<tr>
<td></td>
<td>- Update</td>
</tr>
<tr>
<td></td>
<td>- Add Membership</td>
</tr>
<tr>
<td></td>
<td>- Remove Membership</td>
</tr>
</tbody>
</table>

**NOTE:** A membership operation indicates a "relationship" change with a related or parent object such as a user or user group was added or removed from the membership of an entitlement.

<table>
<thead>
<tr>
<th><strong>Property</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Related Object</td>
<td>The name of the related object.</td>
</tr>
<tr>
<td>Related Object Type</td>
<td>The type of the related object.</td>
</tr>
<tr>
<td>Parent</td>
<td>The name of the object to which the selected entitlement is a child.</td>
</tr>
<tr>
<td>Parent Object Type</td>
<td>The parent object type.</td>
</tr>
</tbody>
</table>

Select an event to display this additional information for some types of events (for example, create and update events).

### Table 110: Additional History tab properties

<table>
<thead>
<tr>
<th><strong>Property</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>The property that was updated.</td>
</tr>
<tr>
<td>Old Value</td>
<td>The value of the property before it was updated.</td>
</tr>
<tr>
<td>New Value</td>
<td>The new value of the property.</td>
</tr>
</tbody>
</table>

### Managing entitlements

Use the controls and tabbed pages on the **Entitlements** page to perform the following tasks to manage Safeguard entitlements:

- Adding an entitlement
- Adding users or user groups to an entitlement
- Creating an access request policy
- Deleting an access request policy
- Modifying an access request policy
- Copying an access request policy
- Viewing policy details
- Modifying an entitlement
- Deleting an entitlement

## Adding an entitlement

It is the responsibility of the Security Policy Administrator to add entitlements to Safeguard.

**To add an entitlement**

1. Navigate to Administrative Tools | Entitlements.
2. Click (or tap) Add Entitlement from the toolbar.
3. In the Entitlement dialog, provide information in each of the tabs:

<table>
<thead>
<tr>
<th>General tab</th>
<th>Where you add general information about the entitlement.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Restrictions tab</td>
<td>Where you indicate entitlement time restrictions.</td>
</tr>
</tbody>
</table>

## Related Topics

Adding users or user groups to an entitlement

### General tab

On the General tab, specify the following information about the entitlement.

**Table 111: Entitlement: General tab properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the entitlement.</td>
</tr>
<tr>
<td></td>
<td>Limit: 50 characters</td>
</tr>
<tr>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>Description</td>
<td>Enter descriptive text about the entitlement.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Limit</td>
<td>255 characters</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority of this entitlement compared to other entitlements. If a user desires to access an account in the scope of two different entitlements, then the entitlement with the highest priority (that is, the lowest number) takes precedence. For more information, see About priority precedence on page 211.</td>
</tr>
</tbody>
</table>

**About priority precedence**

An entitlement defines which users are authorized to checkout passwords for accounts in the scope of its policies. A policy defines scope (that is, which accounts) and the rules for checking out passwords, such as the duration, how many approvals are required, and so forth.

It is possible for an account to be governed by more than one entitlement, or is in the scope of more than one policy within an entitlement. Safeguard uses both entitlement and policy priorities to determine which policy to use for a password release. Safeguard first considers the entitlement priority, then the priorities of access request policies within that entitlement.

**Example scenario:**

- Entitlement A (priority 1)
  - Policy: "Week Day Policy".
    - Policy time restrictions: Monday through Friday 8:00 a.m. to 5:00 p.m.
    - Scope: AccountX

- Entitlement B (priority 2)
  - Policy 1: "Sunday AM" (priority 1)
    - Policy time restrictions: Sunday 8:00 to 12:00.
    - Scope: AccountX
  - Policy 2: "Sunday PM" (priority 2)
    - Policy time restrictions: Sunday 13:00 to 17:00.
    - Scope: AccountX

Notice that AccountX is in the scope of all three of these policies.

If a user requests the password for AccountX for Sunday at 4 p.m., Safeguard first considers Entitlement A because it is priority 1. When it determines that the policy time restrictions prevent the password release, it then considers Entitlement B.

Safeguard first considers Entitlement B’s priority 1 policy. When it determines that the time restrictions prevent the password release, it then considers Policy 2. Once the request is satisfied, Safeguard grants the request.
To change an entitlement’s priority

1. Select the priority number in the entitlement list.
2. Enter another number.

To modify a policy’s priority

1. In Entitlements, select an entitlement and switch to the Access Request Policies tab.
2. Double-click (or double-tap) a policy, or select a policy and click (or tap) Edit Access Policy.
3. Enter or select a new priority number.
4. Click the Refresh button.

Time Restrictions tab

Time restrictions control when the entitlement is in effect relative to the user’s time zone. For more information, see About time restrictions on page 212.

On the Time Restrictions tab, specify the time restriction properties for the entitlement.

Table 112: Entitlement: Time Restrictions tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Time Restrictions</td>
<td>Select this option to enforce time restrictions.</td>
</tr>
<tr>
<td>Daily calendar</td>
<td>Select and drag the hours you want to allow.</td>
</tr>
<tr>
<td>Have the Entitlement Expire on Date and Time</td>
<td>Select this option to enforce an expiration date, then enter the date and time. When an entitlement expires, all the access request policies associated with the entitlement also expire. To set an expiration date on a policy, see Creating an access request policy.</td>
</tr>
</tbody>
</table>

About time restrictions

An entitlement’s time restrictions enforce when Safeguard uses a policy; a policy’s time restrictions enforce when a user can access the account passwords. If the entitlement and the policy both have time restrictions, the user can only check out the password for the overlapping time frame.

Time restrictions control when the entitlement or policy is in effect relative to a user’s time zone. Although Safeguard appliances run on Coordinated Universal Time (UTC), the user’s time zone enforces the time restrictions set in the entitlement or policy. This means that if
the appliance and the user are in different time zones, Safeguard enforces the policy in the user’s time zone set in his account profile.

**Adding users or user groups to an entitlement**

When you add users to an entitlement, you are specifying which people can request passwords to the accounts governed by the selected entitlement’s access request policies, or which people can request sessions for the accounts and assets governed by the selected entitlement’s access request policies.

**NOTE:** It is the responsibility of the Security Policy Administrator to add users to entitlements.

**To add "requester" users to an entitlement**

1. Navigate to Administrative Tools | Entitlements.
2. In Entitlements, select an entitlement from the object list and open the Users tab.
3. Click (or tap) + Add User or User Group from the details toolbar.
4. Select one or more users or user groups from the list in the Users/User Groups selection dialog, and click (or tap) OK.

**NOTE:** You can also double-click (or double-tap) a name to add it.

If you do not see the user or user group you are looking for, depending on your Administrator permissions, you can create them in the Users/User Groups selection dialog. (You must have Authorizer Administrator or User Administrator permissions to create users; or Security Policy Administrator permissions to create user groups.)

**To create new users or user groups in the Users/User Groups selection dialog**

1. Click (or tap) + Create New, then select Create a New User or Create a New User Group.

   For more information about creating users or user groups, see Adding a user or Adding a user group.

   **NOTE:** The Security Policy Administrator only has permission to add groups, not users. For more information, see Administrator permissions on page 421.

2. Create additional users or user groups, as required.
3. Click (or tap) OK in the Users/User Groups selection dialog to add the new users and user groups to the selected entitlement’s membership.
Creating an access request policy

It is the responsibility of the Security Policy Administrator to define access request policies in Safeguard.

A policy defines the scope (that is, which assets, asset groups, accounts, or account groups), the access type (that is, password, SSH or remote desktop), and the rules for checking out passwords, such as the duration, how many approvals are required, and so forth.

NOTE: An access request policy is only used in the entitlement in which it is created. If you delete an entitlement, Safeguard deletes all access request policies associated with that entitlement. You cannot copy an access request policy and add it to another entitlement; access request policies are entitlement-specific.

To add an access request policy to an entitlement

1. Navigate to Administrative Tools | Entitlements.
2. In Entitlements, select an entitlement from the object list and open the Access Request Policies tab.
3. Click (or tap) Create Access Policy from the details toolbar.
4. In the Access Request Policy dialog, provide information in each of the tabs:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td>Where you add general information about the access request policy as well as specify the type of access being requested.</td>
</tr>
<tr>
<td>Scope tab</td>
<td>Where you assign assets, asset groups, accounts, or account groups to an access request policy.</td>
</tr>
<tr>
<td>Requester tab</td>
<td>Where you configure the access request policy requester settings.</td>
</tr>
<tr>
<td>Approver tab</td>
<td>Where you configure the access request policy approver settings.</td>
</tr>
<tr>
<td>Reviewer tab</td>
<td>Where you configure the access request policy reviewer settings.</td>
</tr>
<tr>
<td>Access Config tab</td>
<td>Where you define the access settings for the selected type of request.</td>
</tr>
<tr>
<td>Session Settings tab</td>
<td>Where you configure the recording settings for session access requests.</td>
</tr>
<tr>
<td>Time Restrictions tab</td>
<td>Where you indicate policy time restrictions.</td>
</tr>
<tr>
<td>Emergency tab</td>
<td>Where you enable emergency access for the accounts governed by the access request policy.</td>
</tr>
</tbody>
</table>

Safeguard 2.3 Administration Guide
Entitlements
Related Topics
Deleting an access request policy
Modifying an access request policy
Copying an access request policy
Viewing policy details

Reasons

General tab

On the General tab, enter the following information for the access request policy.

Table 113: Access Request Policy: General tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the access request policy.</td>
</tr>
<tr>
<td></td>
<td>Limit: 50 characters</td>
</tr>
<tr>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>Description</td>
<td>Enter descriptive text that explains the access request policy.</td>
</tr>
<tr>
<td></td>
<td>Limit: 255 characters</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority of this policy compared to other policies in this entitlement.</td>
</tr>
<tr>
<td></td>
<td>If a user desires to access an account in the scope of two different request polices within an entitlement, then the policy with the</td>
</tr>
<tr>
<td></td>
<td>highest priority (that is, the lowest number) takes precedence. For more information, see About priority precedence on page 211.</td>
</tr>
<tr>
<td>Access Type</td>
<td>Specify the type of access being requested:</td>
</tr>
<tr>
<td></td>
<td>• Password Release</td>
</tr>
<tr>
<td></td>
<td>• RDP</td>
</tr>
<tr>
<td></td>
<td>• SSH</td>
</tr>
</tbody>
</table>

**NOTE:** You can configure an access request policy for a password release, however, if the Privileged Passwords module license is not installed, you will not be able to submit a password release request.

Similarly, you can configure an access request policy for a session request, but if the Privileged Sessions module license is not installed, you will not be able to initiate an RDP or SSH session request.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have the Policy Expire on Date and Time</td>
<td>If applicable, select this check box to enforce an expiration date for the policy. Enter the expiration date and time.</td>
</tr>
</tbody>
</table>

**Scope tab**

Use the Scope tab to assign accounts, account groups, assets and asset groups to an access request policy.

1. **On the Scope tab,**
   a. Click (or tap) **Add** from the details toolbar and select one of the following options:
      - Add Account Group
      - Add Account
      - Add Asset Group
      - Add Asset
      
      **NOTE:** Add Asset Group and Add Asset are only available for a session access request (that is, when access type RDP or SSH is selected on the General tab).
   b. In the selection dialog, choose one or more accounts, account groups, assets, or asset groups.
      
      **NOTE:** When adding accounts to a policy, both asset and directory accounts can be selected for a password release request policy; however, only asset accounts can be selected for an RDP or SSH sessions request policy.
   c. Click (or tap) **OK** to save your selection and close the dialog.

2. Repeat step one to add additional account groups, accounts, asset groups, or assets.

   **NOTE:** You can add multiple types of objects to a policy; however, you can only add one type of object (accounts, account groups, assets or asset groups) at a time.

All of the accounts, account groups, assets and asset groups selected appear on the Scope tab in the Access Request Policy dialog. To remove an object from the list, select the object and click (or tap) **Delete**.
**Requester tab**

Use the **Requester** tab to configure the requester settings for an access request policy.

**Table 114: Access Request Policy: Requester tab properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reasons</td>
<td>Click (or tap) + <strong>Select Reason</strong> to add reasons to the selected access request policy. Then when requesting access to a password or a session, a user can select a predefined reason from a list. <strong>NOTE:</strong> You must have reasons configured in Safeguard to use this option. For more information, see Reasons on page 249. If you do not see the reason you are looking for, you can create a reason from the Reasons selection dialog by clicking the + <strong>Create New</strong> toolbar button.</td>
</tr>
<tr>
<td>Require Reason</td>
<td>Select this check box to require that a requester provide a <strong>Reason</strong> when requesting access. If you add reasons to a policy, and leave this option cleared, the users will have the option of choosing a reason; but they will not be required to select a reason. <strong>NOTE:</strong> This option is only available if you have selected Reasons for the policy.</td>
</tr>
<tr>
<td>Require Comment</td>
<td>Select this check box to require that a requester provide a <strong>Comment</strong> when making an access request.</td>
</tr>
<tr>
<td>Require Ticket Number</td>
<td>Select this check box to require that a requester provide a ticket number when making an access request. <strong>NOTE:</strong> You must have the ticketing system configured in Safeguard to use this option. For more information, see Ticketing on page 338.</td>
</tr>
<tr>
<td>Duration of Access Approval</td>
<td>Enter or select the default duration (days, hours, and minutes) that the requester can access the accounts and assets governed by this policy. <strong>NOTE:</strong> The access duration cannot exceed a total of 7 days (10080 minutes).</td>
</tr>
<tr>
<td>Allow Requester to Change Duration</td>
<td>Select this check box to allow the requester the ability to modify the access duration.</td>
</tr>
<tr>
<td>Maximum Time Requester Can Have Access</td>
<td>If you select the <strong>Allow Requester to Change Duration</strong> option, you can set the maximum duration (days, hours, and minutes) that the requester can access the accounts and assets governed by this policy.</td>
</tr>
</tbody>
</table>
**Property** | **Description**
---|---
The default access duration is 7 days. The maximum access duration is 31 days.

**NOTE:** The user can change the access duration, but he cannot access the accounts or assets governed by this policy for longer than the maximum access duration time.

### Approver tab

Use the **Approver** tab to specify the approver settings for an access request policy.

**Table 115: Access Request Policy: Approver tab properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auto-Approved</strong></td>
<td>Select this option to automatically approve all access requests for accounts and assets governed by this policy.</td>
</tr>
<tr>
<td><strong>Notify when Account is Auto-Approved</strong></td>
<td>(Optional) When no approvals are required, enter an email address or select <strong>To</strong> to choose a user to notify when access is auto-approved.</td>
</tr>
<tr>
<td><strong>To</strong></td>
<td>If you used the <strong>To</strong> button to add Safeguard users, you can use the ✒ <strong>Clear</strong> icon to remove an individual address from this list or right-click and select <strong>Remove All</strong> to clear all addresses from the list.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>To send event notifications to a user, you must configure Safeguard to send alerts. For more information, see <a href="#">Configuring alerts</a> on page 72.</td>
</tr>
<tr>
<td><strong>Approvals Required</strong></td>
<td>Select this option to require approval for all access requests for accounts and assets governed by this policy. Enter the following information:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Qty:</strong> Enter or select the minimum number of approvals required from the selected users or user groups listed as <strong>Approvers</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Approvers:</strong> <strong>Browse</strong> to select one or more users or user groups who can approve access requests for accounts and assets governed by this policy.</td>
</tr>
<tr>
<td></td>
<td>Use the ✒ <strong>Clear</strong> icon to remove an individual &quot;approver&quot; user or user group from this list or right-click and select <strong>Remove All</strong> to clear all users from the list.</td>
</tr>
<tr>
<td></td>
<td>Click (or tap) <strong>+ Add</strong> or <strong>Delete</strong> to add or remove approver sets.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>The order of the approver sets is not significant, but all requirements must be met; that is, a request must obtain the number of approvals from each approver set defined.</td>
</tr>
<tr>
<td><strong>TIP:</strong></td>
<td>As a best practice, add user groups as approvers rather than individuals. This makes it possible to add an individual approver to a pending access request. In addition, you can modify an approvers list without editing the policy.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>The users you authorize as &quot;approvers&quot; receive alerts when an access request requires their approval if they have Safeguard configured to send alerts.</td>
</tr>
</tbody>
</table>

**NOTE:** Select this check box to enable notifications.

- Set the amount of time (days, hours, and minutes) to wait before notifying the escalation notification contact list about pending approvals.
- Enter an email address or select To to choose an email address of a Safeguard user.

If you used the To button to add Safeguard users, you can use the Clear icon to remove an individual address from this list or right-click and select Remove All to clear all addresses from the list.

**NOTE:** You can enter email addresses for non-Safeguard users.

**IMPORTANT:** Safeguard does not dynamically maintain the email addresses for an escalation notification contact list. If you change a Safeguard user's email address or delete a Safeguard user after creating a policy, you must update the email addresses in an escalation notification contact list manually. For more information, see User not notified on page 472.

**NOTE:** To send event notifications to a user, you must configure Safeguard to send alerts. For more information, see Configuring alerts on page 72.

Approval Anywhere has been enabled. View enabled users. Indicates that the Approval Anywhere feature has been configured. Click (or tap) the users link to view a list of the users who are authorized to approve requests using this feature.
### Reviewer tab

Use the **Reviewer** tab to define the reviewer settings for an access request policy.

#### Table 116: Access Request Policy: Reviewer tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Not Required</td>
<td>This check box is selected by default indicating that no review is required for completed access requests for accounts and assets governed by this policy.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> When this option is selected, no other options are available.</td>
</tr>
<tr>
<td>Review Required</td>
<td>Select this check box to require a review of completed access requests for accounts and assets governed by this policy.</td>
</tr>
<tr>
<td></td>
<td>- Qty: Enter or select the minimum number of people required to review a completed access request.</td>
</tr>
<tr>
<td></td>
<td>- Reviewers: <strong>Browse</strong> to select one or more users or groups of users who can review access requests for accounts and assets governed by this policy.</td>
</tr>
<tr>
<td></td>
<td>Use the <strong>Clear</strong> icon to remove an individual &quot;reviewer&quot; user or user group from this list or right-click and select <strong>Remove All</strong> to clear all users from the list.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> A reviewer can only review an access request once it is completed.</td>
</tr>
<tr>
<td></td>
<td><strong>TIP:</strong> As a best practice, add user groups as reviews rather than individuals. This makes it possible to add an individual reviewer to a pending access request. In addition, you can modify a reviewers list without editing the policy.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The users you authorize as &quot;reviewers&quot; receive alerts when an access request requires their review if they have Safeguard configured to send alerts.</td>
</tr>
<tr>
<td>Require Comment</td>
<td>Select this check box if the reviewer is required to enter a comment when reviewing an access request.</td>
</tr>
</tbody>
</table>

---

**NOTE:** You can add users as Approval Anywhere approvers by clicking the + **Add** toolbar button in the Approval Anywhere Users dialog.
Access Config tab

Use the Access Config tab to configure the access settings for the type of access being requested, based on the access type specified on the General tab.

Table 117: Access Request Policy: Access Config tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Type</td>
<td>This is a read-only field displaying the type of access selected on the General tab:</td>
</tr>
<tr>
<td></td>
<td>• Password Release</td>
</tr>
<tr>
<td></td>
<td>• SSH</td>
</tr>
<tr>
<td></td>
<td>• RDP</td>
</tr>
<tr>
<td>Include password release with sessions</td>
<td>Select this check box to include a password release with session access requests.</td>
</tr>
</tbody>
</table>

NOTE: You can enter email addresses for non-Safeguard users.

IMPORTANT: Safeguard does not dynamically maintain the email addresses for an escalation notification contact list. If you change a Safeguard user's email address or delete a Safeguard user after creating a policy, you must update the email addresses in an escalation notification contact list manually. For more information, see User not notified on page 472.

NOTE: To send event notifications to a user, you must configure Safeguard to send alerts. For more information, see Configuring alerts on page 72.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>requests</td>
<td><strong>NOTE:</strong> This setting is only available for SSH and RDP session requests.</td>
</tr>
<tr>
<td>Terminate expired sessions</td>
<td>Select this check box to terminate sessions that have expired.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This setting is only available for SSH and RDP session requests.</td>
</tr>
<tr>
<td>Change password after check-in</td>
<td>Select this check box if the password is to be changed after the user checks it back in.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> For password release requests, this option is selected by default.</td>
</tr>
<tr>
<td>Allow simultaneous access</td>
<td>Select this check box to allow multiple users access to the accounts and assets governed by this policy.</td>
</tr>
<tr>
<td>Maximum users at one time</td>
<td>When the <strong>Allow simultaneous access</strong> option is selected, enter the maximum number of users that can request access at one time.</td>
</tr>
<tr>
<td>Asset-Based Session Access</td>
<td>Select one of the following options to define the type of account credentials to be used to access the asset or account when a session is requested:</td>
</tr>
<tr>
<td></td>
<td>- None (default): The credentials are retrieved from the vault when the session is requested.</td>
</tr>
<tr>
<td></td>
<td>- User Supplied: The &quot;requester&quot; user must provide the credentials when the session is requested.</td>
</tr>
<tr>
<td></td>
<td>- Linked Account: The &quot;requester&quot; user's account is linked to an asset account that will be used when the session is requested.</td>
</tr>
<tr>
<td></td>
<td>- Directory Account: Use the <strong>Browse</strong> button to select the directory account to be used when the session is requested.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This setting is only available for SSH and RDP session requests.</td>
</tr>
</tbody>
</table>

**Session Settings tab**

Use the Session Settings tab to configure the settings for session access requests.

**NOTE:** The settings on this tab only apply to RDP and SSH (session) access requests.
Table 118: Access Request Policy: Session Settings tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record sessions</td>
<td>This check box is selected by default indicating that all sessions for the accounts and assets governed by this policy are to be recorded.</td>
</tr>
<tr>
<td>Enable Command Detection</td>
<td>For SSH session requests, select the Enable Command Detection check box to enable command detection, which means commands that are executed on the target host are detected and logged. For RDP session requests, select the Enable Windows Title Detection check box to enable windows title detection, which means the titles of all windows opened on the desktop during a privileged session are detected and logged.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>You can configure Safeguard to send these actions to a syslog server, in an email message, or via an SNMP trap. For more information, see External Integration settings on page 317.</td>
</tr>
<tr>
<td>RDP In-Session Controls</td>
<td>If RDP is selected as the access type on the General tab, select the following option if you want to allow the user to transfer data via the clipboard:</td>
</tr>
<tr>
<td></td>
<td>* Allow Clipboard</td>
</tr>
<tr>
<td></td>
<td>Selecting this option allows the users to copy a file or text from the client machine and paste it to the remote server.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>The data copied during a session using this option is currently not available for play back in this initial release of Safeguard.</td>
</tr>
<tr>
<td>SSH Controls</td>
<td>If SSH is selected as the access type on the General tab, select one or more of the following options to create a session that uses the specified protocol:</td>
</tr>
<tr>
<td></td>
<td>* Allow SFTP (Secure File Transfer)</td>
</tr>
<tr>
<td></td>
<td>* Allow SCP (Secure Copy)</td>
</tr>
<tr>
<td></td>
<td>* Allow X11 Forwarding (Forwards the graphical X-server session from the server to the client.)</td>
</tr>
<tr>
<td>NOTE:</td>
<td>The data transferred during a session using one of these protocols is currently not available for play back in this initial release of Safeguard.</td>
</tr>
</tbody>
</table>
Time Restrictions tab

Use the Time Restrictions tab to specify time restrictions for the access request policy.

Table 119: Access Request Policy: Time Restriction tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Time Restrictions</td>
<td>Select this option to specify time restrictions for access requests for accounts and assets governed by this policy. Time restrictions control when the access request policy is effective relative to the user’s time zone. For more information, see About time restrictions on page 212.</td>
</tr>
<tr>
<td>Daily calendar</td>
<td>Select and drag the days and hours you want to allow the policy to be effective.</td>
</tr>
<tr>
<td>Reset</td>
<td>Click (or tap) Reset to remove any time restrictions set in the daily calendar.</td>
</tr>
</tbody>
</table>

Emergency tab

Use the Emergency tab to enable emergency access for the accounts and assets governed by the access request policy.

Table 120: Access Request Policy: Emergency tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Emergency Access</td>
<td>Select this check box to allow users to request emergency access to accounts and assets governed by this policy. Clear this option to disallow emergency access.</td>
</tr>
</tbody>
</table>

**NOTE:** Emergency Access overrides the Approver requirements. That is, when a user requests access using Emergency Access, the request is immediately approved, provided that the other constraints are met such as the Requester settings.

**NOTE:** Multiple users are allowed to request emergency access simultaneously for the same account or asset.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify When Account is Released with Emergency access To</td>
<td>(Optional) When emergency access is enabled, build an escalation notification contact list, by entering an email address or selecting To to choose an email address of a Safeguard user. If you used the To button to add Safeguard users, you can use the Clear icon to remove an individual address from this list or</td>
</tr>
</tbody>
</table>
right-click and select **Remove All** to clear all addresses from the list.

**NOTE:** You can enter email addresses for non-Safeguard users.

**IMPORTANT:** Safeguard does not dynamically maintain the email addresses for an escalation notification contact list. If you change a Safeguard user's email address or delete a Safeguard user after creating a policy, you must update the email addresses in an escalation notification contact list manually. For more information, see User not notified on page 472.

**NOTE:** To send event notifications to a user, you must configure Safeguard to send alerts. For more information, see Configuring alerts on page 72.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore Time Restrictions</td>
<td>This check box is selected by default indicating that Safeguard is to ignore time restrictions when a user requests emergency access. Clear this check box if you want to enforce the time restrictions set for this policy and only allow emergency access during the specified time period.</td>
</tr>
</tbody>
</table>

**Deleting an access request policy**

**IMPORTANT:** When you delete a policy, Safeguard deletes it permanently; but it does not delete the accounts governed by the policy.

**To delete an access request policy from an entitlement**

1. Navigate to Administrative Tools | Entitlements.
2. In Entitlements, select an entitlement from the object list and open the Access Request Policies tab.
3. Select a policy.
4. Click (or tap) **Delete Selected**.
5. Confirm your request.
Modifying an access request policy

To modify an access request policy

1. Navigate to Administrative Tools | Entitlements.
2. In Entitlements, select an entitlement and open the Access Request Policies tab.
3. Double-click (or double-tap) a policy, or select a policy and click (or tap) Edit Access Policy.
4. Select the view of the policy’s information you want to modify (General, Time Restrictions, Scope, and so forth).

Copying an access request policy

To copy an access request policy

1. Navigate to Administrative Tools | Entitlements.
2. In Entitlements, select an entitlement from the object list and open the Access Request Policies tab.
3. Choose a policy and click (or tap) Copy Access Policy.
4. Enter a unique policy name.
5. Edit the new policy’s settings as desired.

NOTE: You cannot copy a policy and add it to another entitlement; policies are entitlement-specific.

Viewing policy details

To view the details of an entitlement’s policy

1. Navigate to Administrative Tools | Entitlements.
2. In Entitlements, select an entitlement from the object list and open the Access Request Policies tab.
3. Select a policy and click (or tap) Details.
   The policy’s properties dialog displays.
4. To edit the properties, double-click (or double-tap) a property pane (General, Scope, Requester, Approver, Reviewer, Access Config, Session Settings, Time Restrictions, or Emergency), or click (or tap) the Edit icon to the right of a property pane.
The **Access Request Policies** dialog displays allowing you to make the necessary changes.

**NOTE:** You must have Security Policy Administrator permissions to modify policy settings.

## Modifying an entitlement

### To modify an entitlement

1. Navigate to **Administrative Tools** | **Entitlements**.
2. In **Entitlements**, select an entitlement.
3. Select the view of the entitlement's information you want to modify (**General**, **Users**, or **Access Request Policies**).

**For example:**

- To change the selected entitlement's name, description, or time restrictions, double-click (or double-tap) the **General** information on the **General** tab or click (or tap) the ![Edit](edit_icon.png) icon.

  **NOTE:** You can also double-click (or double-tap) an entitlement name to open the **General** settings edit window.

- To add authorized requesters to the selected entitlement, switch to the **Users** tab.
  
  For more information, see [Adding users or user groups to an entitlement on page 213](#).

- To modify an access request policy, switch to the **Access Request Policies** tab.
  
  For more information about access request policy details, see [Creating an access request policy](#).

4. To change an entitlement's priority, select the priority number in the entitlement list and enter another number. For more information, see [About priority precedence on page 211](#).

5. To view or export the details of each operation that has affected the selected entitlement, switch to the **History** tab.

## Deleting an entitlement

**IMPORTANT:** When you delete an entitlement, Safeguard deletes all access request policies associated with that entitlement.
To delete an entitlement

1. Navigate to Administrative Tools | Entitlements.
2. In Entitlements, select an entitlement from the object list.
3. Click (or tap) Delete Selected.
4. Enter the name of the entitlement to confirm you want to delete the entitlement.
A partition is a named container for assets that can be used to segregate assets for delegated management. It is the responsibility of the Asset Administrator to add partitions to Safeguard. Partitions allow you to set up multiple asset managers, each with the ability to define password guidelines for the managed systems in their own workspace. Typically you would partition assets by geographical location, owner, function, or by operating system. For example, Safeguard can enable you to group Unix assets in a partition and delegate the Unix administrator to manage it.

You must assign all assets, and the accounts associated with them, to a partition. By default Safeguard assigns all assets and their associated accounts to the default partition, but you can set a different default.

**NOTE:** To search for a particular partition, see Search box on page 65.

The **Partitions** view displays the following information about the selected partition.

### Table 121: Partitions: Tabs

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td>Displays general information about the selected partition.</td>
</tr>
<tr>
<td>Assets tab</td>
<td>Displays the local assets assigned to the selected partition.</td>
</tr>
<tr>
<td>Accounts tab</td>
<td>Displays the accounts assigned to the selected partition.</td>
</tr>
<tr>
<td>Profiles tab</td>
<td>Displays the profiles associated with this partition.</td>
</tr>
</tbody>
</table>

**NOTE:** When a partition is added, a default asset profile is created for the partition, which can be edited, but not deleted.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovered Accounts tab</td>
<td>Displays the accounts Safeguard discovers when it runs an account discovery job. For more information, see Account discovery job workflow on page 491.</td>
</tr>
<tr>
<td>History tab</td>
<td>Displays the details of each operation that has affected the selected directory.</td>
</tr>
</tbody>
</table>
Use these toolbar buttons to manage partitions.

### Table 122: Partitions: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Partition</td>
<td>Add a partition to Safeguard. For more information, see Adding a partition on page 237.</td>
</tr>
<tr>
<td>Delete Selected</td>
<td>Remove the selected partition. For more information, see Deleting a partition on page 243.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of partitions.</td>
</tr>
<tr>
<td>Set as Default</td>
<td>Set a partition as the default. All new assets you add are automatically assigned to the default partition. For more information, see Setting a default partition on page 244.</td>
</tr>
</tbody>
</table>

### General tab

The **General** tab lists information about the selected partition.

Large tiles at the top of the tab display the number of **Assets**, **Accounts**, **Profiles**, and **Discovered Accounts** associated with the selected partition. Clicking a tile heading opens the corresponding tab.

### Table 123: Partitions General tab: General properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The partition name.</td>
</tr>
<tr>
<td>Delegated Owner</td>
<td>The users who are responsible for managing the assets and accounts in the selected partition.</td>
</tr>
</tbody>
</table>

**Description**: Information about the selected partition.

**Related Topics**

Modifying a partition

### Assets tab

The **Assets** tab displays the local assets assigned to the selected partition.

Click (or tap) **Add Asset** from the details toolbar to add one or more assets to the selected partition.
Table 124: Partitions: Assets tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The asset name.</td>
</tr>
<tr>
<td>Parent</td>
<td>The partition in which the asset resides.</td>
</tr>
<tr>
<td>Profile</td>
<td>The name of the profile that manages the asset.</td>
</tr>
<tr>
<td>Session Request</td>
<td>A check in this column indicates that session access requests are enabled for the asset.</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive information entered when the asset was added.</td>
</tr>
</tbody>
</table>

Use these buttons on the details toolbar to manage the assets assigned to the selected partition.

Table 125: Partitions: Assets tab toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Add Asset</td>
<td>Add one or more assets to the selected partition.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Retrieve and display an updated list of assets associated with the selected partition.</td>
</tr>
<tr>
<td>Search</td>
<td>To locate a specific asset in this list, enter the character string to be used to search for a match. For more information, see Search box on page 65.</td>
</tr>
</tbody>
</table>

Related Topics

Adding assets to a partition
Removing assets from a partition

Accounts tab

The Accounts tab displays the accounts assigned to the selected partition.

NOTE: By default, all accounts associated with an asset are assigned to the same partition profile, but you can reassign them. For more information, see Creating a partition profile on page 239.
Table 126: Partitions: Accounts tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The account name.</td>
</tr>
<tr>
<td>Parent</td>
<td>The partition in which the asset where the account resides.</td>
</tr>
<tr>
<td>Profile</td>
<td>The name of the profile that manages the account.</td>
</tr>
<tr>
<td>Service Account</td>
<td>A check in this column indicates that the account is a service account.</td>
</tr>
<tr>
<td>Password Request</td>
<td>A check in this column indicates that password release requests are enabled for the account.</td>
</tr>
<tr>
<td>Session Request</td>
<td>A check in this column indicates that session access requests are enabled for the account.</td>
</tr>
<tr>
<td>Needs a Password</td>
<td>Displays 🔼 if a password is not set for the account. For more information, see Checking, changing, or setting an account password on page 110.</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive information entered when the account was added.</td>
</tr>
</tbody>
</table>

Use these buttons on the details toolbar to manage the accounts assigned to the selected partition.

Table 127: Partitions: Accounts tab toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️ Refresh</td>
<td>Retrieve and display an updated list of assets and accounts associated with the selected partition.</td>
</tr>
<tr>
<td>🔍 Search</td>
<td>To locate a specific asset or account in this list, enter the character string to be used to search for a match. For more information, see Search box on page 65.</td>
</tr>
</tbody>
</table>

Related Topics

- Adding assets to a partition
- Removing assets from a partition

Profiles tab

The Profiles tab lists the profiles associated with this partition. For more information, see About profiles on page 233.

Click (or tap) + Create Profile from the details toolbar to add a profile to the selected partition.
### Table 128: Partitions: Profiles tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Password management profile name.</td>
</tr>
<tr>
<td>Default</td>
<td>&quot;Default&quot; displays in this column for the default profile. For more information, see Setting a default partition profile on page 241.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the selected profile.</td>
</tr>
</tbody>
</table>

Use these buttons on the details toolbar to manage your partitions profiles.

### Table 129: Partitions: Profiles tab toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Create Profile] Add a profile to the selected partition. For more information, see Creating a partition profile on page 239.</td>
<td></td>
</tr>
<tr>
<td>![Deleted Selected] Remove the selected partition profile.</td>
<td></td>
</tr>
<tr>
<td>![Refresh] Update the list of partition profiles.</td>
<td></td>
</tr>
<tr>
<td>![Edit Profile] Modify the selected partition profile. For more information, see Modifying a partition profile on page 241.</td>
<td></td>
</tr>
<tr>
<td>![Set as Default] Set the selected profile as the default partition profile. For more information, see Setting a default partition profile on page 241.</td>
<td></td>
</tr>
<tr>
<td>![Details] View additional details about the selected partition profile.</td>
<td></td>
</tr>
<tr>
<td>![Search] To locate a specific partition profile or set of profiles in this list, enter the character string to be used to search for a match. For more information, see Search box on page 65.</td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics

- Assigning assets or accounts to a partition profile
- How do I see which assets and/or accounts are governed by a profile

### About profiles

A profile is a set of configuration settings for a set of accounts in a partition or directory. When you create a new partition or directory, Safeguard creates a corresponding default profile with default schedules and rules. You can create multiple profiles to govern the accounts assigned to a partition or directory. Both assets and accounts are assigned to the scope of a profile.
For example, suppose you have an asset with 12 accounts and you configure the profile to check and change passwords every 60 days. If you want the password managed for one of those accounts every 7 days, you can create another profile and add the individual account to the new profile. Now, Safeguard will check and change all the passwords on this asset every 60 days except for this account, which will change every 7 days.

Implicit and explicit association

It is important to understand the difference between implicit and explicit assignments to a profile.

Implicit associations

Safeguard makes implicit assignments. For example, when you add an asset to Safeguard, it automatically adds the asset to the default partition and assigns it to the scope of the default profile. This is called implicit association. Assets implicitly inherit the partition's default profile. Similarly, accounts inherit their parent asset's profile. That means when you add an account to an asset, Safeguard implicitly adds that account to its asset's profile.

Later if you reassign the asset to another profile, Safeguard automatically reassigns all of the asset's associated accounts to the new profile.

Explicit associations

Safeguard allows you to explicitly add an asset or an account to a specific profile. When you explicitly assign an asset to a profile, it overrides the implicit inheritance from the partition so the asset's profile is no longer determined by its partition. Similarly, when you explicitly assign an account to a profile, Safeguard overrides the implicit inheritance from the asset and the account’s profile is no longer determined by its asset.

Now if you reassign the asset to another profile, Safeguard will not reassign the asset's associated accounts that were explicitly assigned to the old profile.

Resetting the default profile

If you set another profile as the default, Safeguard implicitly reassigns all assets and their associated accounts to that new default, but it will not reassign any assets or accounts that you have explicitly assigned to a profile. Once the implicit inheritance is broken, changing a partition's (or directory's) default profile has no effect on the scope of a profile. For more information, see Setting a default partition profile or Setting a default directory profile.

Related Topics

Assigning assets or accounts to a partition profile
Adding accounts to a directory profile
Assigning a profile to an asset
Account Password Rules
How do I manage accounts on unsupported platforms
How do I see which assets and/or accounts are governed by a profile
Discovered Accounts tab

A partition’s Discovered Accounts tab allows you to add accounts to Safeguard as a result of any account discovery jobs that have run against the assets in the selected partition. For more information, see Account discovery job workflow on page 491. The Discovered Accounts tab displays the following for the selected partition.

Table 130: Partitions: Discovered Accounts tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Indicates Ignored or Managed or is blank for any account that you have not previously tagged as Ignore or Manage.</td>
</tr>
<tr>
<td>Account Name</td>
<td>The name of the discovered account.</td>
</tr>
<tr>
<td>Asset Name</td>
<td>The asset associated with the discovered account.</td>
</tr>
<tr>
<td>Profile</td>
<td>The name of the profile that manages the account.</td>
</tr>
<tr>
<td>Date/Time Discovered</td>
<td>The date and time when the account was discovered.</td>
</tr>
</tbody>
</table>

Use these buttons on the details toolbar to manage the discovered accounts.

Table 131: Partitions: Discovered Accounts tab toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage</td>
<td>Select to add the selected account to the selected partition, and assign it to the scope of the default profile. For more information, see Setting a default partition profile on page 241.</td>
</tr>
<tr>
<td>Ignore</td>
<td>Select to prevent Safeguard from managing the selected account.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Retrieve and display an updated list of discovered accounts.</td>
</tr>
<tr>
<td>Search</td>
<td>To locate a specific account or set of accounts in this list, enter the character string to be used to search for a match. For more information, see Search box on page 65.</td>
</tr>
</tbody>
</table>

History tab

The History tab allows you to view or export the details of each operation that has affected the selected partition.

The History tab contains the following information:

Items: Total number of entries in the history log.
Search: For more information, see Search box on page 65.

Time Frame: By default the history details are displayed for the last 24 hours. Click (or tap) one of the time intervals at the top of the grid to display history details for a different time frame. If the display does not refresh after selecting a different time interval, click (or tap) Refresh.

Table 132: Partitions: History tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>The date and time of the event.</td>
</tr>
<tr>
<td>User</td>
<td>The display name of the user that triggered the event.</td>
</tr>
<tr>
<td>Source IP</td>
<td>The network DNS name or IP address of the managed system that triggered the event.</td>
</tr>
<tr>
<td>Object Name</td>
<td>The name of the selected partition.</td>
</tr>
<tr>
<td>Event</td>
<td>The type of operation made to the selected partition:</td>
</tr>
<tr>
<td></td>
<td>- Create</td>
</tr>
<tr>
<td></td>
<td>- Delete</td>
</tr>
<tr>
<td></td>
<td>- Update</td>
</tr>
<tr>
<td></td>
<td>- Add Membership</td>
</tr>
<tr>
<td></td>
<td>- Remove Membership</td>
</tr>
</tbody>
</table>

**NOTE:** A membership operation indicates a "relationship" change with a related or parent object such as a delegated administrator was added or removed from the selected partition.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related Object</td>
<td>The name of the related object.</td>
</tr>
<tr>
<td>Related Object Type</td>
<td>The type of the related object.</td>
</tr>
<tr>
<td>Parent</td>
<td>The name of the object to which the selected partition is a child.</td>
</tr>
<tr>
<td>Parent Object Type</td>
<td>The parent object type.</td>
</tr>
</tbody>
</table>

Select an event to display this additional information for some types of events (for example, create and update events).

Table 133: Additional History tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>The property that was updated.</td>
</tr>
<tr>
<td>Old Value</td>
<td>The value of the property before it was updated.</td>
</tr>
<tr>
<td>New Value</td>
<td>The new value of the property.</td>
</tr>
</tbody>
</table>
Managing partitions

Use the controls and tabbed pages on the Partitions page to perform the following tasks to manage partitions:

- Adding a partition
- Adding assets to a partition
- Removing assets from a partition
- Creating a partition profile
- Modifying a partition profile
- Setting a default partition profile
- Assigning assets or accounts to a partition profile
- Modifying a partition
- Deleting a partition
- Setting a default partition

Adding a partition

It is the responsibility of the Asset Administrator to add partitions to Safeguard. When you assign an asset to a partition, all the accounts associated with that asset are assigned to that partition, as well.

To add a partition

1. Navigate to Administrative Tools | Partitions.
2. Click (or tap) Add Partition from the toolbar.
3. In the Partition dialog, enter the following information:
   a. Name: Enter a unique name for the partition.
      Limit: 50 characters
   b. Description: (Optional) Enter information about this partition.
      Limit: 255 characters
   c. Delegated Owner: (Optional) Browse to select one or more users to manage the assets and accounts in this partition.
      You can use the Clear icon to remove an individual delegated owner from this list or right-click and select Remove All to clear all of the delegated owners from the list.
      By default, an Asset Administrator can manage all partitions; however, you can delegate partition management to a user with no administrator permissions.
When you create a new partition, Safeguard creates a corresponding default profile with default schedules and rules.

- Select the profile and click (or tap) Edit Profile to associate different schedules and rules. For more information, see Creating a partition profile on page 239.
- OR-
- Modify the values of the default schedules and rules in Settings. See Safeguard Access settings and Asset Management settings.

Adding assets to a partition

Use the Assets tab on the Partitions view to add one or more assets to a partition.

To add assets to a partition

1. Navigate to Administrative Tools | Partitions.
2. In Partitions, select a partition from the object list and open the Assets tab.
3. Click (or tap) Add Asset from the details toolbar.
4. On the Asset dialog, select one or more assets.
5. Click (or tap) OK.

For more information, see Assigning an asset to a partition on page 151.

If you do not see the asset you are looking for, depending on your Administrator permissions, you can create it in the selection dialog. (You must have Asset Administrator permissions to create assets.)

1. NOTE: You can only assign an asset to one partition at a time. When you assign an asset to a partition, all accounts associated with that asset are automatically reassigned to that partition, as well. Then, any new accounts you add for that asset are automatically assigned to that partition.

   You cannot remove assets from a partition. However, you can add them to another partition either from the scope of the other partition or from an asset's General properties.

To create a new asset from the Asset selection dialog

1. Click (or tap) Create New.
   For more information, see Adding an asset on page 136.
2. Create additional assets, as required.
3. Click (or tap) OK in the Asset selection dialog to assign the new assets to the selected partition.
Removing assets from a partition

You cannot remove assets from a partition. However, you can add them to another partition either from the scope of the other partition or from an asset's General properties. For more information, see Adding assets to a partition on page 238.

When you add an asset to a partition, all the accounts associated with that asset that are not explicitly assigned to another partition, are also added to the scope of that partition.

Creating a partition profile

It is the responsibility of the Asset Administrator or the partition's delegated administrator to add profiles to partitions.

To add a profile to a partition

1. Navigate to Administrative Tools | Partitions.
2. In Partitions, select a partition from the object list and open the Profiles tab.
3. Click (or tap) + Create Profile from the details toolbar.
4. On the General tab, supply the following information:
   a. Name: Enter a unique name for the profile.
      Limit: 50 characters
      Required
   b. Description: Enter information about this profile.
      Limit: 255 characters
5. On the Check Password tab, select a previously defined check password setting from the drop-down menu. Check password settings are the rules Safeguard uses to verify account passwords.

   **NOTE:** Expand the Description to see information about the selected check password setting.

   - Click (or tap) ⌘ to modify the selected check password setting.
   - Click (or tap) + to create a new check password setting.

Selecting either of these icons displays the Check Password Settings dialog allowing you to specify the appropriate check password settings. For more information, see Adding check password settings on page 347.

6. On the Change Password tab, select a previously defined change password setting from the drop-down menu. Change password settings are the rules Safeguard uses to reset account passwords.

   **NOTE:** Expand the Description to see information about the selected change password setting.
- Click (or tap) ✏️ to modify the selected change password setting.
- Click (or tap) ✖️ to create a new change password setting.

Selecting either of these icons displays the **Change Password Settings** dialog allowing you to specify the appropriate change password settings. For more information, see *Adding change password settings* on page 344.

7. On the **Account Password Rules** tab, select a previously defined account password rule. An account password rule is a complexity rule that governs the construction of the new password created by Safeguard during an automatic password change.

    **NOTE:** Expand the **Description** to see information about the selected account password rule.
    - Click (or tap) ✏️ to modify the selected account password rule.
    - Click (or tap) ✖️ to create a new account password rule.

For more information, see *Adding an account password rule* on page 341.

8. On the **Account Discovery** tab, select a previously defined account discovery setting. Account discovery settings are the rules Safeguard uses to perform account discovery. For more information, see *Account discovery job workflow* on page 491.

    **NOTE:** Expand the **Description** to see information about the selected account discovery setting.
    - Click (or tap) ✏️ to modify the selected account discovery setting.
    - Click (or tap) ✖️ to create a new account discovery setting.

For more information, see *Adding an asset account discovery setting* on page 268.

9. On the **Password Sync Groups** tab, add or update a password sync group governed by the partition profile change schedule. For more information, see *Password Sync Groups* on page 354.

    - Click (or tap) ✖️ **Add** to create a new password sync group associated with the partition profile and assign accounts. The **Password Sync Group** dialog displays. For more information, see *Adding a password sync group*.
    - Click (or tap) ✖️ **Delete Selected** to remove the selected password sync group.
    - Click (or tap) ✖️ **Refresh** to refresh the selected password sync group.
    - Click (or tap) ✏️ **Edit** to modify the selected sync group and account assignments. The **Password Sync Group** dialog displays. For more information, see *Modifying a password sync group* on page 356.
    - Click (or tap) ✖️ **Change Sync Group Password** to reset the selected sync group password. When selected, accounts in the sync group re-sync with the new sync group password.

10. Click (or tap) **Create Profile** to save your selections and create the partition profile.
Related Topics

Assigning assets or accounts to a partition profile
Setting a default partition profile
Assigning a profile to an asset
Account Password Rules

Modifying a partition profile

NOTE: Any modifications that you make to a profile affects all the assets and accounts governed by that profile.

To modify a partition profile

1. Navigate to Administrative Tools | Partitions.
2. In Partitions, select a partition from the object list and open the Profiles tab.
3. Select a profile:
   a. To modify the settings or rules, either double-click (or double-tap) the profile or click (or tap) the Edit Profile icon.
   b. To add assets to the profile, click (or tap) the Details icon and switch to the Assets tab of the details window.
   c. To add accounts to the profile, click (or tap) the Details icon and switch to the Accounts tab of the details window.

   For more information, see Assigning assets or accounts to a partition profile on page 242.

Setting a default partition profile

When you create a new partition, Safeguard creates a corresponding default profile with default schedules and rules.

NOTE: Safeguard sets the default schedules to "Never" verify or reset passwords. To change the settings, see Modifying a partition profile.

To set another profile as the default

1. Navigate to Administrative Tools | Partitions.
2. In Partitions, select a partition from the object list and open the Profiles tab.
3. Select a profile and click (or tap) Set as Default from the details toolbar or context menu.
NOTE: All assets and accounts that are not explicitly assigned to the default profile are automatically reassigned to the new default profile. For more information, see About profiles on page 233.

NOTE: Each Asset Administrator can set a unique default partition profile. Once you set a default profile, all new assets and accounts you add are automatically assigned to that profile.

Assigning assets or accounts to a partition profile

This topic explains how to assign an asset or an account to a partition profile. You can also configure Safeguard to run automatic asset or account discovery jobs. For more information, see How do I setup discovery jobs on page 489.

To add assets or accounts to a partition profile

1. Navigate to Administrative Tools | Partitions.
2. In Partitions, select a partition from the object list and open the Profiles tab.
3. Select a profile and click (or tap) the Details icon.
4. To add an asset to the selected partition profile, open the Assets tab.
   a. Click (or tap) + Add Asset.
   b. On the Asset dialog, select the assets to be added.
   c. Click (or tap) OK.
5. To add an account to the selected partition profile, open the Accounts tab.
   a. Click (or tap) + Add Account.
   b. On the Account dialog, select the accounts to be added.
   c. Click (or tap) OK.

NOTE: You can only add assets and accounts to a profile that are assigned to the scope of the partition.

If you do not see the account you are looking for, it might be assigned to a different partition. Depending on your Administrator permissions, you can create a new account in the selection dialog. (You must have Asset Administrator permissions to create assets and accounts.)

To create a new account from the Account selection dialog

1. Click (or tap) + Create New.
   For more information, see Adding an account on page 102.
2. Create additional items, as required.
3. Click (or tap) OK in the Account selection dialog to assign the new accounts to the selected partition.

**Related Topics**

Assigning a profile to an asset
Setting a default partition profile

**Modifying a partition**

*To modify a partition*

1. Navigate to Administrative Tools | Partitions.
2. In Partitions, select a partition from the object list.
3. Select the view of the partition’s information you want to modify (General, Assets, or Profiles).

For example:

- To change a partition's name or description, or delegate partition management to a user, double-click (or double-tap) the General information on the General tab or click (or tap) the Edit icon.

  ![NOTE: You can also double-click (or double-tap) a partition name to open the General settings edit window.]

- To assign assets to the partition, open the Assets tab.

  ![NOTE: You can multi-select items to assign more than one asset to a partition.]

- To modify the password validation and reset settings, open the Profiles tab, select a profile and click (or tap) the Edit icon.

4. To set the default partition, click (or tap) Set as Default from the toolbar or context menu.
5. To view or export the details of each operation that has affected the selected partition, open the History tab.

**Deleting a partition**

*To delete a partition*

1. Navigate to Administrative Tools | Partitions.
2. In Partitions, select a partition from the object list.
3. Click (or tap) Delete Selected.
4. In the **Asset Partition** dialog, select the partition where assets and accounts are to be reassigned.

   **NOTE:** When deleting a partition, Safeguard transfers all assets and accounts into the selected partition. Safeguard deletes profiles and associated profile settings, discovery jobs, and history data.

5. Click (or tap) **OK** to reassign the assets and accounts and remove the selected partition.

### Setting a default partition

Safeguard automatically adds new assets to the default partition and the default profile. For more information, see [Setting a default partition profile on page 241](#).

**To set the default partition**

1. Navigate to **Administrative Tools | Partitions**.
2. In **Partitions**, right-click (or press and hold) a partition and choose **Set as Default** from the context menu.
   - OR-
3. Select a partition and click (or tap) **Set as Default** from the toolbar.

   **NOTE:** Each Asset Administrator can set a unique default partition. Once you set a default partition, all new assets you add are automatically assigned to that partition.
Settings

The Settings page in Administrative Tools is where you configure Safeguard to run backups, install updates, manage clusters, manage certificates, enable event notifications, enable external integration, define profile configuration settings, define user password rules, define discovery rules, and run troubleshooting tools.

NOTE: You must have administrator permissions to access the Settings page and the administrator permissions you have determine what you can do.

Use the Search control at the top of the Settings page to locate a particular setting. For example, if you type password and press the Enter key, a list of all the password settings appears; select an entry from this list to display the selected settings page.

Table 134: Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Access Request settings  | Where you enable (or disable) access request services, such as session requests, password release requests, password check and password change management.  
                            Where you define reason codes for access requests.                                                                                     |
| Appliance settings       | Where you view appliance information, diagnose and reset or update the Safeguard appliance.                                                 
                            Where you enable (or disable) the Application to Application service and Lights Out Management, apply license, configure networking settings, and generate a support bundle. |
<p>| Asset Management settings| Where you configure account discovery rules                                                                                                                                                        |
|                          | NOTE: These configuration rules apply to asset accounts only. Directory account discovery is done on the directory entity dialogs.                                                           |
|                          | Where you define and manage dynamic tags for assets, asset accounts, and directory accounts.                                                                                                       |
| Backup and Retention settings | Where you run or schedule backups, manage backups and define archive servers for storing backup files.                                    |</p>
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificates settings</td>
<td>Where you manage the chain of trusted certificates.</td>
</tr>
<tr>
<td>Cluster settings</td>
<td>Where you can create a cluster of appliances to reduce downtime and data loss in the case of natural or human-induced disaster. Where you define managed networks for your organization so Safeguard can more effectively manage assets and accounts, and service access requests.</td>
</tr>
<tr>
<td>External Integration settings</td>
<td>Where you configure event notifications. Where you configure integration with the Application to Application service, Approval Anywhere, Email, SNMP, Starling, Syslog, and external federation providers, secondary authentication service providers, and external ticketing system. Where you join Safeguard to Starling.</td>
</tr>
<tr>
<td>Messaging settings</td>
<td>Where you configure a login notification or the message of the day displayed on the Safeguard Home page.</td>
</tr>
<tr>
<td>Profile settings</td>
<td>Where you define the profile configuration settings, including account password rules and password check and change schedules.</td>
</tr>
<tr>
<td>Safeguard Access settings</td>
<td>Where you configure user password rules and Safeguard login controls.</td>
</tr>
<tr>
<td>Sessions settings</td>
<td>Where you configure global settings related to the One Identity Safeguard Privileged Sessions module. Where you configure the SSH banner and manage the SSH Host Key.</td>
</tr>
</tbody>
</table>

**Access Request settings**

Use the Access Request settings to enable (or disable) access request and password management services and to define global reason codes that can be used when creating access request policies.
Table 135: Access Request settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable or Disable Services (Access request and password management services) | Where you enable or disable the following Safeguard services:  
  - Session requests  
  - Password requests  
  - Check password management  
  - Change password management |
| Reasons                                                  | Where you configure access request reason codes, which can then be used when creating access request policies.                                  |

### Enable or Disable Services (Access request and password management services)

One Identity Safeguard allows you to enable or disable access request and password management services. These settings control session and password release requests, manual account password validation and reset tasks as well as the automatic profile check and change tasks in Directories and Partitions.

All services are enabled by default. The toggles appear blue with the switch to the right when a service is enabled and gray with the switch to the left when a service is disabled.

**NOTE:** Even though these global settings are enabled by default. By default, these services are disabled for service accounts and for accounts and assets found as part of a discovery job.

Service accounts can be modified to adhere to these schedules and discovered accounts can be activated when managed.

It is the responsibility of the Appliance Administrator to manage the access request and password management services.

Table 136: Enable or Disable Services settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Session Requests Enabled         | Session requests are enabled by default indicating that authorized users can make session access requests.  
  Click (or tap) the **Session Requests Enabled** toggle to disable this service so sessions can not be requested. |
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>NOTE:</strong> When the Privileged Sessions module is disabled, no new session access requests can be initiated. Depending on the access request policies that control the target asset/account, you will see a message informing you that Sessions is not available. In addition, current session access requests cannot be launched. Again a message appears informing you Sessions is not available. For example, you may see the following message &quot;This feature is temporarily disabled. See your appliance administrator for details&quot;.</td>
</tr>
<tr>
<td>Password Requests Enabled</td>
<td>Password requests are enabled by default indicating that authorized users can make password release requests. Click (or tap) the <strong>Password Requests Enabled</strong> toggle to disable this service so passwords can not be requested. <strong>NOTE:</strong> Disabling the password request service will place any open requests on hold until this service is re-enabled.</td>
</tr>
<tr>
<td>Check Password Management Enabled</td>
<td>Check password management is enabled by default indicating that Safeguard automatically performs the password check task if the profile is scheduled, and allows you to manually check an account's password. Click (or tap) the <strong>Check Password Management Enabled</strong> toggle to disable the password validation service. <strong>NOTE:</strong> Safeguard enables automatic password management services by default. Typically, you would only disable them during an organization-wide maintenance window. When disabling a password management service, Safeguard allows all currently running tasks to complete; however, no new tasks will be allowed to start.</td>
</tr>
<tr>
<td>Change Password Management Enabled</td>
<td>Change password management is enabled by default indicating that Safeguard automatically performs the password change task if the profile is scheduled, and allows you to manually reset an account's password. Click (or tap) the <strong>Change Password Management Enabled</strong> toggle to disable the password reset service.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>

NOTE: Safeguard enables automatic password management services by default. Typically, you would only disable them during an organization-wide maintenance window. When disabling a password management service, Safeguard allows all currently running tasks to complete; however, no new tasks will be allowed to start.

Reasons

In an access request policy, a Security Policy Administrator can require that a requester provide a reason for requesting access to a password or session. Then, when requesting access, the user can select a predefined reason from a list. For example, you might use these access request reasons:

- Software Updates
- System Maintenance
- Hardware Issues
- Problem Ticket

**To configure access request reasons**

1. In Settings, select Access Request | Reasons.
2. Click (or tap) + Add Reason to add a new reason.
3. In the Reason dialog, enter the following:
   a. Name: Enter a name for the reason.
      Limit: 50 characters
      Required
   b. Description: Enter a description for the reason.
      Limit: 255 characters
      Required
4. Click (or tap) Add Reason.
5. To edit a reason, click (or tap) Edit Reason.
   The Reason dialog appears allowing you to modify the name or description.
6. To delete a reason, click (or tap) Delete Reason.
   In the confirmation dialog, click (or tap) Yes.
Related Topics
Creating an access request policy

Appliance settings

Use the Appliance settings to view general information about the appliance, run diagnostic tools, and reset or update the One Identity Safeguard appliance.

One Identity Safeguard provides the following information to help you resolve many common problems you may encounter as you deploy and use your appliance.

Table 137: Appliance settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Information</td>
<td>Where you view general information about the appliance, as well as its performance utilization and the memory usage. This page also contains power controls to shut down or restart your appliance.</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>Where you run diagnostic tests on your appliance.</td>
</tr>
<tr>
<td>Enable or Disable Services (Application to Application service)</td>
<td>Where you enable or disable the Application to Application functionality.</td>
</tr>
<tr>
<td>Factory Reset from the desktop client</td>
<td>Where you perform a factory reset to revert your appliance to its original state when it first came from the factory.</td>
</tr>
<tr>
<td>Licensing</td>
<td>Where you add or update a Safeguard license.</td>
</tr>
<tr>
<td>Lights Out Management (BMC)</td>
<td>Where you enable and disable lights out management, which allows you to remotely manage the power state and serial console to Safeguard using the baseboard management controller (BMC).</td>
</tr>
<tr>
<td>Networking</td>
<td>Where you view and configure the primary network interface, and if applicable, the sessions network interface.</td>
</tr>
<tr>
<td>Support Bundle</td>
<td>Where you create a support bundle containing system and configuration information to send to One Identity Support to analyze and diagnose issues with your appliance.</td>
</tr>
<tr>
<td></td>
<td>If you have the Privileged Sessions module licensed, this is where you enable (and disable) session debug logging to be included in a support bundle.</td>
</tr>
<tr>
<td>Time</td>
<td>Where you enable Network Time Protocol (NTP) and set the primary and secondary NTP servers.</td>
</tr>
</tbody>
</table>
NOTE: A replica in the cluster will always reference the primary appliance as its NTP server.

**Updates**

Where you upload and install an update file. For more information, see Updates on page 265.

In addition to the appliance options, One Identity Safeguard provides these troubleshooting tools:

**Table 138: Additional troubleshooting tools**

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Center</td>
<td>View the details of specific events or user activity. For more information, see Activity Center on page 50.</td>
</tr>
<tr>
<td>LCD status messages</td>
<td>An LCD screen on the appliance to view the status of the appliance as it is starting up or shutting down. For more information, see LCD status messages on page 458.</td>
</tr>
<tr>
<td>Recovery kiosk</td>
<td>A terminal or laptop connected directly to the appliance to view basic appliance information, restart the appliance remotely, shut down the appliance, reset the bootstrap administrator’s password to its initial value, perform a factory rest, or to generate and send a support bundle to a Windows share. For more information, see Recovery kiosk on page 462.</td>
</tr>
</tbody>
</table>

**Appliance Information**

It is the responsibility of the Operations Administrator or the Appliance Administrator to monitor the status of the appliance.

The following displays on the top of the Appliance Information pane.

**Table 139: Appliance properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Name</td>
<td>The name of the appliance. To modify this name, click (or tap) Edit.</td>
</tr>
<tr>
<td>Host</td>
<td>The appliance network server IP address.</td>
</tr>
<tr>
<td>Client Version</td>
<td>The version of the Safeguard desktop client application.</td>
</tr>
<tr>
<td>Appliance Version</td>
<td>The version of the Safeguard appliance.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The amount of time (hours and minutes) the appliance has been running.</td>
</tr>
</tbody>
</table>
In addition, this view contains two tabbed pages to display general information and performance data for the appliance.

**Appliance: General tab properties**

**Disk** displays the amount of used and free disk space.

**Table 140: General tab: Appliance properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>The system manufacturer.</td>
</tr>
<tr>
<td>Model</td>
<td>The system model.</td>
</tr>
<tr>
<td>Bios Description</td>
<td>The system bios description.</td>
</tr>
<tr>
<td>Bios Serial Number</td>
<td>The system's bios serial number.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The media access control address (MAC address) assigned to the network interface for communications.</td>
</tr>
<tr>
<td>Ship Date</td>
<td>The appliance ship date.</td>
</tr>
<tr>
<td>Processor</td>
<td>The processor information.</td>
</tr>
<tr>
<td>Virtual Memory</td>
<td>The virtual memory allocation.</td>
</tr>
<tr>
<td>Physical Memory</td>
<td>The physical memory allocation.</td>
</tr>
<tr>
<td>TLS 1.2 only</td>
<td>Click (or tap) this toggle to disable earlier versions of the Transport Layer Security (TLS) protocol and use only TLS v1.2.</td>
</tr>
</tbody>
</table>

**NOTE:** You must reboot your appliance after enabling **TLS 1.2 only**.

**Power**

Use the power controls to shut down or restart your appliance.

- For more information on shutting down the appliance, see **Shutting down the appliance** on page 253.
- For more information on restarting the appliance, see **Restarting the appliance** on page 254.
Appliance: Performance tab properties

Table 141: Performance tab: Performance properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Displays the CPU information and the performance utilization of your appliance.</td>
</tr>
<tr>
<td>Memory</td>
<td>Displays the memory usage of your appliance; what is currently in use and what is free.</td>
</tr>
</tbody>
</table>

Setting the appliance name

Safeguard automatically assigns a name to the appliance; however, you can change the name from the Appliance Information page.

To set the appliance name

1. In Settings, select Appliance | Appliance Information.
2. Click (or tap) Edit to enable the Appliance Name text box.
3. Enter a new appliance name and click (or tap) Save.

Shutting down the appliance

You can shut down an appliance from the Administrative Tools view in the Windows desktop client or directly from the appliance itself.

⚠️ CAUTION: Rebooting the appliance causes a service outage for any current users.

To shutdown an appliance

1. In Settings, select Appliance | Appliance Information.
2. Type an explanation for shutting down the Safeguard appliance in the Reason box and click (or tap) Shut Down.

⚠️ IMPORTANT: After the appliance powers off you will need physical access to start it. Press the Green check mark button on the front panel of the appliance for NO more than one second to power on the appliance.

⚠️ CAUTION: Once the Safeguard appliance is booted, DO NOT press and hold the Green check mark button. Holding this button for four or more seconds will cold reset the power of the appliance and may result in damage.

3. To confirm your action, enter the words Shut Down in the box and click (or tap) OK.
4. The One Identity Safeguard 2000 Appliance LCD screen displays "LCD service terminating."

![NOTE: You can also use the Red X button on the front panel of the appliance to shut it down. Press and hold the Red X button for four seconds until it displays POWER OFF.](image)

![CAUTION: Once the Safeguard appliance is booted, DO NOT press and hold the Red X button for more than 13 seconds. This will hard power off the appliance and may result in damage.](image)

## Restarting the appliance

Use the Power controls on the **Administrative Tools** view in the Windows desktop client to restart an appliance.

**To restart the appliance**

1. In **Settings**, select **Appliance | Appliance Information**.
2. Type an explanation for restarting the Safeguard appliance in the **Reason** box and click (or tap) **Restart**.
3. To confirm your action, enter the word **Restart** in the box and click (or tap) **OK**.
4. The One Identity Safeguard 2000 Appliance LCD screen displays the run level status of the appliance as it is starting up. For more information, see [LCD status messages](#) on page 458.

## Diagnostics

Safeguard makes these diagnostic tests available for the Appliance Administrator and Operations Administrator.

![NOTE: When you run these diagnostic tests, they are run on the appliance.](image)

**Table 142: Appliance Tests**

<table>
<thead>
<tr>
<th>Test</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping</td>
<td>To verify network connectivity and response time between the appliance to the specified host.</td>
</tr>
<tr>
<td>NS Lookup</td>
<td>To obtain DNS details of the specified host in relation to the appliance.</td>
</tr>
<tr>
<td>Trace Route</td>
<td>To obtain route information; traceroute determines the paths packets take from one IP address to another.</td>
</tr>
</tbody>
</table>
Test | Description
--- | ---
Telnet | To test TCP/IP connectivity between the appliance and specified host.
Show Routes | To retrieve routing table information.

**Related Topics**
Troubleshooting  
Frequently asked questions

**Ping**

Use the ping test to verify network connectivity and response time between the Safeguard appliance and the specified host.

**Table 143: Ping diagnostic test settings**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping through</td>
<td>Select a network interface to issue the diagnostic command:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Network (X0):</strong> Select to ping the primary interface.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Sessions (X1):</strong> Select to ping the sessions interface.</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>Enter the remote host's IP address or Hostname.</td>
</tr>
<tr>
<td>Ping</td>
<td>Click (or tap) <strong>Ping</strong> to run the test.</td>
</tr>
<tr>
<td></td>
<td>The test results display in the <strong>Output</strong> window.</td>
</tr>
<tr>
<td>More Settings</td>
<td>Select <strong>More Settings</strong> to configure these additional (optional) options:</td>
</tr>
<tr>
<td></td>
<td>- Resolve IP addresses to hostnames</td>
</tr>
<tr>
<td></td>
<td>- Number of echo requests to send</td>
</tr>
<tr>
<td></td>
<td>- Send buffer size</td>
</tr>
<tr>
<td></td>
<td>- Set 'don't fragment' flag in packet (IPv4 only)</td>
</tr>
<tr>
<td></td>
<td>- Time to live</td>
</tr>
<tr>
<td></td>
<td>- Type of serve</td>
</tr>
<tr>
<td></td>
<td>- Record route for count hops (IPv4 only)</td>
</tr>
<tr>
<td></td>
<td>- Time stamp for count hops (IPv4 only)</td>
</tr>
<tr>
<td></td>
<td>- Timeout in milliseconds to wait for each reply</td>
</tr>
</tbody>
</table>
**NS Lookup**

Use the NS Lookup query to obtain the domain name server or IP address of the specified host in relation to the Safeguard appliance.

**Table 144: NS Lookup diagnostic test settings**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Interface</td>
<td>Select a network interface to issue the diagnostic command:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Network (X0)</strong>: Select to query at the primary interface.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Sessions (X1)</strong>: Select to query at the sessions interface.</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>Enter the remote host's IP address or Hostname.</td>
</tr>
<tr>
<td>Record Type</td>
<td>Select the type of DNS record to be queried.</td>
</tr>
<tr>
<td>Lookup</td>
<td>Click (or tap) <strong>Lookup</strong> to run the test.</td>
</tr>
<tr>
<td></td>
<td>The test results display in the <strong>Output</strong> window.</td>
</tr>
</tbody>
</table>

**Trace Route**

Use the Trace Route test to obtain route information, such as the paths packets take from one IP address to another.

**Table 145: Trace Route diagnostic test settings**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trace route through</td>
<td>Select a network interface to issue the diagnostic command:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Network (X0)</strong>: Select to test the primary interface.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Sessions (X1)</strong>: Select to test the sessions interface.</td>
</tr>
<tr>
<td>IP or Hostname</td>
<td>Enter the remote host's IP address or Hostname.</td>
</tr>
<tr>
<td>Trace</td>
<td>Click (or tap) <strong>Trace</strong> to run the test.</td>
</tr>
<tr>
<td></td>
<td>The test results display in the <strong>Output</strong> window.</td>
</tr>
<tr>
<td>More Settings</td>
<td>Select <strong>More Settings</strong> to configure these additional (optional) options:</td>
</tr>
<tr>
<td></td>
<td>- Resolve IP addresses to hostname</td>
</tr>
<tr>
<td></td>
<td>- Maximize number of hops to search for target</td>
</tr>
<tr>
<td></td>
<td>- Timeout in milliseconds to wait for each reply</td>
</tr>
</tbody>
</table>
**Telnet**

Use Telnet to test TCP/IP connectivity between the Safeguard appliance and the specified host.

**Table 146: Telnet diagnostic test settings**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connect through</strong></td>
<td>Select a network interface to issue the diagnostic command:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Network (X0)</strong>: Select to test the primary interface.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Sessions (X1)</strong>: Select to test the sessions interface.</td>
</tr>
<tr>
<td><strong>IP or Hostname</strong></td>
<td>Enter the remote host's IP address or Hostname.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Enter the port number on a target host.</td>
</tr>
<tr>
<td><strong>Connect</strong></td>
<td>Click (or tap) <strong>Connect</strong> to run the test.</td>
</tr>
<tr>
<td></td>
<td>The test results display in the <strong>Output</strong> window.</td>
</tr>
<tr>
<td><strong>More Settings</strong></td>
<td>Select <strong>More Settings</strong> to configure this additional (optional) option:</td>
</tr>
<tr>
<td></td>
<td>- Connection Timeout</td>
</tr>
</tbody>
</table>

**Show Routes**

Use Show Routes to retrieve routing tables to further investigate connectivity issues.

**Table 147: Show Routes diagnostic test settings**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Show Routes through</strong></td>
<td>Select a network interface to issue the diagnostic command:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Network (X0)</strong>: Select to retrieve routing tables for the primary interface.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Sessions (X1)</strong>: Select to retrieve routing tables for the sessions interface.</td>
</tr>
<tr>
<td><strong>Show Routes</strong></td>
<td>Click (or tap) <strong>Show Routes</strong> to run the test.</td>
</tr>
<tr>
<td></td>
<td>The test results display in the <strong>Output</strong> window.</td>
</tr>
</tbody>
</table>
Enable or Disable Services (Application to Application service)

The Enable or Disable Services pane on the Appliance settings page, displays a single toggle, Application to Application Enabled, for enabling or disabling the Application to Application service. It is the responsibility of the Appliance Administrator to manage the Application to Application service.

The Application to Application service is disabled by default. The toggle appears blue with the switch to the right when the service is enabled and gray with the switch to the left when the service is disabled.

Factory Reset from the desktop client

As an Appliance Administrator, you can use the Factory Reset feature to reset a Safeguard appliance to recover from major problems or to clear the data and configuration settings on the appliance.

⚠️ CAUTION: Care should be taken when performing a factory reset against an appliance, because this operation removes all data and audit history, returning it to its original state when it first came from the factory. The appliance must go through configuration again as if it had just come from the factory. For more information, see Setting up One Identity Safeguard for the first time on page 37.

In addition, performing a factory reset may change the default SSL certificate and default SSH host key.

💡 NOTE: Clustered environment: Performing a factory reset on a clustered appliance will not automatically remove the appliance from a cluster. You will need to unjoin an appliance that has been factory reset from the cluster. The factory reset appliance must be configured again. For more information, see Setting up One Identity Safeguard for the first time on page 37.

To perform a factory reset from the desktop client

1. In Settings, select Appliance | Factory Reset.
2. Click (or tap) Factory Reset.
3. In the Factory Reset confirmation dialog, enter the words Factory Reset and click (or tap) OK.

The appliance will go into Maintenance mode to revert the appliance. Once completed, you will be prompted to restart the desktop client. If the appliance had been in a cluster, you may need to unjoin the factory reset appliance. The factory reset appliance must be configured again. For more information, see Setting up One Identity Safeguard for the first time on page 37. In addition, when you log into the appliance, you will be prompted to add your Safeguard licenses.
Licensing

It is the responsibility of the Appliance Administrator to manage the Safeguard licenses. The first time you log into Safeguard, it prompts you to add a license. In addition, you can add a new module license or update a license from the Settings | Appliance | Licensing pane.

NOTE: For more information, see Product licensing on page 33.

Table 148: Licensing options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding a license</td>
<td>To add a new module license to Safeguard.</td>
</tr>
<tr>
<td>Applying an updated license</td>
<td>To update a Safeguard module license.</td>
</tr>
</tbody>
</table>

Adding a license

The first time you log into Safeguard as the Appliance Administrator, it prompts you to add a license. In addition, you can add additional Safeguard module licenses from the Administrative Tools | Settings | Appliance page.

To add a new module license

1. In Settings, select Appliance | Licensing.
2. Click (or tap) +.
3. Browse to select the license file.
   Once you add a license, Safeguard displays the current license information and additional links that allow you to update the license or view the license history for a module.
4. To add another module license, click (or tap) Add Another License in the Success dialog.

NOTE: To avoid disruptions in the use of Safeguard, the Appliance Administrator must configure the SMTP server, and define email templates for the License Expired and the License Expiring Soon event types. This ensures you will be notified of an approaching expiration date. For more information, see Enabling email notifications on page 327.
Applying an updated license

As the Appliance Administrator, you can update a module license from the Settings | Appliance | Licensing pane.

**To update a module license**

1. In Settings, select Appliance | Licensing.
2. Select Update License in the lower left corner of a module's licensing information pane.
3. Browse to select the license file. Select Open.

**NOTE:** To avoid disruptions in the use of Safeguard, the Appliance Administrator must configure the SMTP server, and define email templates for the License Expired and the License Expiring Soon event types. This ensures you will be notified of an approaching expiration date. For more information, see Enabling email notifications on page 327.

Lights Out Management (BMC)

The Lights Out Management feature allows you to remotely manage the power state and serial console to Safeguard using the baseboard management controller (BMC). When a LAN interface is configured, this enables the Appliance Administrator to power on an appliance remotely or to interact with the recovery kiosk.

**IMPORTANT:** This feature requires a LAN interface to be enabled and configured. One Identity Safeguard's BMC supports the following LAN interfaces to provide this functionality:

- SSH
- IPMI v2
- Web
- Serial over Lan

It is strongly recommended that the LAN interface only be enabled in trusted environments.

The Lights Out Management (BMC) pane displays a single toggle, Enable Lights Out Management (BMC), for enabling and disabling this capability. Once enabled, additional fields appear allowing the Appliance administrator to set the password, network address, subnet mask, and gateway for the BMC.

**NOTE:** Once Lights Out Management is enabled in Safeguard, you can access the BMC via a web interface or by using SSH to connect to the IPMI port to remotely manage the power state and serial console to Safeguard. The default user for accessing the BMC is ADMIN.
Enabling Lights Out Management

It is the responsibility of the Appliance Administrator to enable and configure the Lights Out Management feature.

**NOTE:** When Lights Out Management is enabled, the Appliance Administrator can set or change the password and modify the network information for the baseboard management console (BMC). When disabled, Safeguard immediately resets the password to a random value and resets the network settings to default values.

**To enable Lights Out Management**

1. In **Settings**, select **Appliance | Lights Out Management (BMC)**.
2. Click (or tap) the **Enable Lights Out Management** toggle to enable this feature.
3. Enter the following information about the BMC:
   a. **IP address**: The IPv4 address of the host machine.
   b. **Netmask**: The network mask IPv4 address.
   c. **Default Gateway**: The default gateway IPv4 address.
4. Click (or tap) the **Set BMC Admin Password** button to set the password for the host machine.
   Maximum password length: 20 characters.
   **NOTE:** If this feature was previously enabled, you will see an **Update BMC Admin Password** button instead. Optionally, click (or tap) the **Update BMC Admin Password** button to reset the password for the host machine.
5. Click (or tap) **OK** to save the settings on the host machine.

Networking

Use the **Networking** pane to view and configure the primary network interface, and if applicable, a proxy server to relay web traffic, and the sessions network interface.

It is the responsibility of the Appliance Administrator to ensure the network interfaces are configured correctly. Click (or tap) the **Edit** icon next to the Network Interface or Proxy Server heading to edit or configure the network properties.

Network Interface X0 (primary interface)

**Table 149: Network Interface X0 properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>The media access control address (MAC address), a unique identi-</td>
</tr>
</tbody>
</table>
### Property Description

- **IP Address**: The IPv4 address of the network interface.
- **Netmask**: The IPv4 network mask.
- **Default Gateway**: The IPv4 default gateway.
- **IPv6 Address**: The IPv6 address of the network interface.
- **IPv6 Prefix Length**: The IPv6 subnet prefix length.
- **IPv6 Gateway**: The IPv6 default gateway.
- **DNS Servers**: The IP address for the primary DNS servers.
- **DNS Suffixes**: The network suffixes for the DNS servers.

**NOTE:** You can modify the network suffixes for the DNS servers by clicking the Edit icon next to the Network Interface X0 heading.

### Proxy Server X0

The **Proxy Server X0** settings must be configured if your company policies do not allow devices to connect directly to the web. Once configured, Safeguard uses the configured proxy server for outbound web requests to external integrated services, such as Starling.

**NOTE:** Only HTTP web proxy is supported.

#### Table 150: Proxy Server X0 properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy URI</td>
<td>The IP address or DNS name of the proxy server. Required</td>
</tr>
<tr>
<td>Port</td>
<td>The port number used by the proxy server to listen for HTTP requests.</td>
</tr>
<tr>
<td></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>Value: Integer from 1 to 65535.</td>
</tr>
<tr>
<td>Username</td>
<td>The user name used to connect to the proxy server.</td>
</tr>
<tr>
<td>Password</td>
<td>The password required to connect to the proxy server.</td>
</tr>
</tbody>
</table>

**NOTE:** If different ports are specified in the proxy URI and the **Port** field, the **Port** field takes precedence.

**NOTE:** The username and password are only required if your proxy server requires them to be specified.
NOTE: The username and password are only required if your proxy server requires them to be specified.

Network Interface X1 (sessions interface)

NOTE: If the embedded sessions appliance is used, the Network Interface X1 information must be configured to use One Identity Safeguard for Privileged Sessions.

Table 151: Network Interface X1 properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>The MAC address, a unique identifier assigned to the session interface for communications.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IPv4 address of the session interface.</td>
</tr>
<tr>
<td>Netmask</td>
<td>The IPv4 network mask.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>The IPv4 default gateway.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>The IPv6 address of the session interface.</td>
</tr>
<tr>
<td>IPv6 Prefix Length</td>
<td>The IPv6 subnet prefix length.</td>
</tr>
<tr>
<td>IPv6 Gateway</td>
<td>The IPv6 default gateway.</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>The IP address for the primary DNS servers.</td>
</tr>
<tr>
<td>DNS Suffixes</td>
<td>The network suffixes for the DNS servers.</td>
</tr>
</tbody>
</table>

Support Bundle

To analyze and diagnose issues, One Identity Support may ask the Appliance Administrator or Operations Administrator to send a support bundle containing system and configuration information.

NOTE: As an alternative, you can use the Recovery kiosk to generate and send a support bundle to a Windows share. For more information, see Recovery kiosk on page 462.
To create a support bundle

1. In Settings, select Appliance | Support Bundle.
2. If you have the Privileged Sessions module licensed, select the Include Session Log check box if you want to include the Sessions debug log in the support bundle.
3. Click (or tap) Generate Support Bundle.
4. Browse to select a location to save the support bundle .zip file and click (or tap) Save.
5. Send the support bundle to One Identity Support. For more information, see About us on page 517.

Related Topics

Troubleshooting
Frequently asked questions

Time

Time displays the current appliance time and allows you to enable Network Time Protocol (NTP) and set the primary and secondary NTP servers. In addition, when enabled, the NTP client status can be displayed.

It is the responsibility of the Appliance Administrator to manage the appliance time.

- **NOTE:** A warning will appear if your local time is not within 5 minutes of the appliance time. One Identity recommends that you set an NTP server to eliminate possible time-related issues.

- **NOTE:** **Clustered environments:** NTP setting changes are made on the primary appliance in a cluster. When a replica appliance is enrolled into the cluster, it points to the primary appliance's VPN IP address as the Primary NTP Server and the NTP client service is enabled on the replica appliance. When performing a failover operation to promote a replica to be the new primary, the Primary NTP Server is preserved and applied from the 'old' primary appliance.

To enable Network Time Protocol (NTP) and set the primary and secondary NTP servers

1. In Settings, select Appliance | Time.
2. Select the Enable Network Time Protocol (NTP) check box to enable NTP.
3. Provide the following information:
   - **Primary NTP Server:** Enter the IP address or DNS name of the primary NTP server.
- **Secondary NTP Server**: (Optional) Enter the IP address or DNS name of the secondary NTP server.

4. Click (or tap) **OK** to save your selections.

When NTP is enabled, the following information about the NTP client status is displayed:

- Last Sync Time
- Leap Indicator
- Poll Interval
- Precision
- Reference ID
- Root Delay
- Root Dispersion
- Source
- Stratum

**NOTE:** Select **Show Details** and **Hide Details** to display more or less information.

### Related Topics

How do I set the appliance system time

### Updates

It is the responsibility of the Appliance Administrator to update or upgrade One Identity Safeguard by installing an update file to modify the software or configuration of the running appliance.

Download the latest update from: https://support.oneidentity.com/one-identity-safeguard/.

**NOTE:** **Clustered environment**: Apply the patch so all appliances in the cluster are on the same version. The procedure for patching cluster members depends on the Safeguard version you are currently running.

- If you are running Safeguard 2.0.1.x or earlier, you must unjoin replica appliances, install the patch on each appliance, and then enroll the replica appliances to rebuild your cluster. For more information, see Patching cluster members in the *One Identity Safeguard 2.0 Administration Guide*.

- If you are running Safeguard 2.1.x or 2.2.x, you can use the enhanced cluster patching feature where unjoining replica appliances is no longer required. For more information, see Patching cluster members on page 409.
IMPORTANT: Always back up your system before you install an update file. For more information, see Safeguard Backup and Restore on page 292.

To install an update file

1. In Settings, select Appliance | Updates.
   The current appliance and client versions are displayed.
2. Click (or tap) Upload a File and browse to select an update file.
   NOTE: When you select a file, Safeguard uploads it to the server, but does not install it.
3. Once the file has successfully uploaded, click (or tap) one of the following:
   - Install Now to install the update file.
     NOTE: Once you install an update file, you cannot uninstall it.
   - Remove to delete the file from the server without installing it.
   The Updates pane shows the upgrade progress and when the appliance has been successfully upgraded.

Asset Management settings

Use the Asset Management settings to configure the schedule and settings used by discovery jobs that find privileged accounts or systems on your network, and to define and manage dynamic tags.

Table 152: Asset Management settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Discovery</td>
<td>Where you configure the rules Safeguard uses to perform asset account discovery.</td>
</tr>
<tr>
<td></td>
<td>NOTE: The rules configured here only apply to asset accounts. For more information on configuring discovery rules for directory accounts, see Managing directory account discovery jobs on page 195.</td>
</tr>
<tr>
<td>Directory Tags</td>
<td>Where you view and manage dynamic tags for directory accounts.</td>
</tr>
<tr>
<td>Tags</td>
<td>Where you view and manage dynamic tags for assets and asset accounts.</td>
</tr>
</tbody>
</table>
Account Discovery

Account Discovery settings are the rules Safeguard uses to perform account discovery against the assets that are in the scope of a partition profile.

There are two ways to configure and schedule account discovery jobs. You can set up discovery rules in Settings | Asset Management | Account Discovery and then add them to a profile or you can add a new discovery setting as you create a new profile.

You can configure the setting to automatically add all the discovered accounts to Safeguard for management, or you can configure the setting to allow you to manually include the discovered accounts.

The Account Discovery pane displays the following about the listed account discovery settings.

Table 153: Account Discovery Settings: Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the account discovery setting.</td>
</tr>
<tr>
<td>Partition</td>
<td>The partition on which Safeguard runs the selected account discovery setting.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the selected account discovery setting.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Displays the selected account discovery setting's schedule.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage the account discovery settings.

Table 154: Account Discovery Settings: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Account Discovery Setting</td>
<td>Add an account discovery setting. For more information, see Adding an asset account discovery setting on page 268.</td>
</tr>
<tr>
<td>Delete Selected</td>
<td>Remove the selected account discovery setting.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of account discovery settings.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modify the selected account discovery setting.</td>
</tr>
<tr>
<td>Copy</td>
<td>Clone the selected account discovery setting.</td>
</tr>
</tbody>
</table>

Related Topics

Account discovery job workflow
Creating a partition profile
Adding an asset account discovery setting

It is the responsibility of the Asset Administrator or the partition’s delegated administrator to configure the rules that govern how Safeguard performs account discovery. For more information, see Account discovery job workflow on page 491.

NOTE:
Safeguard supports account discovery on the following platforms:
- AIX
- HP-UX
- Linux
- MAC OS X
- Solaris
- Windows

To add an asset account discovery setting

1. In Settings, select Asset Management | Account Discovery.
2. Click (or tap) + Add Account Discovery Setting to open the Account Discovery Settings dialog.
3. In the Account Discovery Settings dialog, provide the following:
   a. **Partition**: Browse to select a partition.
   b. **Name**: Enter a name for the account discovery setting.
      Limit: 50 characters
      Required
   c. **Description**: Enter descriptive text about the account discovery setting.
      Limit: 255 characters
   d. **Schedule**: Click (or tap) the Schedule button and choose an interval.
      In the Schedule dialog,
      - **Interval**: Choose **Never**, **Minute**, **Hour**, **Day**, **Week**, or **Month**.
      | **NOTE**: **Best Practice**: Do not use the **Minute** interval.
      - **Time of day**: Set the start time.
      - **Repeat interval**: Select the interval you would like to repeat the account discovery task.
        - If **Weekly**, select which days of the week you want to repeat the account discovery task.
        - If **Monthly**, set the task recurrence pattern: Day of month or week of month and day of week.
- **Time Zone**: Select the time zone.

e. **Find all accounts**: Select this option to discover all accounts assigned to the assets in the selected partition.

f. **Find accounts based on rules**: Select this option to discover only accounts that match a discovery rule’s criteria. When you select this option Safeguard displays a list of discovery rules configured for this partition and allows you to add a new rule. For more information, see Adding an asset account discovery rule on page 269.

g. **Automatically Manage Found Accounts**: Select this check box to automatically add the discovered accounts to Safeguard.

### Adding an asset account discovery rule

When you select the **Find account based on rules** option in the **Account Discovery Settings** dialog, Safeguard displays a list of discovery rules configured for this partition and allows you to add a new rule.

**NOTE**: Account discovery is not available for Macintosh OS X platforms.

**NOTE**: **All search terms return exact matches**. A user name search for "ADM" only returns "ADM", not "AADMM" or "1ADM2". To find all names that contain "ADM", you must include ".*" in the search term; like this: ".*ADM.*

**All search terms are case sensitive**. On Windows platforms (which are case insensitive), to find all accounts that start with "adm", regardless of case, you must enter `[Aa][Dd][Mm].*`.

### To add an asset account discovery rule

1. In the Account Discovery Settings dialog, select the **Find accounts based on rules** option to open the Add Discovery Rule window.

   **NOTE**: For information about how to find this option, see Adding an asset account discovery setting on page 268.

2. Click (or tap) **Add Discovery Rule** to open the Account Discovery Rule dialog.

3. Set the discovery rule search criteria:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a unique name for the account discovery rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Limit</strong>: 50 characters</td>
<td>Required</td>
</tr>
</tbody>
</table>

   | RID           | Enter one or more Relative Identifier numbers. To enter multiple IDs or ID ranges, you must enter each element of the list separately. For example: enter **1000**, enter **5000-7000**, then enter **10000**. |

---

Safeguard 2.3 Administration Guide
Settings

Page 269
| NOTE: Spaces and commas are not allowed. |
| Limit: 255 numeric characters |

| GID | Enter one or more Group Identifier numbers. To enter multiple IDs or ID ranges, you must enter each element of the list separately. For example: enter 8, enter 10-12, then enter 15. |
| Limit: 255 numeric characters |

| UID | Enter one or more User Identifier numbers. To enter multiple IDs or ID ranges, you must enter each element of the list separately. For example: enter 1, enter 5-7, then enter 10. |
| Limit: 255 numeric characters |

| Name | Enter a single regular expression pattern. |
| Limit: 255 alphanumeric characters |

| Group | Enter a single regular expression pattern. |
| Limit: 255 alphanumeric characters |

4. To test the rule before saving it, click (or tap) **Preview**.
   The Assets dialog displays a list of assets assigned to this partition based on the criteria you set in this rule.

5. Select an asset on which to run the proposed discovery rule and click (or tap) **OK**.
   The Accounts dialog displays a preview list of all the accounts that meet the rule's criteria.

6. Close the Accounts list and return to the Account Discovery Rule dialog to click (or tap) **OK** to save the rule, or modify the rule criteria and re-run the Preview, if necessary.
   Safeguard adds the new rule to the Account Discovery Settings dialog.

7. Optionally select the **Automatically Manage Found Accounts** check box to automatically add the discovered accounts to Safeguard.

8. Click (or tap) **OK** to save the discovery job.

When Safeguard runs the discovery job, according to the schedule you have set, it displays the accounts it finds on the partition's **Discovered Accounts tab**.
Directory Tags

Directory administrators can define rules that will dynamically add tags to directory accounts so that they can be easily identified and added to dynamic groups. Use the Administrative Tools | Settings | Asset Management | Directory Tags pane to create and manage dynamic tags for directory accounts.

In addition, Asset administrators can manually add tags to directory accounts on the General tab of the Accounts view. For more information, see Manually adding a tag to an account.

The Directory Tags pane provides a centralized view of all the tags defined for directory accounts. It displays the following details.

Table 155: Directory Tags: Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name assigned to the tag when it was created.</td>
</tr>
<tr>
<td>Directories</td>
<td>The parent directory to which the tag belongs.</td>
</tr>
<tr>
<td>Rules</td>
<td>Indicates whether there is a rule associated with the selected tag. A check mark in this column indicates that the tag has a directory rule.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the tag.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage directory tags.

Table 156: Directory Tags: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ New</td>
<td>Add a dynamic tag definition. For more information, see Adding a tag for dynamic tagging of directory accounts on page 272.</td>
</tr>
<tr>
<td>! Delete</td>
<td>Remove the selected tag definition. For more information, see Deleting a directory account tag on page 274.</td>
</tr>
<tr>
<td>⌍ Refresh</td>
<td>Update the list of tags.</td>
</tr>
<tr>
<td>✎ Edit</td>
<td>Modify the selected tag definition. For more information, see Modifying a directory account tag on page 275.</td>
</tr>
</tbody>
</table>
| ⌒ Copy  | Clone the selected tag definition and assign it to one or more

NOTE: You cannot modify the directory assignment of an existing tag using the Edit operation. Use the Copy operation to clone the tag and assign it to an additional directory. Use the Delete operation to remove the tag from the existing directory.
### Additional directories

For more information, see [Copying a directory account tag to another directory](#) on page 277.

**NOTE:** If the tag already exists in the directory, the tag will be replaced with the cloned one.

### Occurrences

View a list of directory accounts that are assigned to the selected tag. For more information, see [Viewing directory account tag assignments](#) on page 278.

### Search

Search for a specific tag or set of tags in the list.

### Related Topics

*When does the rules engine run for dynamic grouping and tagging*

### Adding a tag for dynamic tagging of directory accounts

Use the **Add** button on the **Directory Tags** pane in the **Asset Management** settings page to add a dynamic tag for directory accounts.

#### To add a dynamic tag for directory accounts

1. Navigate to **Administrative Tools** | **Settings** | **Asset Management** | **Directory Tags**.
2. Click (or tap) the **+** toolbar button.
   
   The **New Tag** dialog displays.
3. On the **General** tab, enter the following information:
   
   - **Name**: Enter a unique name for the tag.
   - **Description**: Enter information about the tag.
   - **Partition**: Click (or tap) **Browse** to select the directory to which this tag is to be assigned.
4. On the **Directory Account Rule** tab, enter the conditions for a directory account rule.
   
   - **Don't include a directory account rule for this tag**: Select this check box if you do not want to include a directory account rule. Selecting this check box disables the rule editor controls on this page. Proceed to the next tab.
   - **Rule editor**: Use the rule editor to define conditions for tagging directory accounts.
### Table 157: Directory Account Rules tab: Rule editor controls

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| **AND | OR**       | Click (or tap) **AND** to "and" multiple search criteria together; where all criteria must be met in order to be included.  
Click (or tap) **OR** to "or" multiple search criteria together; where at least one of the criteria must be met in order to be included. |
| Attribute    | In the first query clause box, select the attribute to be searched. Valid attributes include:          |
|              |   - Name (Default)                                                                                  |
|              |   - Description                                                                                     |
|              |   - Platform                                                                                        |
|              |   - Disabled                                                                                        |
|              |   - Tag                                                                                             |
|              |   - Service Name                                                                                    |
|              |   - Domain Name                                                                                     |
|              |   - NETBIOS Name                                                                                    |
|              |   - Distinguished Name                                                                              |
|              |   - SID                                                                                             |
| Operator     | In the middle clause query box, select the operator to be used in the search. The operators available depend upon the data type of the attribute selected. 
For string attributes, the operators may include:                                             |
|              |   - Contains (Default)                                                                              |
|              |   - Does not contain                                                                                 |
|              |   - Starts with                                                                                      |
|              |   - Ends with                                                                                        |
|              |   - Equals                                                                                          |
|              |   - Not equal                                                                                       |
|              | For boolean attributes, the operators may include:                                                  |
|              |   - Is True                                                                                         |
|              |   - Is False                                                                                        |
| Search string| In the last clause query box, enter the search string or value to be used to find a match.          |
To delete a directory account tag

1. Navigate to Administrative Tools | Settings | Asset Management | Directory Tags.
2. Select the tag definition to be deleted.
3. Click (or tap) the Delete toolbar button.
4. On the Remove Selected confirmation dialog, click (or tap) Yes.
5. If the tag is being used, removing the tag may result in changes to your policy configuration; therefore, you are given the opportunity to confirm or cancel the remove operation.
- To remove the tag, enter **Force Delete** and click (or tap) **OK**.
- To cancel the remove operation, click (or tap) **Cancel**.

## Modifying a directory account tag

Use the **Edit** button on the **Directory Tags** pane on the **Asset Management** settings page to modify a directory account tag.

### To modify a directory account tag

1. Navigate to **Administrative Tools | Settings | Asset Management | Directory Tags**.
2. Select the tag to be modified.
3. Select the **edit** toolbar button.

   The **Directory Tag** dialog displays allowing you to modify the selected tag.
4. On the **General** tab, you can modify the following settings:
   - **Name**
   - **Description**

   **NOTE:** You cannot modify the directory assignment of an existing tag using the **Edit** operation. Use the **Copy** operation to clone the tag and assign it to an additional directory. Use the **Delete** operation to remove the tag from the existing directory.
5. On the **Directory Account Rules** tab, you can modify the conditions for the directory account rule.

   - **Don’t include a directory account rule for this tag**: Select this check box if you do not want to include a directory account rule. Selecting this check box disables the rule editor controls on this page. Proceed to the next tab.
   - **Rule editor**: Use the rule editor to modify the conditions for tagging directory accounts.

### Table 158: Directory Account Rules tab: Rule editor controls

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>**AND</td>
<td>OR**</td>
</tr>
<tr>
<td><strong>Property</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>--------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| **Attribute** | In the first query clause box, select the attribute to be searched. Valid attributes include:  
  - Name (Default)  
  - Description  
  - Platform  
  - Disabled  
  - Tag  
  - Service Name  
  - Domain Name  
  - NETBIOS Name  
  - Distinguished Name  
  - SID |
| **Operator** | In the middle clause query box, select the operator to be used in the search. The operators available depend upon the data type of the attribute selected.  
For string attributes, the operators may include:  
  - Contains (Default)  
  - Does not contain  
  - Starts with  
  - Ends with  
  - Equals  
  - Not equal  
For boolean attributes, the operators may include:  
  - Is True  
  - Is False |
| **Search string** | In the last clause query box, enter the search string or value to be used to find a match. |
| **Add| Remove** | Click (or tap) the **Add Grouping** button to add an additional set of conditions to be met. |
| **+ | −** | Click (or tap) **+** to the left of a search clause to add an additional clause to the search criteria.  
Click (or tap) **−** to remove the search clause from the search criteria. |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A new grouping is added under the last query clause in a group and appears in a bordered pane showing that it is subordinate to the higher level query conditions. Click (or tap) the <strong>Remove</strong> button to remove a grouping from the search criteria.</td>
</tr>
</tbody>
</table>

Click **Preview** to run the query in order to review the results of the query before adding the dynamic tag.

Click **Preview** at the bottom of the dialog to preview the effects the currently defined rule conditions will have on a group.

6. On the **Summary** tab, review your changes and click (or tap) **OK**.

**Copying a directory account tag to another directory**

Dynamic tags for directory accounts belong to a directory. Use the **Copy** button on the Directory Tags pane on the **Asset Management** settings page to clone a directory account tag and assign it to a different directory.

| NOTE: You cannot modify the directory assignment of an existing tag using the **Edit** operation. Use the **Copy** operation to clone the tag and assign it to an additional directory. Use the **Delete** operation to remove the tag from the existing directory. |

**To copy a directory account tag to another directory**

1. Navigate to Administrative Tools | Settings | Asset Management | Directory Tags.
2. Click (or tap) the **Copy** toolbar button.
   - The **Copy to** dialog displays allowing you to select one or more directories.
3. Select the check box for the directories to which the selected tag is to be assigned.
   - If you do not see the directory you are looking for, you can create a new directory by clicking **Create New**. Clicking **Create New** displays the Directory dialog allowing you to add a directory to Safeguard. For more information, see Adding a directory on page 188. You must have Directory Administrator permissions to add directories to Safeguard.
4. Click (or tap) **OK**.
   - If a tag with the same name already exits in the selected directory, you will be asked if you want to replace the tag.
Viewing directory account tag assignments

Use the **Occurrences** button on the **Directory Tags** pane on the **Asset Management** page to view a list of all directory accounts assigned to a dynamic tag.

**To view directory account tag assignments**

1. Navigate to **Administrative Tools | Settings | Asset Management | Directory Tags**.
2. Select a tag definition from the list.
3. Click (or tap) the ![Occurrences](image) toolbar button.
   - The **Occurrences** dialog displays, which contains a list of all the directory accounts assigned to the selected dynamic tag. This dialog includes the object name.
4. Use the Search box to locate a specific tag or set of tags in this list. Enter the character string to be used to search for a match.
5. Click (or tap) **Close** to close the dialog and return to the **Directory Tags** pane.

**Tags**

Asset administrators can define rules that will dynamically add tags to assets and asset accounts so that they can be easily identified and added to dynamic groups. Use the **Administrative Tools | Settings | Asset Management | Tags** pane to create and manage dynamic tags for assets and asset accounts.

In addition, Asset administrators can manually add tags to assets and accounts on the **General** tab of the **Assets** or **Accounts** view. For more information, see [Manually adding a tag to an asset](#) and [Manually adding a tag to an account](#).

The **Tags** pane provides a centralized view of all the tags defined for assets and asset accounts, regardless of how they were assigned. It displays the following details.

**Table 159: Tags: Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name assigned to the tag when it was created.</td>
</tr>
<tr>
<td>Asset Partition</td>
<td>The asset partition to which the tag belongs.</td>
</tr>
<tr>
<td>Rules</td>
<td>Indicates whether there is a rule associated with the selected tag. A check mark in this column indicates that the tag has an asset or asset account rule.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the tag.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage tags.
Table 160: Tags: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✦ New</td>
<td>Add a dynamic tag. For more information, see Adding a tag for dynamic tagging of assets or asset accounts on page 279.</td>
</tr>
<tr>
<td>Delete</td>
<td>Remove the selected tag. For more information, see Deleting an asset or asset account tag on page 283.</td>
</tr>
<tr>
<td>⌜ Refresh</td>
<td>Update the list of tags.</td>
</tr>
</tbody>
</table>
| ✒ Edit | Modify the selected tag. For more information, see Modifying an asset or asset account tag on page 284.  
  
  NOTE: You cannot modify the partition assignment of an existing tag using the Edit operation. Use the Copy operation to clone the tag and assign it to an additional partition. Use the Delete operation to remove the tag from the existing partition. |
| ☒ Copy | Clone the selected tag and assign it to one or more additional partitions. For more information, see Copying an asset or asset account tag to another partition on page 287.  
  
  NOTE: If the tag already exists in the partition, the tag will be replaced with the cloned one. |
| ⚬ Occurrences | View a list of assets and asset accounts that are assigned to the selected tag. For more information, see Viewing asset and asset account tag assignments on page 288. |
| Search | Search for a specific tag or set of tags in this list. |

Related Topics

When does the rules engine run for dynamic grouping and tagging

Adding a tag for dynamic tagging of assets or asset accounts

Use the ✦ New button on the Tags pane in the Asset Management settings page to add a dynamic tag for an asset or asset account.

To add an asset or asset account dynamic tag

1. Navigate to Administrative Tools | Settings | Asset Management | Tags.
2. Click (or tap) the ✦ toolbar button.
   The Tag dialog displays.
3. On the **General** tab, enter the following information:
   - **Name**: Enter a unique name for the tag.
   - **Description**: Enter information about the tag.
   - **Partition**: Click (or tap) **Browse** to select the partition to which this tag is to be assigned.

4. On the **Asset Account Rules** tab, enter the conditions for an asset account rule.
   - **Don't include an account rule for this tag**: Select this check box if you do not want to include an account rule. Selecting this check box disabled the rule editor controls on this page. Proceed to the next tab.
   - **Rule editor**: Use the rule editor to define conditions for tagging asset accounts.

<table>
<thead>
<tr>
<th>Table 161: Asset Account Rules tab: Rule editor controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Property</strong></td>
</tr>
<tr>
<td>**AND</td>
</tr>
<tr>
<td><strong>Attribute</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Operator</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
5. On the Asset Rules tab, enter the conditions for an asset rule.

- **Don't include an asset rule for this tag**: Select this check box if you do not want to include an asset rule. Selecting this check box disabled the rule editor controls on this page. Proceed to the next tab.

- **Rule editor**: Use the rule editor to define conditions for tagging assets.

### Table 162: Asset Rules tab: Rule editor controls

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AND</td>
<td>Click (or tap) <strong>AND</strong> to &quot;and&quot; multiple search criteria together; where all criteria must be met in order to be included.</td>
</tr>
<tr>
<td>OR</td>
<td>Click (or tap) <strong>OR</strong> to &quot;or&quot; multiple search criteria</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Attribute</td>
<td>In the first query clause box, select the attribute to be searched. Valid attributes include:</td>
</tr>
<tr>
<td></td>
<td>• Name (default)</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Platform</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
</tr>
<tr>
<td></td>
<td>• Tag</td>
</tr>
<tr>
<td></td>
<td>• Discovery Job Name</td>
</tr>
<tr>
<td></td>
<td>• Partition Name</td>
</tr>
<tr>
<td></td>
<td>• Profile</td>
</tr>
<tr>
<td></td>
<td>• Network Address</td>
</tr>
<tr>
<td>Operator</td>
<td>In the middle clause query box, select the operator to be used in the search. The operators available depend upon the data type of the attribute selected.</td>
</tr>
<tr>
<td></td>
<td>For string attributes, the operators may include:</td>
</tr>
<tr>
<td></td>
<td>• Contains (Default)</td>
</tr>
<tr>
<td></td>
<td>• Does not contain</td>
</tr>
<tr>
<td></td>
<td>• Starts with</td>
</tr>
<tr>
<td></td>
<td>• Ends with</td>
</tr>
<tr>
<td></td>
<td>• Equals</td>
</tr>
<tr>
<td></td>
<td>• Not equal</td>
</tr>
<tr>
<td></td>
<td>For boolean attributes, the operators may include:</td>
</tr>
<tr>
<td></td>
<td>• Is True</td>
</tr>
<tr>
<td></td>
<td>• Is False</td>
</tr>
<tr>
<td>Search string</td>
<td>In the last clause query box, enter the search string or value to be used to find a match.</td>
</tr>
<tr>
<td>+ / −</td>
<td>Click (or tap) + to the left of a search clause to add an additional clause to the search criteria.</td>
</tr>
<tr>
<td></td>
<td>Click (or tap) − to remove the search clause from the search criteria.</td>
</tr>
<tr>
<td>Add Grouping</td>
<td>Click (or tap) the Add Grouping button to add an</td>
</tr>
</tbody>
</table>
### Removing a dynamic tag

A new grouping is added under the last query clause in a group and appears in a bordered pane showing that it is subordinate to the higher level query conditions.

Click (or tap) the **Remove** button to remove a grouping from the search criteria.

### Previewing

Click (or tap) **Preview** to run the query in order to review the results of the query before adding the dynamic tag.

6. On the **Summary** tab, review your selections.

   - **Asset Account Rules**: Open the **Asset Account Rules** tab to review the conditions for an asset account rule.
   - **Asset Rules**: Open the **Asset Rules** tab to review the conditions for an asset rule.

7. Click (or tap) **Add** to create the tag, close the dialog, and return to the **Tags** pane.

### Deleting an asset or asset account tag

Click (or tap) **Delete** on the **Tags** pane in the **Asset Management** settings page to delete an asset or asset account tag from Safeguard.

**NOTE:** All references to a tag will be removed, no matter how it was assigned (dynamically or manually).

**NOTE:** A tag can be assigned to multiple object types. That is, you can have the same tag assigned to assets, asset accounts, and directory accounts.

#### To delete an asset or asset account tag

1. Navigate to **Administrative Tools | Settings | Asset Management | Tags**.
2. Select the tag to be deleted.
3. Click (or tap) the **Delete** toolbar button.
4. On the **Remove Selected** confirmation dialog, click (or tap) **Yes**.
5. If the tag is being used, removing the tag may result in changes to your policy configuration; therefore, you are given the opportunity to confirm or cancel the remove operation.
   - To remove the tag, enter **Force Delete** and click (or tap) **OK**.
   - To cancel the remove operation, click (or tap) **Cancel**.
Modifying an asset or asset account tag

Use the Edit button on the Tags pane on the Asset Management settings page to modify an asset or asset account tag.

**To modify an asset or asset account tag**

1. Navigate to Administrative Tools | Settings | Asset Management | Tags.
2. Select the tag to be modified.
3. Select the Edit toolbar button.
   The Tag dialog displays allowing you to modify the selected tag.
4. On the General tab, you can modify the following settings:
   - Name
   - Description

   **NOTE:** You cannot modify the partition assignment of an existing tag using the Edit operation. Use the Copy operation to clone the tag and assign it to an additional partition. Use the Delete operation to remove the tag from the existing partition.

5. On the Asset Account Rules tab, you can modify the conditions for an asset account rule.
   - **Don't include an account rule for this tag:** Select this check box if you do not want to include an account rule. Selecting this check box disables the rule editor controls on this page. Proceed to the next tab.
   - Rule editor: Use the rule editor to modify the conditions for tagging asset accounts.

   **Table 163: Asset Account Rules tab: Rule editor controls**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
   | **AND | OR** | Click (or tap) **AND** to "and" multiple search criteria together; where all criteria must be met in order to be included.  
   Click (or tap) **OR** to "or" multiple search criteria together; where at least one of the criteria must be met in order to be included. |
   | Attribute | In the first query clause box, select the attribute to be searched. Valid attributes include:  
   - Name (Default)  
   - Description |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td></td>
</tr>
<tr>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Tag</td>
<td></td>
</tr>
<tr>
<td>Service Account</td>
<td></td>
</tr>
<tr>
<td>Partition Name</td>
<td></td>
</tr>
<tr>
<td>Asset Tag</td>
<td></td>
</tr>
<tr>
<td>Operator</td>
<td>In the middle clause query box, select the operator to be used in the search. The operators available depend upon the data type of the attribute selected. For string attributes, the operators may include: · Contains (Default) · Does not contain · Starts with · Ends with · Equals · Not equal For boolean attributes, the operators may include: · Is True · Is False</td>
</tr>
<tr>
<td>Search string</td>
<td>In the last clause query box, enter the search string or value to be used to find a match.</td>
</tr>
<tr>
<td>Add Grouping</td>
<td>Click (or tap) the <strong>Add Grouping</strong> button to add an additional set of conditions to be met.</td>
</tr>
<tr>
<td>Remove</td>
<td>A new grouping is added under the last query clause in a group and appears in a bordered pane showing that it is subordinate to the higher level query conditions. Click (or tap) the <strong>Remove</strong> button to remove a grouping from the search criteria.</td>
</tr>
<tr>
<td>Preview</td>
<td>Click (or tap) <strong>Preview</strong> to run the query in order to review the results of the query before adding the dynamic tag.</td>
</tr>
</tbody>
</table>
6. On the **Asset Rules** tab, you can modify the conditions for an asset rule.

- **Do not include an asset rule for this tag**: Select this check box if you do not want to include an asset rule. Selecting this check box disables the rule editor controls on this page. Proceed to the next tab.
- **Rule editor**: Use the rule editor to modify the conditions for tagging assets.

### Table 164: Asset Rules tab: Rule editor controls

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>**AND</td>
<td>OR**</td>
</tr>
<tr>
<td><strong>Attribute</strong></td>
<td>In the first query clause box, select the attribute to be searched. Valid attributes include:</td>
</tr>
<tr>
<td></td>
<td>- Name (default)</td>
</tr>
<tr>
<td></td>
<td>- Description</td>
</tr>
<tr>
<td></td>
<td>- Platform</td>
</tr>
<tr>
<td></td>
<td>- Disabled</td>
</tr>
<tr>
<td></td>
<td>- Tag</td>
</tr>
<tr>
<td></td>
<td>- Discovery Job Name</td>
</tr>
<tr>
<td></td>
<td>- Partition Name</td>
</tr>
<tr>
<td></td>
<td>- Profile</td>
</tr>
<tr>
<td></td>
<td>- Network Address</td>
</tr>
<tr>
<td><strong>Operator</strong></td>
<td>In the middle clause query box, select the operator to be used in the search. The operators available depend upon the data type of the attribute selected. For string attributes, the operators may include:</td>
</tr>
<tr>
<td></td>
<td>- Contains (Default)</td>
</tr>
<tr>
<td></td>
<td>- Does not contain</td>
</tr>
<tr>
<td></td>
<td>- Starts with</td>
</tr>
<tr>
<td></td>
<td>- Ends with</td>
</tr>
<tr>
<td></td>
<td>- Equals</td>
</tr>
<tr>
<td></td>
<td>- Not equal</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>For boolean attributes, the operators may include:</td>
</tr>
<tr>
<td></td>
<td>• Is True</td>
</tr>
<tr>
<td></td>
<td>• Is False</td>
</tr>
<tr>
<td>Search string</td>
<td>In the last clause query box, enter the search string or value to be used to find a match.</td>
</tr>
<tr>
<td>+</td>
<td>−</td>
</tr>
<tr>
<td></td>
<td>Click (or tap) − to remove the search clause from the search criteria.</td>
</tr>
<tr>
<td>Add Grouping</td>
<td>Click (or tap) the Add Grouping button to add an additional set of conditions to be met.</td>
</tr>
<tr>
<td>Remove</td>
<td>A new grouping is added under the last query clause in a group and appears in a bordered pane showing that it is subordinate to the higher level query conditions.</td>
</tr>
<tr>
<td></td>
<td>Click (or tap) the Remove button to remove a grouping from the search criteria.</td>
</tr>
<tr>
<td>Preview</td>
<td>Click (or tap) Preview to run the query in order to review the results of the query before adding the dynamic tag.</td>
</tr>
</tbody>
</table>

7. On the Summary tab, review your changes and click (or tap) OK.

**Copying an asset or asset account tag to another partition**

Tags for assets and asset accounts belong to a partition. Use the **Copy** button on the Tags pane on the Asset Management settings page to clone an asset or asset account tag and assign it to a different partition.

**NOTE:** You cannot modify the partition assignment of an existing tag using the Edit operation. Use the **Copy** operation to clone the tag and assign it to an additional partition. Use the **Delete** operation to remove the tag from the existing partition.

**To copy an asset or asset account tag to another partition**

1. Navigate to Administrative Tools | Settings | Asset Management | Tags.
2. Click (or tap) the **i** toolbar button.
   The **Copy to** dialog displays allowing you to select one or more partitions.
3. Select the check box for the partitions to which the selected tag is to be assigned.
If you do not see the partition you are looking for, you can create a new partition by clicking **Create New**. Clicking **+** displays the **Partition** dialog allowing you to add a partition to Safeguard. For more information, see **Adding a partition** on page 237. You must have Asset Administrator permissions to add partitions to Safeguard.

4. Click (or tap) **OK**.

If a tag with the same name already exits in the selected partition, you will be asked if you want to replace the tag.

### Viewing asset and asset account tag assignments

Use the **Occurrences** button on the **Tags** pane on the Asset Management page to view a list of all the assets and asset accounts assigned to a tag.

#### To view asset and asset account tag assignments

1. Navigate to **Administrative Tools** | **Settings** | **Asset Management** | **Tags**.
2. Select a tag from the list.
3. Click (or tap) the **Occurrences** toolbar button.

   The **Occurrences** dialog displays, which contains a list of all the assets and asset accounts assigned to the selected dynamic tag. This dialog includes the object name and the type of object: asset or account.

4. Use the Search box to locate a specific tag or set of tags in this list. Enter the character string to be used to search for a match.
5. Click (or tap) **Close** to close the dialog and return to the **Tags** pane.

### Backup and Retention settings

Use the Backup and Retention settings to manage your Safeguard backups and archive servers.

It is the responsibility of the Appliance Administrator to configure the Safeguard backup and retention settings.

#### Table 165: Backup and Retention settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive Servers</td>
<td>Where you add and manage archive servers for storing backup files and session recordings.</td>
</tr>
<tr>
<td>Audit Log Management</td>
<td>Where you define the audit logs to be archived and purged as well as a schedule for performing the audit log archival task.</td>
</tr>
<tr>
<td>Safeguard Backup</td>
<td>Where you initiate or schedule a backup, upload or download a</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>and Restore</td>
<td>backup file, or specify the archive server where a backup file is to be stored.</td>
</tr>
<tr>
<td>Safeguard Backup Retention</td>
<td>Where you enable (or disable) backup retention and set the maximum number of backup files you want Safeguard to store on the appliance.</td>
</tr>
</tbody>
</table>

### About backups

One Identity Safeguard backs up the following:

- All settings, except:
  - Appliance IP address
  - Network Time Protocol (NTP) configurations
  - Domain Name System (DNS) configuration
- Transaction history
- All information about Safeguard objects:
  - Accounts
  - Account groups
  - Assets
  - Asset groups
  - Directories
  - Entitlements
  - Partitions
  - Users
  - User groups

Safeguard encrypts and signs the data before it makes it available for downloading to an off-appliance storage. Only a genuine Safeguard appliance can decrypt the backup and then only when it is on the appliance. This means that if a backup has been downloaded from an appliance for off-appliance storage, you must first upload it to an appliance, which will verify the signature, ensuring that it is an authentic backup for Safeguard.

### Archive Servers

Archive servers are external physical servers where you store backup files and session recordings. Use the Archive Servers page on the Backup and Retention settings view to configure and manage archive servers.
The Archive Servers page displays the following information about previously configured archive servers.

**Table 166: Archive Servers: Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the archive server.</td>
</tr>
<tr>
<td>Archive Method</td>
<td>The transfer protocol type being used.</td>
</tr>
<tr>
<td>Network Address</td>
<td>The network DNS name or IP address used to connect to the server over the network.</td>
</tr>
<tr>
<td>Storage Path</td>
<td>The file path where you want to store backup files on the archive server.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the archive server.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage archive server configurations.

**Table 167: Archive Servers: Toolbar**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✪ Add Archive Server</td>
<td>Add an archive server. For more information, see Adding an archive server on page 290.</td>
</tr>
<tr>
<td>🗑️ Delete Selected</td>
<td>Remove the selected archive server configuration.</td>
</tr>
<tr>
<td>⌁ Refresh</td>
<td>Update the list of archive server configurations.</td>
</tr>
<tr>
<td>✏️ Edit</td>
<td>Modify the selected archive server configuration.</td>
</tr>
</tbody>
</table>

**Adding an archive server**

Use the Archive Servers page on the Backup and Retention settings view to configure archive servers, which can then be selected to archive a backup file or assigned to an appliance to store its session recordings.

**To configure an archive server**

1. In Settings, select Backup and Retention | Archive Servers.
2. Click (or tap) ✪ Add Archive Server and provide the following:

   - Name: Enter the display name for the archive server. Limit: 100 characters
<table>
<thead>
<tr>
<th><strong>Required</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Network Address</strong></td>
</tr>
<tr>
<td><strong>Storage Path</strong></td>
</tr>
</tbody>
</table>
| **Archive Method** | Choose a transfer protocol type:  
  - **CIFS**: Common Internet File System.  
  - **SCP**: Secure Copy Protocol  
  - **SFTP**: Secure File Transfer Program Required |
| **Port** | The port used by SSH to log into the managed system.  
  ![NOTE](https://example.com) Not applicable for CIFS archive mode. |
| **Authentication Type** | Select the type of authentication to be used to access the archive server:  
  - Password (default)  
  - Directory Account  
  - SSH  
  ![NOTE](https://example.com) Not applicable for CIFS archive mode. |
| **SSH Key Generation and Deployment Settings** | If **SSH** is selected as the authentication type, select one of the following settings:  
  - Automatically Generate the SSH Key  
  - Install and Use SSH Key from Safeguard  
  Optionally, select **Manually Deploy the SSH key** check box  
  **Browse** to select the SSH key to be used. |
| **Account Name** | If **Password** or **SSH** is selected as the authentication type, enter the service account name. |
Password

If **Password** or **SSH** is selected as the authentication type, enter the service account password.

Service Account

If **Directory Account** is selected as the authentication type, click (or tap) **Select Account** to chose the service account is be used to access the archive server.

Auto Accept SSH Host Key

Select this check box to have Safeguard automatically accept the SSH host key when it creates the archive server.

**Test Connection**

Click this button to verify that the appliance can communicate with this archive server. For more information, see About **Test Connection** on page 142.

3. Click (or tap) **OK**.

Once you have configured your archive servers, you need to designate a target archive for both your backup files and session recordings.

- For backup files, see Archive Backup on page 296
- For session recordings, see Session Recordings Storage Management on page 363

### Audit Log Management

Safeguard allows you to define and schedule an audit log management task to purge audit logs from the Safeguard appliance and archive older audit logs to a designated archive server. Archiving audit logs allows you to keep critical and relevant data online and current while eliminating or archiving audit logs that are no longer required.

Use the **Audit Log Management** page on the **Backup and Retention** settings view to define and schedule when to perform an audit log archival task.

### Safeguard Backup and Restore

It is the responsibility of the Appliance Administrator to manage Safeguard backups.

The **Safeguard Backup and Restore** page lists this information for the backups that are currently in the database.

**Table 168: Safeguard Backup and Restore: Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>The date of the backup.</td>
</tr>
<tr>
<td>Time</td>
<td>The time of the backup.</td>
</tr>
<tr>
<td>Progress</td>
<td>The status of the backup: <em>Running</em> or <em>Complete</em>.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>File Size (MB)</td>
<td>The size of the backup file in megabytes.</td>
</tr>
<tr>
<td>Appliance Name</td>
<td>The name of the appliance.</td>
</tr>
<tr>
<td>Appliance Version</td>
<td>The version of the Safeguard appliance.</td>
</tr>
<tr>
<td>User</td>
<td>The name of the user that created the backup.</td>
</tr>
<tr>
<td>Last Archived Date</td>
<td>The date the selected backup ran.</td>
</tr>
<tr>
<td>Archive Server Name</td>
<td>The name of the server on which the backup was archived.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage Safeguard backups.

### Table 169: Safeguard Backup and Restore: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run Now</td>
<td>Create a backup copy of the data that is currently on the appliance.</td>
</tr>
<tr>
<td>✖️ Delete</td>
<td>Remove the selected backup file from the Backups page and the Safeguard database.</td>
</tr>
<tr>
<td>⌚️ Refresh</td>
<td>Update the list of backup files on the Backups page.</td>
</tr>
<tr>
<td>☀️ Settings</td>
<td>Where you configure an automatic backup schedule.</td>
</tr>
<tr>
<td>Download</td>
<td>Save the selected backup file in a location on your appliance.</td>
</tr>
<tr>
<td>Upload</td>
<td>Retrieve a backup file from a file location and add it to the Backups page list.</td>
</tr>
<tr>
<td>Restore</td>
<td>Overwrite the current data and restore Safeguard to the selected backup.</td>
</tr>
<tr>
<td>☑️ Archive</td>
<td>Store a backup file on an external archive server. For more information, see Archive Backup on page 296.</td>
</tr>
</tbody>
</table>

**TIP:** As a best practice, store backups on an archive server that is external from the appliance so that the backup image is available for restoration even if there is a catastrophic disk or hardware failure. Keep only a minimum number of backup files on the appliance. After you download or archive the backup files, use Delete to remove them from the desktop client application. You can set the maximum number of backup files you want Safeguard to retain on the appliance in Backup and Retention settings.
Run Now

To create a new backup
1. In Settings, select Backup and Retention | Safeguard Backup and Restore.
2. Click (or tap) Run Now.
   Safeguard makes a copy of the current database.

⚠️ CAUTION: If you restore a backup that is older than the Maximum Password Age set in the Login Control settings, all user accounts (including the bootstrap administrator) will be locked out and you will have to reset all of the user account passwords. To avoid this situation, you can reset the Maximum Password Age to zero before you perform the backup, then reset it after the restore.

 טי Tip: As a best practice, perform backups more frequently than the Maximum Password Age setting.

⚠️ CAUTION: Safeguard can not restore any access request workflow events in process at the time of a backup.

Backup Settings

✎ Settings is where you configure an automatic backup schedule.

To schedule backups
1. In Settings, select Backup and Retention | Safeguard Backup and Restore.
2. Click (or tap) Settings.
3. In the Backup Settings dialog, specify the backup schedule:
   a. Interval: Choose Never, Minute, Hour, Day, Week, or Month.
      ✨ NOTE: Best Practice: Do not use the Minute interval.
   b. Time of day: Set the start time.
   c. Repeat interval: Select the interval at which you would like to repeat the backup task.
   d. If Weekly, select which days of the week the backup task is to run.
   e. If Monthly, set the recurrence pattern. Select one of the following options and specify the monthly repeat interval:
      - Day of month
      - Week of month | Day of week
TIP: If you schedule a backup and a backup has already occurred for that interval (Minute, Hour, Day, Week, or Month), Safeguard will not execute another backup until the following minute, hour, day, week, or month. For example, if a backup has already occurred today and you set the backup schedule to run a daily backup, Safeguard will not run the backup until tomorrow.

f. **Time Zone**: Select the time zone.

g. Select **Send to archive server** to store the backup files externally from the appliance.

NOTE: This option is only available if you have configured an archive server. For more information, see Adding an archive server on page 290.

You configure the maximum number of backup files you want Safeguard to store on the appliance on the **Safeguard Backup Retention** page.

**Download**

Safeguard allows you to save a selected backup file in a location on your computer.

**To download the backup file**

1. In **Settings**, select **Backup and Retention | Safeguard Backup and Restore**.
2. Select a backup file and click (or tap) **Download**.
3. Browse to select a location of your choice.
4. Give the file a name and click (or tap) **OK**.

NOTE: Safeguard copies the backup file; it does not remove the backup from the list displayed on the Backup and Restore page.

**Upload**

Safeguard allows you to retrieve a backup file from a file location and add it to the **Safeguard Backup and Restore** page list on the appliance.

**To upload a backup file**

1. In **Settings**, select **Backup and Retention | Safeguard Backup and Restore**.
2. Click (or tap) **Upload**.
3. Browse to select a backup file and click (or tap) **Open**.
## Restore

Safeguard allows you to restore the data on your appliance to a selected backup.

⚠️ **CAUTION:** If you restore a backup that is older than the Maximum Password Age set in the Login Control settings, all user accounts (including the bootstrap administrator) will be disabled and you will have to reset all of the user account passwords. If your bootstrap administrator’s password is locked out, you can reset it from the recovery kiosk. For more information, see Admin password reset on page 466.

### To restore Safeguard to a backup

1. In **Settings**, select **Backup and Retention | Safeguard Backup and Restore**.
2. Select a backup.
   - 📌 **NOTE:** If the backup file is not listed, you can **Upload** it first.
3. Click (or tap) ☐️ **Restore**.
4. In the **Restore** dialog, enter the word **Restore** in the box and click (or tap) **OK**. Safeguard automatically restarts the appliance, if necessary.
5. Once the appliance is fully operational, it asks you to restart the Windows desktop client.
   - 📌 **NOTE:** All modifications to Safeguard objects since the backup was created will be lost.

⚠️ **CAUTION:** After a restore, requesters, approvers, and reviewers will not have access to any access request workflow events that were in process at the time of the backup. The Activity Center displays those workflow events as incomplete.

- 📌 **NOTE:** Safeguard does not restore the appliance IP address, NTP settings or the DNS settings. To verify that these settings are correct after a restore, go to **Settings | Appliance Information**.

## Archive Backup

Safeguard allows you to store backup files on an external archive server.

### To archive a backup file

1. In **Settings**, select **Backup and Retention | Safeguard Backup and Restore**.
2. Select the backup to be archived.
3. Click (or tap) 📁 **Archive** and select **Archive Backup**.
4. In the **Archive Servers** selection dialog, choose an archive server.
NOTE: You can add an archive server from the Archive Servers selection dialog by clicking the Add Archive Server toolbar button.

Safeguard copies the backup file to the archive server.

Safeguard Backup Retention

It is the responsibility of the Appliance Administrator to configure the maximum number of backup files you want Safeguard to store on the appliance.

To configure the appliance backup retention settings

1. In Settings, select Backup and Retention | Safeguard Backup Retention.
2. Select the Enable Backup Retention check box.
3. Enter the maximum number of backup files you want to store on the appliance.
4. Click (or tap) OK.

Once Safeguard saves the maximum number of backup files, next time it performs a backup, it deletes the backup file with the oldest date.

Certificates settings

Use the Certificate settings to manage the certificates used to secure One Identity Safeguard. The panes on this page display default certificates that can be replaced or user-supplied certificates that have been added to Safeguard.

It is the responsibility of the Appliance Administrator to manage the certificates used by Safeguard.

Table 170: Certificates settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Log Signing Certificate</td>
<td>Where you manage the audit log signing certificate used to validate audit logs stored on an archive server.</td>
</tr>
<tr>
<td>Certificate Signing Request</td>
<td>Where you can view and manage certificate signing requests (CSRs)</td>
</tr>
<tr>
<td>Sessions Certificates</td>
<td>Where you manage session certificates, including installing session certificates or creating CSRs to enroll a sessions certificate.</td>
</tr>
<tr>
<td>SSL Certificates</td>
<td>Where you manage SSL certificates, including installing SSL certificates or creating CSRs to enroll a public SSL certificate.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Trusted Certificates</td>
<td>Where you add and manage certificates trusted by Safeguard, for example your company’s root Certificate Authority (CA) certificate.</td>
</tr>
</tbody>
</table>

### About certificates

The certificate infrastructure in One Identity Safeguard consists of the following:

#### Replaceable certificates

One Identity Safeguard ships with the following default certificates which are meant to be replaced:

- A self-signed SSL certificate for HTTPS. The name of the SSL certificate matches the hostname of the Safeguard appliance and uses the appliance’s default IP addresses as the Subject Alternative Name (SAN).
- A self-signed Certificate Authority (CA) certificate used by the Privileged Sessions module that generates server SSL certificates on-the-fly to secure RDP connections when an RDP session is initiated using Safeguard. The "requester" must accept the certificate in order to launch a remote desktop session.
- A signing certificate used to validate that archived audit logs were created by and came from Safeguard.

#### User-supplied certificates

Safeguard allows you to specify the security certificates to be used. When replacing or adding certificates, keep the following considerations in mind:

- Safeguard supports Certificate Signing Requests (CSRs) to enroll any type of certificate. CSRs use the Public-Key Cryptography Standard (PKCS) #10 format.
- For uploading certificates with private keys, Safeguard supports .pfx (or .p12) files which follow the PKCS #12 standard.
- For SSL certificates, Safeguard allows you to upload or use a CSR to enroll multiple certificates that can then be applied to different appliances.
- Safeguard provides an SSL certificate store that allows you to assign any uploaded or enrolled SSL certificate to any appliance.
- Prior to adding an asset that uses SSL server certificate validation, you must add the server’s signing authority certificate to the Trusted Certificates store in Safeguard.
- For sessions certificates, uploading a new certificate or using a CSR to enroll a new certificate will replace the default certificate supplied with Safeguard.
# Audit Log Signing Certificate

The **Audit Log Signing Certificate** pane on the Certificates setting page displays details about the certificate used to sign the audit log files saved to an archive server. The audit log signing certificate proves that the audit logs were created by and came from a particular Safeguard cluster.

This signing certificate is used by administrators who want to verify that the exported Audit Log History originated from their Safeguard cluster. This certificate's public key, in addition to the certificate's issuer, must be available if you wish to validate the signed audit log.

**NOTE:** While Safeguard ships a default audit log signing certificate, One Identity recommends that you load your own.

If you replace the default certificate with your own, the certificate must have the following:

- Enhanced Key Usage extension with the Server Authentication (1.3.6.1.5.5.7.3.1) OID value.
- Digital Signature key Usage extension with the Server Authentication (2.5.29.37.3) OID value.

**NOTE:** It is recommended to generate the CSR from within the Safeguard user interface using the **Add Certificate | Create Certificate Signing Request (CSR)** option. The administrator will have a copy of the public key which will be used to verify the validity of the archived audit logs.

You can have only one audit log signing certificate defined, which is used by all Safeguard appliances in the same cluster. That is, Safeguard uses the default certificate or a certificate you uploaded to replace the default certificate.

The following properties and controls are available to manage your audit log signing certificate.

**Table 171: Audit Log Certificates: Properties**

<table>
<thead>
<tr>
<th>Properties/Controls</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Refresh</strong></td>
<td>Click (or tap) <strong>Refresh</strong> to update the certificate displayed on the <strong>Audit Log Certificates</strong> pane.</td>
</tr>
<tr>
<td>Subject</td>
<td>The name of the subject (such as user, program, computer, service or other entity) assigned to the certificate when it was requested.</td>
</tr>
<tr>
<td>Thumbprint</td>
<td>A unique hash value that identifies the certificate.</td>
</tr>
</tbody>
</table>
| **Add Certificate** | Click (or tap) **Add Certificate** and select one of the following options to replace the default certificate with a new certificate:  
  - Install Certificate generated from CSR  
  - Install Certificate with Private Key |
### Properties/Controls

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📜 Create Certificate Signing Request (CSR)</td>
<td></td>
</tr>
</tbody>
</table>

| Use Default | Click (or tap) Use Default to reset the certificate back to the default. |

### Installing an audit log signing certificate

If you do not want to use the default certificate provided with Safeguard, you can replace it with another certificate with a private key.

#### To install an audit log signing certificate

1. In **Settings**, select **Certificates | Audit Log Signing Certificates**.
2. Click (or tap) the **Add Certificate** button for the sessions certificate to be replaced. Select the appropriate option:
   - Install Certificate generated from CSR
   - Install Certificate with Private Key
3. **Browse** to select the certificate file (.pfx file) and click (or tap) **OK**.
4. Once installed, this new certificate will replace the default certificate listed on the **Audit Log Signing Certificates** pane.

### Creating a Certificate Signing Request for audit logs

If you do not want to use a default sessions certificate provided with Safeguard, you can enroll a certificate using a Certificate Signing Request (CSR) to replace the default certificate.

#### To create a CSR for an audit log signing certificate

1. In **Settings**, select **Certificates | Audit Log Signing Certificates**.
2. Click (or tap) the **Add Certificate** button for the certificate to be replaced and select **Create Certificate Signing Request (CSR)**.
3. In the **Certificate Signing Request** dialog, enter the following information:
   a. **Subject (Distinguished Name)**: Enter the distinguished name of the person or entity to whom the certificate is being issued. Maximum length of 500 characters.
NOTE: Click (or tap) **Use Distinguished Name Creator** to create the distinguished name based on fully-qualified domain name, department, organization unit, locality, state/county/region, and country.

b. **Alternate DNS Names**: Optionally, enter additional or alternate host names (such as, IP addresses, sites, common names) that are to be protected by this certificate.

c. **Key Size**: Select the bit length of the private key pair:
   - 1024
   - 2048 (default)
   - 4096

**NOTE**: The bit length determines the security level of the certificate. A higher bit length means stronger security.

4. Click (or tap) **OK** to save your selections and enroll the certificate.

Certificates enrolled via CSR are listed in the **Certificate Signing Request** pane.

**Certificate Signing Request**

Some certificates require a digital signature before a certification authority (CA) can process the certificate request. The Certificate Signing Request pane displays details about any certificates enrolled via Certificate Signing Requests (CSRs). From this pane, you can also delete a CSR.

**NOTE**: Safeguard supports the Public-Key Cryptography Standard (PKCS) #10 format for CSRs.

Certificates enrolled via a CSR appear on this pane including the following details.

**Table 172: Certificate Signing Request: Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>The distinguished name of the person or entity to whom the certificate is being issued.</td>
</tr>
<tr>
<td>Certificate Type</td>
<td>The type of certificate requested:</td>
</tr>
<tr>
<td></td>
<td>- Audit Log Signing Certificate</td>
</tr>
<tr>
<td></td>
<td>- RDP Connection Signing Certificate</td>
</tr>
<tr>
<td></td>
<td>- Session Recording Signing Certificate</td>
</tr>
<tr>
<td></td>
<td>- SSL Certificate</td>
</tr>
<tr>
<td></td>
<td>- Timestamping Authority Certificate</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Thumbprint</td>
<td>A unique hash value that identifies the certificate.</td>
</tr>
<tr>
<td>Key Size</td>
<td>The bit length of the private key pair.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage certificate signing requests.

**Table 173: Certificate Signing Request: Toolbar**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Delete Selected</strong></td>
<td>Delete the selected CSR from Safeguard.</td>
</tr>
<tr>
<td><strong>Refresh</strong></td>
<td>Update the list of CSRs.</td>
</tr>
</tbody>
</table>

**Sessions Certificates**

The **Sessions Certificates** pane on the Certificates setting page displays details about the certificates that are used by One Identity Safeguard to provide Privileged Sessions functionality.

- The Timestamping Certificate Authority and the Session Recording Signing Certificate are used to sign an SSH or RDP session recording.
- The RDP Connection Signing Certificate is specific to an RDP session. When an RDP connection is established through Safeguard, the Privileged Sessions module generates an RDP certificate which is then signed by the RDP Connection Signing Certificate. This generated certificate is then presented to the RDP client.

Each of these certificates must be trusted by the client workstations that will be making sessions requests and reviewing sessions. This may be accomplished by signing the certificates with an enterprise root authority that is trusted by the client workstations (recommended), or the certificates may be distributed to each workstation via group policy or other distribution means.

**NOTE:** While Safeguard ships with default certificates, One Identity recommends that you load your own.

**Table 174: Sessions Certificates**

<table>
<thead>
<tr>
<th>Certificate</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamping Certificate</td>
<td>This certificate is used to sign timestamps embedded in session recordings to prove when the session recording occurred.</td>
</tr>
<tr>
<td>Authority</td>
<td></td>
</tr>
</tbody>
</table>
NOTE: If you replace the default certificate with your own, the certificate must have:

- a Key Usage extension with a Digital Signature value
- an Enhanced Key Usage extension, marked as critical, with the Time Stamping (1.3.6.1.5.5.7.3.8) OID value

You must also have the certificate's private key.

When playing back recorded sessions using the Safeguard Desktop Player, this certificate's public key, in addition to the certificate's issuer, must be available if you wish to validate the signed timestamps.

### Session Recording Signing Certificate

This certificate is used to sign the session recording files to prevent manipulation and prove that they were created by, and came from, Safeguard.

NOTE: If you replace the default certificate with your own, the certificate must have an Enhanced Key Usage extension with the Server Authentication (1.3.6.1.5.5.7.3.1) OID value

You must also have the certificate's private key.

When playing back recorded sessions using the Safeguard Desktop Player, this certificate's public key, in addition to the certificate's issuer, must be available if you wish to validate the signed recording.

### RDP Connection Signing Certificate

This is a Certificate Authority (CA) certificate that issues the server SSL certificate presented when a user connects a privileged session via RDP. Each time that an RDP connection is established through Safeguard, an SSL certificate is generated by this CA on-the-fly; therefore, this CA certificate should already be trusted as part of the customer's enterprise PKI.

You must also have the certificate's private key.

You can have only one certificate of each type defined. That is, Safeguard uses the default certificate or a certificate you uploaded to replace the default certificate.

For each of these certificates, the following properties and controls are available to manage your sessions certificates.

### Table 175: Sessions Certificates: Properties

<table>
<thead>
<tr>
<th>Properties/Controls</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>Click (or tap) <strong>Refresh</strong> to update the list of certificates on the Sessions Certificates pane.</td>
</tr>
<tr>
<td>Subject</td>
<td>The name of the subject (such as user, program, computer, service or other entity) assigned to the certificate when it was</td>
</tr>
</tbody>
</table>
Properties/Controls | Description
--- | ---
Thumbprint | A unique hash value that identifies the certificate.
**Add Certificate** | Click (or tap) **Add Certificate** and select one of the following options to replace the default certificate with a new certificate:
- **Install Certificate generated from CSR**
- **Install Certificate with Private Key**
- **Create Certificate Signing Request (CSR)**
**Use Default** | Click (or tap) **Use Default** to reset the certificate back to the default.

Related Topics

- What is required for One Identity Safeguard Privileged Sessions
- How do I prevent Safeguard messages when making RDP connections

## Installing a sessions certificate

If you do not want to use the default certificate provided with Safeguard, you can replace it with another certificate with a private key.

**NOTE:** For uploading certificates with private keys, Safeguard supports .pfx (or .p12) files which follow the PKCS #12 standard.

**To install a session certificate**

1. In **Settings**, select **Certificates | Sessions Certificates**.
2. Click (or tap) the **Add Certificate** button for the sessions certificate to be replaced. Select the appropriate option:
   - **Install Certificate generated from CSR**
   - **Install Certificate with Private Key**
3. **Browse** to select the certificate file (.pfx file) and click (or tap) **OK**.
4. Once installed, this new certificate will replace the default certificate listed on the **Sessions Certificates** pane.
Creating a Certificate Signing Request for Sessions

If you do not want to use a default sessions certificate provided with Safeguard, you can enroll a certificate using a Certificate Signing Request (CSR) to replace the default certificate.

To create a CSR for a sessions certificate

1. In Settings, select Certificates | Sessions Certificates.
2. Click (or tap) the Add Certificate button for the certificate to be replaced and select Create Certificate Signing Request (CSR).
3. In the Certificate Signing Request dialog, enter the following information:
   a. Subject (Distinguished Name): Enter the distinguished name of the person or entity to whom the certificate is being issued. Maximum length of 500 characters.
      
      NOTE: Click (or tap) Use Distinguished Name Creator to create the distinguished name based on fully-qualified domain name, department, organization unit, locality, state/county/region, and country.

   b. Alternate DNS Names: Optionally, enter additional or alternate host names (such as, IP addresses, sites, common names) that are to be protected by this certificate.

   c. Key Size: Select the bit length of the private key pair:
      
      - 1024
      - 2048 (default)
      - 4096

      NOTE: The bit length determines the security level of the certificate. A higher bit length means stronger security.

4. Click (or tap) OK to save your selections and enroll the certificate.

        Certificates enrolled via CSR are listed in the Certificate Signing Request pane.

Resetting to use default certificate

If you have uploaded and replaced a default sessions certificate, you can reset this user-supplied certificate to use the default certificate provided with Safeguard.
To reset a certificate back to the default sessions certificate:

1. In Settings, select Certificates | Sessions Certificates.
2. Click (or tap) Use Default for the certificate that is to be reset to use the default certificate.
3. In the Use Default confirmation dialog, enter the word default and click (or tap) OK.
   Once installed, the default certificate will display in the Sessions Certificates pane and be used by the Privileged Sessions module.

SSL Certificates

Safeguard enables an Appliance Administrator to upload SSL certificates with private keys or enroll SSL certificates via a CSR.

**NOTE:** Initially, the default self-signed SSL certificate used for HTTPS is listed and assigned to the appliance. This default certificate is not a trusted certificate and should be replaced.

The SSL Certificates pane displays the following information for the SSL certificates stored in the database.

**Table 176: SSL Certificates: Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliances</td>
<td>Lists the name of the appliance to which the certificate is assigned.</td>
</tr>
<tr>
<td>Subject</td>
<td>The name of the subject (such as user, program, computer, service or other entity) assigned to the certificate when it was requested.</td>
</tr>
<tr>
<td>Alternate DNS Names</td>
<td>Additional or alternate host names (such as, IP addresses, sites, common names) that were specified when the certificate was requested.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> For the default self-signed SSL certificate, the name and IP address of the appliance is used.</td>
</tr>
<tr>
<td>Invalid Before</td>
<td>A &quot;start&quot; date and time that must be met before a certificate can be used.</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>The date and time when the certificate expires and can no longer be used.</td>
</tr>
<tr>
<td>Thumbprint</td>
<td>A unique hash value that identifies the certificate.</td>
</tr>
<tr>
<td>Issued By</td>
<td>The name of the certificate authority (CA) that issued the certificate.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage SSL certificates.
### Table 177: SSL Certificates: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Add Certificate</td>
<td>Upload an SSL certificate. For more information, see <em>Installing an SSL certificate</em> on page 307.</td>
</tr>
<tr>
<td>+ Add Certificate</td>
<td>Create a CSR to enroll a certificate. For more information, see <em>Creating a Certificate Signing Request (CSR)</em> on page 308.</td>
</tr>
<tr>
<td></td>
<td>Assign the selected certificate to one or more appliances. For more information, see <em>Assigning a certificate to appliances</em> on page 308.</td>
</tr>
<tr>
<td>✖ Unassign Certificate</td>
<td>Unassign the selected certificate from one or more appliances.</td>
</tr>
<tr>
<td>✖ Delete Selected</td>
<td>Delete the selected certificate from Safeguard.</td>
</tr>
<tr>
<td>✡ Refresh</td>
<td>Update the list of SSL certificates available (uploaded to Safeguard).</td>
</tr>
</tbody>
</table>

### Installing an SSL certificate

**To install an SSL certificate**

1. In *Settings*, select Certificates | SSL Certificates.
2. Click (or tap) + Add Certificate and select Upload Certificate.
3. Browse to select the certificate file.
4. After the certificate has been uploaded, assign the certificate to one or more appliances. For more information, see *Assigning a certificate to appliances* on page 308.
   
   You may also upload the certificate's root CA to the list of trusted certificates. For more information, see *Trusted Certificates* on page 309.

| CAUTION: Improper access to the private SSL key could compromise traffic to and from the appliance. For the most secure configuration, create a Certificate Signature Request (CSR) and have it signed by your normal signing authority.

Then use the signed request as your Safeguard SSL Webserver Certificate. This way, no administrator will have access to the private SSL key that is used by Safeguard and the traffic will be secure.
Creating a Certificate Signing Request

A certificate signing request (CSR) is submitted to a Certificate Authority (CA) to obtain a digitally signed certificate. When creating a CSR, you uniquely identify the user or entity that will use the requested certificate. Safeguard allows you to upload or enroll SSL certificates using CSRs. Once uploaded or enrolled, the SSL certificate is added to the SSL certificate store allowing you to assign it to one or more Safeguard appliances.

To create a CSR for SSL

1. In Settings, select Certificates | SSL Certificates.
2. Click (or tap) + Add Certificate and select Create Certificate Signing Request (CSR).
3. In the Certificate Signing Request dialog, enter the following information:
   a. Subject (Distinguished Name): Enter the distinguished name of the person or entity to whom the certificate is being issued. Maximum length of 500 characters.
      
      NOTE: Click (or tap) Use Distinguished Name Creator to create the distinguished name based on fully-qualified domain name, department, organization unit, locality, state/county/region, and country.
   b. Alternate DNS Names: Optionally, enter additional host names (such as, IP addresses, sites, common names) that are to be protected by this certificate.
   c. Key Size: Select the bit length of the private key pair:
      - 1024
      - 2048 (default)
      - 4096
      
      NOTE: The bit length determines the security level of the SSL certificate. A higher bit length means stronger security.
4. Click (or tap) OK to save your selections and enroll the certificate.

Certificates enrolled via CSR are listed in the SSL Certificates pane and the Certificate Signing Request pane.

Assigning a certificate to appliances

Safeguard supports an SSL certificate store that is owned by the cluster. This allows you to assign any SSL certificate that you have previously uploaded or enrolled via CSR to any appliance in your clustered environment.
To assign a certificate to appliances

1. In Settings, select Certificates | SSL Certificates.
2. Select a certificate from the grid and click (or tap) the Assign Certificate to Appliance(s) toolbar button.
3. In the Appliances selection dialog, select one or more appliances and click (or tap) OK to save your selection.

Trusted Certificates

It is the responsibility of the Appliance Administrator to add or remove trusted root certificates to the Safeguard appliance, if necessary, in order for the SSL certificate to resolve the chain of authority. When Safeguard connects to an asset that has the Verify SSL Certificate option enabled, Safeguard compares the signing authority of the certificate presented by the asset to the certificates in the trusted certificate store.

The Trusted Certificates pane displays the following information for the user-supplied certificates added to the trusted certificate store.

Table 178: Trusted certificates: Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>The name of the subject (such as user, program, computer, service or other entity) assigned to the certificate when it was requested.</td>
</tr>
<tr>
<td>Invalid Before</td>
<td>A &quot;start&quot; date and time that must be met before a certificate can be used.</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>The date and time when the certificate expires and can no longer be used.</td>
</tr>
<tr>
<td>Thumbprint</td>
<td>A unique hash value that identifies the certificate.</td>
</tr>
<tr>
<td>Issued By</td>
<td>The name of the certificate authority (CA) that issued the certificate.</td>
</tr>
</tbody>
</table>

Adding a trusted certificate

Prior to adding an asset that uses SSL server certificate validation, add the certificate's root CA and any intermediate CAs to the Trusted Certificates store in Safeguard.

To add a trusted certificate

1. In Settings, select Certificates | Trusted Certificates.
2. Click (or tap) + Add Certificate from the details toolbar.
3. Browse to select a certificate file (DER Encoded file: .cer or .der).
4. Click (or tap) **Open** to add the selected certificate file to Safeguard.

**Removing a trusted certificate**

*To remove certificates from the appliance*

1. In **Settings**, select **Certificates | Trusted Certificates**.
2. Select a certificate.
3. Click (or tap) **Delete Selected** from the details toolbar.
   
   **IMPORTANT:** Safeguard does not allow you to remove built-in certificate authorities.

**Cluster settings**

Use the Cluster settings to create a clustered environment, to monitor the health of the cluster and its members, and to define managed networks.

Before creating a Safeguard cluster, it is recommended you read the Disaster recovery chapter to gain a better understanding of how clustering works in Safeguard.

A Safeguard cluster consists of two or more Safeguard appliances configured to communicate over TCP port 655. One appliance in the cluster is designated as the "primary". Non-primary appliances are referred to as "replicas".

It is the responsibility of the Appliance Administrator or the Operations Administrator to create a cluster, monitor the status of the cluster, and define managed networks.

**Table 179: Cluster settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Management</td>
<td>Where you create and manage a cluster and monitor the health of the cluster and its members.</td>
</tr>
<tr>
<td>Managed Networks</td>
<td>Where you define managed networks to distribute the task load for the clustered environment.</td>
</tr>
</tbody>
</table>

**Cluster Management**

The **Cluster Management** page is divided into the following panes:
• **Cluster view pane**: The left pane displays a graphical representation of each appliance belonging to the cluster.

• **Appliance details and cluster health pane**: The right pane displays details about the appliance selected in the left pane. From this pane you can run maintenance and diagnostic tasks against the selected appliance.

   **NOTE**: If you do not see the right pane, click (or tap) an appliance node in the left pane.

Use these toolbar buttons on the **Cluster Management** page to manage the members of a cluster.

**Table 180: Cluster Management: Toolbar**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>← Back</td>
<td>Return to the main Settings view.</td>
</tr>
<tr>
<td>† Add Replica</td>
<td>Join an appliance to the primary appliance as a replica. For more information, see Enrolling replicas into a cluster on page 403.</td>
</tr>
<tr>
<td>⏰ Refresh</td>
<td>Update the list of appliances in a cluster.</td>
</tr>
<tr>
<td>‼️ Reset Cluster</td>
<td>Reset a cluster to recover a cluster that has lost consensus. For more information, see Resetting a cluster that has lost consensus on page 412.</td>
</tr>
</tbody>
</table>

**CAUTION**: Resetting a cluster should be your last resort. It is recommended that you restore from a backup rather than reset a cluster.

**Cluster view pane**

Initially, the Cluster view pane (left pane) displays a single "primary" node for the appliance you are currently logged into. As you join appliances to the cluster, replica nodes will be shown as being connected to the primary node.

The "health" indicators on the nodes and in the upper right corner of this pane provide a quick view as to whether cluster members are in an error, warning, or healthy state.

Clicking a member of the cluster in this pane displays details about the appliance and the health of the cluster member. For more information, see Appliance details and cluster health pane on page 311.

**Appliance details and cluster health pane**

Cluster members periodically query other appliances in the cluster to obtain their health information. Cluster member information and health information is cached in memory,
with the most recent results displayed on the Cluster settings screen.
In the cluster view (left pane), click (or tap) a member of the cluster to refresh the display
of the right pane. From the right pane you can monitor the health of the selected appliance
and perform operations against the appliance.

Table 181: Cluster health toolbar buttons

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔴 Unjoin</td>
<td>Click (or tap) 🔴 Unjoin to remove a replica from the cluster. For more information, see Unjoining replicas from a cluster on page 404.</td>
</tr>
<tr>
<td>🔄 Failover</td>
<td>Click (or tap) 🔄 Failover to promote a replica to the primary appliance. For more information, see Failing over to a replica by promoting it to be the new primary on page 406.</td>
</tr>
<tr>
<td>⚡ Activate</td>
<td>Click (or tap) ⚡ Activate to activate a read-only appliance so it can add, modify and delete data. For more information, see Activating a read-only appliance on page 407.</td>
</tr>
</tbody>
</table>

⚠️ CAUTION: Activating this appliance will take it out of the read-only state and enable password check and change for managed accounts. Ensure that no other Safeguard appliance is actively monitoring these accounts, otherwise access to managed accounts could be lost. |
| 📣 Note: This option is only available for read-only appliances that are online. For example, appliances that have been unjoined from a Safeguard cluster or restored from a backup. |

🔍 Diagnose | Click (or tap)🔍 Diagnose to open the Diagnostics pane where you can perform the following: |
<p>| | • View appliance information. For more information, see Appliance Information on page 251. |
| | • Run diagnostic tests against the appliance. For more information, see Diagnostics on page 254. |
| | • Perform a factory reset. For more information, see Factory Reset from the desktop client on page 258. |
| | • View or edit networking settings. For more information, see Networking on page 261. |
| | • Generate a support bundle. For more information, see |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Support Bundle</strong> on page 263.</td>
<td>View or edit time settings. For more information, see Time on page 264.</td>
</tr>
<tr>
<td><strong>Check Health</strong></td>
<td>Click (or tap) <strong>Check Health</strong> to capture and display the current state of the selected appliance.</td>
</tr>
<tr>
<td><strong>Restart</strong></td>
<td>Click (or tap) <strong>Restart</strong> to restart the selected appliance. Confirm your intentions by entering a <strong>Reason</strong> and clicking (or tapping) <strong>Restart</strong>.</td>
</tr>
</tbody>
</table>

Below the toolbar, this pane displays the following information about the appliance selected in the cluster view.

**Table 182: Appliance properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance name</td>
<td>The name of the appliance.</td>
</tr>
<tr>
<td>IP address</td>
<td>The IPv4 address (or IPv6 address) of the appliance configuration interface. <strong>NOTE:</strong> You can modify the appliance IP address using the web client. For more information, see How do I modify the appliance configuration settings on page 484.</td>
</tr>
<tr>
<td>Appliance type</td>
<td>Indicates either <strong>Primary</strong> or <strong>Replica</strong>.</td>
</tr>
<tr>
<td>Appliance state</td>
<td>Indicates the appliance state. For a list of available states, see Appliance states on page 416.</td>
</tr>
<tr>
<td>Disk Space</td>
<td>The amount of used and free disk space.</td>
</tr>
</tbody>
</table>

Click (or tap) **View More** to show or hide this additional information:

**Appliance**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>The serial number of the appliance.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The amount of time (days, hours, and minutes) the appliance has been running.</td>
</tr>
</tbody>
</table>
Primary (displayed on replicas)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Address</td>
<td>The network DNS name or the IP address of the primary appliance in the cluster.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The media access control address (MAC address), a unique identifier assigned to the network interface for communications.</td>
</tr>
<tr>
<td>Link Present</td>
<td>Displays either Yes or No to indicate if there is an open communication link.</td>
</tr>
<tr>
<td>Link Latency</td>
<td>The amount of time (in milliseconds) it takes for the primary to communicate with the replica. Network latency is an expression of how much time it takes for a packet of data to get from one designated point to another. Ideally latency is as close to zero as possible.</td>
</tr>
</tbody>
</table>

Information

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Health Check</td>
<td>Last date and time Safeguard obtained the selected appliance's information.</td>
</tr>
<tr>
<td>Version</td>
<td>The appliance version number.</td>
</tr>
</tbody>
</table>

Managed Networks

Managed networks are named lists of network segments that can be serviced by specific Safeguard appliances within a clustered environment. Managed networks are used for scheduling tasks, such as password change, account discovery, and asset discovery, in a clustered environment to distribute the task load. That is, using managed networks you can distribute the load in such a way that there is minimal cluster traffic and specify to use the appliances that are closest to the target asset to perform the actual task.

The Managed Networks page displays the following information about previously defined managed networks. Initially, this page contains the properties for the Default Managed Network, which implicitly includes all networks and is served by all appliances in the cluster.

Table 183: Managed Networks: Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name assigned to the managed network when it was added to Safeguard.</td>
</tr>
</tbody>
</table>
Use the Managed Networks page on the Cluster settings view to add managed networks, which can be used to distribute the task load in a clustered environment. It is the responsibility of the Appliance Administrator to define and maintain managed networks.

### Adding a managed network

Use the Managed Networks page on the Cluster settings view to add managed networks, which can be used to distribute the task load in a clustered environment. It is the responsibility of the Appliance Administrator to define and maintain managed networks.
To add a managed network

1. In Settings, select Cluster | Managed Networks.
2. Click (or tap) Add.
3. In the Managed Network dialog, provide the following information:
   a. Name: Enter the display name for the managed network.
      Limit: 50 characters
      Required
   b. Description: (Optional) Enter information about the managed network.
      Limit: 255 characters
   c. Subnets: Click (or tap) Add to specify the subnets, or group of hosts,
      to be managed.
      Enter each subnet using CIDR notation. For example, 0.0.0.0/0.
      NOTE: You can add a subnet to only one managed network. You will
      receive an error if you attempt to add the same subnet to another
      managed network. If you are unsure if an IP address has already been
      associated with a managed network, use the Resolve Network search
      box. For more information, see Resolving IP address on page 316.
   d. Managed By: Select the appliances to be used to manage the specified
      subnets.
      NOTE: You do not need to specify an appliance when you initially define a
      managed network. You can use the Edit button to specify the
      managing appliance at a later time.
4. Click (or tap) OK to save your selections and add the managed network.

Deleting a managed network

To delete a managed network

1. In Settings, select Cluster | Managed Networks.
2. Select the managed network to be deleted, click (or tap) Delete.
3. In the confirmation dialog, click (or tap) Yes.

Resolving IP address

As an Appliance Administrator you can use the Managed Networks page to search for an
IP address within a managed network’s list of subnets.
To find an IP address in a managed network

1. In Settings, select Cluster | Managed Networks.
2. In the Resolve Network search box, type the IP address, and press Enter.

The managed network that contains the subnet that most closely matches the IP address is highlighted. If there are no subnets that match the IP address, the Default Managed Network is highlighted.

External Integration settings

The Appliance Administrator can configure the appliance to send event notifications to various external systems, the integration with an external ticketing system, and configure both external and secondary authentication service providers. However, it is the Security Policy Administrator's responsibility to configure the Approval Anywhere feature.

Table 185: External Integration settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application to Application</td>
<td>Where you configure application registrations to use the Application to Application service, which allows third-party applications to retrieve credentials from Safeguard.</td>
</tr>
<tr>
<td>Approval Anywhere</td>
<td>Where you define the Safeguard users who are authorized to use Approval Anywhere to approve access requests.</td>
</tr>
<tr>
<td>Email</td>
<td>Where you configure Safeguard to automatically send email notifications when certain events occur.</td>
</tr>
<tr>
<td>External Federation</td>
<td>Where you configure a relying party trust relationship with one or more federated authentication servers or services.</td>
</tr>
<tr>
<td>Secondary Authentication</td>
<td>Where you configure the secondary authentication service providers in Safeguard.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Where you configure Safeguard to send SNMP traps to your SNMP console when certain events occur.</td>
</tr>
<tr>
<td>Starling</td>
<td>Where you join Safeguard to Starling to take advantage of other Starling services, such as Starling Two-Factor Authentication and Starling Identity Analytics &amp; Risk Intelligence.</td>
</tr>
<tr>
<td>Syslog</td>
<td>Where you configure Safeguard to send event notifications to a syslog server with details about the event.</td>
</tr>
<tr>
<td>Ticketing</td>
<td>Where you configure Safeguard to integrate with your company’s external ticket system.</td>
</tr>
</tbody>
</table>
Application to Application

In order for third-party applications to use the Application to Application service to integrate with the Safeguard vault, you must first register the application in Safeguard. This can be done using the Administrative Tools | Settings | External Integration | Application to Application pane.

The Application to Application pane displays a list of previously registered third-party applications. From this page, the Security Policy Administrator can add new application registrations, and modify or remove existing registrations.

The Application to Application pane displays the following details about application registrations.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name assigned to the application's registration.</td>
</tr>
<tr>
<td>Certificate User</td>
<td>The name of the certificate user associated with the registered application.</td>
</tr>
</tbody>
</table>

NOTE: If there is no certificate user listed for an application registration, contact your Security Policy Administrator to add one. The Application to Application service on the third-party application will not work with the Safeguard vault until a certificate user has been specified.

<table>
<thead>
<tr>
<th>Enable/Disable</th>
<th>Indicates whether the application registration is enabled. The toggle appears blue with the switch to the right when a registration is enabled and gray with the switch to the left when a registration is disabled. Click (or tap) the toggle to enable or disable an application registration.</th>
</tr>
</thead>
</table>

NOTE: When an application registration is disabled, Application to Application access is disabled for that third-party application until the registration is enabled again.

<table>
<thead>
<tr>
<th>Description</th>
<th>Information about the application's registration.</th>
</tr>
</thead>
</table>

Use these toolbar buttons to manage application registrations.

Table 187: Application to Application: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add an application registration to Safeguard. For more information, see Adding an application registration on page 321.</td>
</tr>
<tr>
<td>Delete Selected</td>
<td>Remove the selected application registration from Safeguard. For more information, see Deleting an application registration on page</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Refresh</strong></td>
<td>Update the list of application registrations.</td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td>Modify the selected application registration.</td>
</tr>
<tr>
<td><strong>API Keys</strong></td>
<td>Display the API keys that were generated for Access Request Broker or Credential Retrieval. An API key can then be copied and used in the third-party application to authenticate with Safeguard.</td>
</tr>
</tbody>
</table>

**NOTE:** For credential retrieval, the registration process generates an API key for each managed account. However, for access request broker, the registration process generates a single API key for all users or user groups that are added.

**About Application to Application functionality**

Using the Application to Application service, third-party applications can interact with Safeguard in the following ways:

- Credential retrieval: A third-party application can retrieve a credential from the Safeguard vault in order to perform automated functions on the target asset. In addition, you can replace hard coded passwords in procedures, scripts, and other programs with programmatic calls.

- Access request broker: A third-party application can initiate an access request on behalf of an authorized user so that the authorized user can be notified of the available request and log in to Safeguard to retrieve a password or start a session.

**Credential retrieval**

A credential retrieval request using the Application to Application service allows the third-party application to retrieve credentials from the Safeguard vault without having to go through the normal workflow process.

For example, say you have an automated system that performs a routine system diagnostic on various services in the data center every 24 hours. In order for the automated system to perform the diagnostics, it must first authenticate to the target server. Since all of the credentials for the target servers are stored in the Safeguard vault, the automated system retrieves the credentials for a specified system by calling the Application to Application service.
Access request broker

An access request broker request using the Application to Application service allows the application to create an access request on behalf of another user.

For example, say you have a ticketing system and one of the types of tickets that can be created is to request access to a specific asset. The ticketing system can be integrated with Safeguard through the Application to Application service to create an access request on behalf of the user that entered the ticket into the system. Once the request is created, it follows the normal access request workflow in Safeguard and the user who entered the ticket will be notified when access is granted.

In order for a third-party application to perform one of tasks provided by the Application to Application service, the application must first be registered with Safeguard. This registration will be associated with a certificate user and authentication to the Application to Application service will be done using the certificate and an API key. The registered application will not be allowed to authenticate to Safeguard other than for the purpose specified. The properties associated with an application registration are:

- **API key:** As part of the registration process, an API key is generated. An administrator must then copy this API key and make it available to the third-party application.

- **Certificate user:** In addition to the API key, the application registration must be associated with a certificate user. The certificate that is associated with the certificate user must be signed by a certificate authority that is also trusted by Safeguard.

  **NOTE:** Use your corporate PKI for issuing this certificate and installing in on the third-party application.

The Application to Application service is disabled by default and must be enabled before any credential retrievals or access request broker functions can be performed. An Appliance administrator can use the desktop client or Safeguard API to enable the service.

**Using the desktop client:**

1. Navigate to **Administrative Tools | Settings | Appliance | Enable or Disable Service.**
2. Click the **Application to Application Enabled** toggle to enable the service.

Using the API, use the following URL:

https://appliance/service/appliance/v2/A2AService/Enable

**NOTE:** You must re-enable the service after rebooting the appliance.

In addition, you can check the current state of the service using this same desktop client page or using the following URL:

https://appliance/service/appliance/v2/A2AService/Status

**Related Topics**

What needs to be set up to use Application to Application
Adding an application registration

Allowing a third-party application to perform one of tasks provided by the Application to Application service, starts with registering the third-party application with Safeguard.

Prerequisites:

- User Administrator adds certificate users to Safeguard.
- Asset Administrator adds assets and accounts to Safeguard.

To add an application registration

1. Log into the Safeguard desktop client as a Security Policy Administrator.
2. Navigate to Administrative Tools | Settings.
3. Select External Integration | Application to Application.
4. Click (or tap) + Add.
   The New Registration dialog displays.
5. On the General tab, specify the following information:
   a. Name: Enter a name for the application registration.
   b. Description: Enter information about the application registration.
   c. Certificate User: Click (or tap) Browse to select a certificate user who is associate with the third-party application being registered.
      
      NOTE: You do not need to specify a certificate user when you initially add an application registration. Once the User Administrator creates the certificate user associated with the application, use the Edit button on the Application to Application pane to specify the certificate user. The Application to Application service on the third-party application will not work with the Safeguard vault until a certificate user has been specified.
   d. I want to configure this registration for: Select the tasks to be performed by the Application to Application service:
      
      - Access Request Broker: Select this check box if you want the third-party application to create an access request on behalf of another user.
      - Credential Retrieval: Select this check if you want the third-party application to retrieve credentials from the Safeguard vault without having to go through the normal workflow process.
      
      Depending on the check boxes selected, additional tabs are displayed.
6. The Access Request Broker tab displays a list of users for which the third-party
application can create an access request on behalf of.

- Click (or tap) + to add a user or user group to the list.
- Click (or tap) **Edit Restrictions** to specify IP address restrictions for all of the users and user groups in the list.

A restriction is a list of IP addresses or range of IP addresses that are allowed to call the Application to Application service to perform this task. That is, if a restriction is added to a Credential Retrieval or Access Request Broker task, the service will only allow requests that initiate from the IP addresses specified in the restriction list.

The IP address notation can be:

- An IPv4 or IPv6 address (for example, 10.5.32.4)
- An address range in CIDR notation (for example, 10.5.0.0/16)

- Click (or tap) — to remove the selected user from the list.

7. The **Credential Retrieval** tab displays a list for which the third-party can retrieve credentials from Safeguard without going through the normal workflow process.

- Click (or tap) + to add an account to the list.
- Click (or tap) **Restrictions** in the Restrictions column to specify IP address restrictions for the selected account.

A restriction is a list of IP addresses or range of IP addresses that are allowed to call the Application to Application service to perform this task. That is, if a restriction is added to a Credential Retrieval or Access Request Broker task, the service will only allow requests that initiate from the IP addresses specified in the restriction list.

The IP address notation can be:

- An IPv4 or IPv6 address (for example, 10.5.32.4)
- An address range in CIDR notation (for example, 10.5.0.0/16)

- Click (or tap) — to remove the selected account from the list.

8. Click (or tap) **Create Registration**.

Once an application registration is added to Safeguard, the third-party application can authenticate with Safeguard using the API key that was generated and the certificate that was associated with the registration. To make a request, you must retrieve the relevant API key for the application using an authorized account (that is, using bearer token authentication) and install the correct certificate on the host that will make the request. For more information, see How do I make a request using the Application to Application service on page 499.

**Deleting an application registration**

Click 9or tap) **Delete** on the **Application to Application** pane in the **External Integration** settings view to delete an application registration from Safeguard.
To delete an application registration

1. Navigate to Administrative Tools | Settings | External Integration | Application to Application.
2. Select the application registration to be deleted.
3. Click (or tap) the \ toolbar button.
4. Confirm your request.

Regenerating an API key

If, as the Security Policy Administrator, you discover that the API key has been stolen or misplaced, you can regenerate the API key at any time. When you regenerate an API key, it invalidates the old API key and prevents any services from using that key to access the Application to Application service.

To regenerate an API key

1. Log into the Safeguard desktop client as a Security Policy Administrator.
2. Navigate to Administrative Tools | Settings.
3. Select External Integration | Application to Application.
4. Select an application registration from the list.
5. Click (or tap) \ from the toolbar.
6. On the API Keys dialog, select the API key to be replaced.
7. Click (or tap) .

You can now view or copy the new API key to the clipboard and use this new API key in your third-party application to access the Application to Application interfaces. See How do I make a request using the Application to Application service.

Approval Anywhere

The Safeguard Approval Anywhere feature integrates its access request workflow with Starling Two-Factor Authentication, allowing approvers to receive a notification through an app on their mobile device when an access request is submitted. The approver can then approve (or deny) access requests through their mobile device without needing access to the desktop or web application.

The Approval Anywhere feature is enabled when you join Safeguard to Starling. For more information, see Starling on page 334. Once enabled, it is the responsibility of the Security Policy Administrator to define the users who are authorized to use Approval Anywhere to approve access requests. This can be done using the Administrative Tools | Settings | External Integration | Approval Anywhere pane.
NOTE: In previous versions of Safeguard, you had to specify a Starling API key in order to use Approval Anywhere and Starling Two-Factor Authentication as a secondary authentication provider. This is no longer necessary when you join Safeguard to Starling. If you previously configured these features, once you join to Starling, Safeguard automatically migrates your previous configurations to use the credential string generated by the join process.

The Approval Anywhere pane displays the following about the users authorized to use the Approval Anywhere feature.

Table 188: Approval Anywhere: Properties

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Safeguard user.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This user must also be added as an approver in an access request policy.</td>
</tr>
<tr>
<td>Mobile Phone</td>
<td>Valid mobile phone number in E.164 format for the authorized user.</td>
</tr>
<tr>
<td>Alternate Mobile Phone</td>
<td>Alternate mobile phone number in E.164 format.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Valid email address for the authorized user.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage the users authorized to use Approval Anywhere.

Table 189: Approval Anywhere: Toolbar

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add Safeguard users who are authorized to use this feature to approve (or deny) access requests.</td>
</tr>
<tr>
<td></td>
<td>NOTE: Approval Anywhere approvers must have a valid mobile phone number in E.164 format and a valid email address defined. If a user does not display a valid mobile phone number or email address, edit the user record before proceeding. For more information, see Modifying a user on page 386. E.164 format: +&lt;country code&gt;&lt;area code&gt;&lt;phone number&gt;</td>
</tr>
<tr>
<td></td>
<td>NOTE: These same users must also be added as approvers in an access request policy.</td>
</tr>
<tr>
<td>Remove</td>
<td>Remove the selected user as an authorized user.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of users authorized to use Approval Anywhere.</td>
</tr>
</tbody>
</table>
Adding authorized user for Approval Anywhere

Once Safeguard is joined to Starling, use the Approval Anywhere pane to add the Safeguard users that can use the Approval Anywhere feature to approve access requests.

1. **NOTE:** If you upgraded from a previous version of Safeguard where you have already configured Approval Anywhere, your existing configure will continue to work. However, you will not be able to manage your Approval Anywhere users until you join Safeguard to Starling. Once you join to Starling, Safeguard automatically migrates your previous configurations to use the credential string generated by the join process.

2. **TIP:** Ensure OneTouch approvals is enabled on the two-factor authentication app on your mobile device.

To add users who are authorized to use Approval Anywhere

1. Log into the Safeguard desktop client as a Security Policy administrator.
2. Navigate to Administrative Tools | Settings.
3. Select External Integration | Approval Anywhere.
4. Click (or tap) + Add.
5. In the Users dialog, select users from the list and click (or tap) OK.
   
   **NOTE:** Approval Anywhere approvers must have a valid mobile phone number in E.164 format and a valid email address defined. If a user does not display a valid mobile phone number or email address, edit the user record before proceeding. For more information, see Modifying a user on page 386.

   E.164 format: +<country code><area code><phone number>

6. Add these Approval Anywhere users as "approvers" in the appropriate access request policy. For more information, see Creating an access request policy on page 214.

Once a user is added as an Approval Anywhere user and as an approver in an access request policy, when an access request requires approval, Safeguard sends a notification to the approver's Starling 2FA mobile app. The approver can either approve or deny the access request directly from the Starling 2FA mobile app.

**NOTE:** Revoking an access request that has already been approved is not available via the mobile app. You must use the Safeguard desktop or web client to perform that action.

Email

It is the responsibility of the Appliance Administrator to configure Safeguard to automatically send email notifications when certain events occur.
Use the **Email** pane to configure the SMTP server to be used for email notifications and to edit the email templates that define the content of email notifications.

**TIP:** You must configure the DNS Server and set up the user's email address correctly.

**To configure the SMTP Server**

1. In **Settings**, select **External Integration | Email**.
2. To configure the email notifications, enter these global settings for all Safeguard emails:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server Address</td>
<td>Enter the IP address or DNS name of the mail server. When unspecified, Safeguard disables the email client.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> When entering an IPv6 address, you must encapsulate it in square brackets, such as [b86f:b86f:b86f:1:b86f:b86f:b86f:b86f].</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If you are using a mail exchanger record (MX record), you must specify the domain name for the mail server.</td>
</tr>
<tr>
<td>SMTP Port</td>
<td>Enter the TCP port number for the email service.</td>
</tr>
<tr>
<td></td>
<td>Default: 25</td>
</tr>
<tr>
<td></td>
<td>Range: 1 to 32767</td>
</tr>
<tr>
<td>Sender Email</td>
<td>Enter an email address to use as the &quot;From&quot; address for all emails originating from the appliance.</td>
</tr>
<tr>
<td></td>
<td>Required if you specify the <strong>SMTP Server Address</strong>.</td>
</tr>
<tr>
<td></td>
<td>Limit: 512 characters</td>
</tr>
<tr>
<td>Require Transport Layer</td>
<td>Select this option to require that Safeguard uses TLS to provide communication security over the internet.</td>
</tr>
<tr>
<td>Security</td>
<td></td>
</tr>
</tbody>
</table>

**To validate your setup**

1. Select the **Test Email Settings** link.
2. Enter a **Send To** email address of where to send the test message and click (or tap) **Send**. Safeguard sends an email using the configuration settings.

The grid at the bottom of this pane lists the email templates used to define the content to be included in email notifications. Use these toolbar buttons to manage email templates.
### Enabling email notifications

For users to receive email notifications, there are a few things you must configure properly.

**To enable email notifications**

1. Each user must set up his or her email address correctly.
   a. The Authorizer Administrator or User Administrator sets this up in the user’s **Contact Information**. For more information, see [Adding a user](#) on page 375.
   -OR-
   b. The user sets this up in his or her **My Account** settings. For more information, see [User avatar](#) on page 44.

2. The Appliance Administrator must configure the SMTP server. For more information, see [Email](#) on page 325.

**TIP:** You can setup email subscriptions to any email event type through the API: https://<Appliance IP>/service/core/swagger/ui/index#/EventSubscribers. For more information, see [How do I access the API](#) on page 475.

### Modifying an email template

Safeguard provides default email templates for most events, such as when a password change fails or when emergency access is granted or an access request is denied. However, you can customize individual email templates.

Each template corresponds to a single event type; the event triggers an email notification that uses the template.
To modify an email template

1. Open the email template for editing.
2. In the Email Template configuration dialog,
   a. **Event**: Select an event type for an email template. For more information, see Enabling email notifications on page 327.

   ![NOTE: You can create only one email template per event type.]

   b. **Subject**: Enter a "subject" line for the email message.
      As you type, click (or tap) + Insert Event Property Macro to insert predefined text into the subject line. For example, you might create the following subject line:
      Approval is required for {{Requester}}'s request
      where Safeguard generates the data defined by the macro within the double braces. (For more information about using macros, see note at the end of this topic.)
      Required
      Limit: 1024 characters
   c. **Reply to**: Enter the email address of the person to reply to concerning this notification.
      Limit: 512 characters
   d. **Body**: Enter the body of the message.
      As you type, click (or tap) + Insert Event Property Macro to insert predefined text into the body. For example, you might create the following body for an email template:
      {{Requester}} has requested the password for {{AccountName}} on
      {{AssetName}}
      where Safeguard generates the data defined by the macro within the double braces. (For more information about using macros, see note below.)
      Required
      Limit: 16384 characters
   e. **Preview Email**: Select this link to display the Preview Email dialog so you can see how your email message will look.

   ![NOTE: Each event type supports specific macros that are appropriate for that type of event. You can enter the macro into the text of the subject line or body using keywords surrounded by double braces rather than inserting the macro. However, Safeguard ignores macros that are not supported by the event type. Unsupported macros appear blank in the email preview. ]
External Federation

One Identity Safeguard supports the SAML 2.0 Web Browser SSO Profile, allowing you to configure federated authentication with many different Identity Provider STS (IdP-STS) servers and services, such as Microsoft's AD FS and Azure AD.

It is the responsibility of the Appliance Administrator to configure the external federation service providers in Safeguard.

The External Federation pane displays the following details about the external federation service providers defined.

Table 191: External Federation: Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name assigned to the external federation service provider.</td>
</tr>
</tbody>
</table>

**NOTE:** The name is used for administrative purposes only and will not be seen by end users.

| Realm    | The unique realm value, typically a DNS suffix, that matches the email addresses of users intended to use the specified IdP-STS for authentication. |

Use these toolbar buttons to manage external federation service provider configurations.

Table 192: External Federation: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📦 Add</td>
<td>Add an external federation service provider. For more information, see How do I add an external federation provider trust in Safeguard on page 480.</td>
</tr>
<tr>
<td>🔴 Delete Selected</td>
<td>Remove the selected service provider configuration.</td>
</tr>
<tr>
<td>⌛ Refresh</td>
<td>Update the list of authentication service provider configurations.</td>
</tr>
<tr>
<td>🖋 Edit</td>
<td>Modify the selected service provider configuration.</td>
</tr>
<tr>
<td>⚡ Download</td>
<td>Download a copy of the Safeguard federation metadata XML. This file is used to create the corresponding trust relationship on your IdP-STS server.</td>
</tr>
</tbody>
</table>

Related Topics

How do I configure external federation authentication
Secondary Authentication

One Identity Safeguard allows you to require that a user log in with two-factor authentication. You can set up a secondary authentication service provider or a remote access server. Safeguard's strong two-factor authentication ensures that only authorized users are permitted access.

The Starling 2FA secondary authentication service provider is automatically added when you join Safeguard to Starling. For more information, see Starling on page 334. It is the responsibility of the Appliance Administrator to configure other secondary authentication service providers in Safeguard. This can be done using the Administrative Tools | Settings | External Integration | Secondary Authentication pane.

**NOTE:** In previous versions of Safeguard, you had to specify a Starling API key in order to use Approval Anywhere and Starling Two-Factor Authentication as a secondary authentication provider. This is no longer necessary when you join Safeguard to Starling. If you previously configured these features, once you join to Starling, Safeguard automatically migrates your previous configurations to use the credential string generated by the join process.

**NOTE:** It is the responsibility of either the Authorizer Administrator or the User Administrator to configure a user account to use two-factor authentication when logging into Safeguard. For more information, see Requiring user to log in using secondary authentication on page 380.

The **Secondary Authentication** pane displays the following about the service providers defined for secondary authentication.

**Table 193: Secondary Authentication: Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name assigned to the secondary authentication provider.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The Starling 2FA service provider is automatically added to Safeguard when you join Safeguard to One Identity Starling. You cannot manually add, edit, or delete the Starling 2FA secondary authentication provider. For more information, see Starling on page 334.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of service provider:</td>
</tr>
<tr>
<td></td>
<td>• Starling Two-Factor Authentication</td>
</tr>
<tr>
<td></td>
<td>• Radius</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage secondary authentication service provider configurations.
### Table 194: Secondary Authentication: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Add] Add</td>
<td>Add a Radius secondary authentication service provider configuration. For more information, see Adding a Radius secondary authentication service provider on page 331.</td>
</tr>
<tr>
<td>![Delete Selected] Delete Selected</td>
<td>Remove the selected service provider configuration.</td>
</tr>
<tr>
<td>![Refresh] Refresh</td>
<td>Update the list of authentication service provider configurations.</td>
</tr>
<tr>
<td>![Edit] Edit</td>
<td>Modify the selected service provider configuration.</td>
</tr>
</tbody>
</table>

**NOTE:** You cannot delete the Starling 2FA secondary authentication provider configuration. You must unjoin Safeguard from Starling. For more information, see Starling on page 334.

**NOTE:** You cannot edit the Starling 2FA secondary authentication provider configuration.

### Adding a Radius secondary authentication service provider

It is the responsibility of the Appliance Administrator to configure the secondary authentication service providers in Safeguard.

**To add a Radius secondary authentication service provider**

1. In Settings, select External Integration | Secondary Authentication.
2. Click (or tap) ![Add] Add to add a new secondary authentication service provider.
3. In the Secondary Authentication dialog, supply the following information:
   a. **Type:** Select Radius.  
      Required
   a. **Name:** Enter a display name for the secondary authentication service provider.  
      **NOTE:** The display name must be unique.  
      Limit: 100 characters
      Required
   b. **Server Address:** Enter a network DNS name or the IP address used to connect to the secondary authentication service provider over the network.  
      Limit: 255 characters
Required

c. **Secondary Server Address**: (Optional) Enter a network DNS name or the IP address for an additional or redundant secondary authentication service provider.
   Limit: 255 characters

d. **Shared Secret**: Enter the server's secret key.
   Limit: 255 characters
   Required
   **TIP**: Click (or tap) to show the server's secret key.

e. **Port**: Enter the server authentication port number on which the secondary authentication service provider will be listening for connections.
   Default: 1812
   Required

f. **Timeout**: Specify how long to wait before a Radius authentication times out.
   Default: 3 seconds
   Valid range: 3 - 60 seconds
   Required

**SNMP**

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. One Identity Safeguard allows you to configure SNMP subscriptions for sending SNMP traps to your SNMP console when certain events occur. The **SNMP** pane displays the following about the SNMP subscribers defined.

**Table 195: SNMP: Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Address</td>
<td>The IP address or FQDN of the primary SNMP network server.</td>
</tr>
<tr>
<td>Port</td>
<td>The UDP port number for SNMP traps.</td>
</tr>
<tr>
<td>Version</td>
<td>The SNMP version being used.</td>
</tr>
<tr>
<td>Community</td>
<td>The SNMP community string being used by the SNMP subscriber.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the SNMP subscriber.</td>
</tr>
<tr>
<td># of Events</td>
<td>The number of events selected to be sent to the SNMP console.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage the SNMP subscriptions.
### Table 196: SNMP: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✨ New</td>
<td>Add a new SNMP subscription. For more information, see Configuring SNMP subscriptions on page 333.</td>
</tr>
<tr>
<td>🗑️ Delete Selected</td>
<td>Remove the selected SNMP subscription.</td>
</tr>
<tr>
<td>🔄 Refresh</td>
<td>Update the list of SNMP subscriptions.</td>
</tr>
<tr>
<td>✍️ Edit</td>
<td>Modify the selected SNMP subscription.</td>
</tr>
<tr>
<td>☤️ Copy</td>
<td>Clone the selected SNMP subscription.</td>
</tr>
</tbody>
</table>

### Configuring SNMP subscriptions

It is the responsibility of the Appliance Administrator to configure Safeguard to send SNMP traps to your SNMP console when certain events occur.

**NOTE:** To download Safeguard MIB-module definitions from your appliance, enter the following URL into your web browser; no authentication is required:
https://<Appliance IP address>/docs/mib/SAFEGUARD-MIB.mib

**To configure SNMP subscriptions**

1. In Settings, select External Integration | SNMP.
2. Click (or tap) ✨ New to open the SNMP subscription configuration dialog.
3. Provide the following information:

<table>
<thead>
<tr>
<th>Network Address</th>
<th>Enter the IP address or FQDN of the primary SNMP network server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Limit: 255 characters Required</td>
</tr>
<tr>
<td>UDP Port</td>
<td>Enter the UDP port number for SNMP traps.</td>
</tr>
<tr>
<td></td>
<td>Default: 162 Required</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description of the SNMP subscriber.</td>
</tr>
<tr>
<td></td>
<td>Limit: 255 characters</td>
</tr>
<tr>
<td>Events</td>
<td>Browse to select one or more SNMP event types.</td>
</tr>
<tr>
<td></td>
<td>Use the ✗ Clear icon to remove an individual event from this list or right-click and select Remove All to clear all events</td>
</tr>
</tbody>
</table>
NOTE: The SNMP pane displays the number of events that you select, not the names of the events.

| Community | Enter the SNMP community string, such as "public". The SNMP community string is like a user ID or password that allows access to a device's statistics, such as a router. A PRTG Network Monitor sends the community string along with all SNMP requests. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device simply discards the request and does not respond. |

Verifying SNMP configuration

Use the Send Test Event link located under the SNMP table on the Settings | External Integration | SNMP pane.

To validate your setup

1. When configuring your SNMP subscription, on the SNMP dialog add the "test" event to your event subscription.
2. Back on the SNMP settings pane, select the SNMP configuration from the table, then select Send Test Event.
   Safeguard sends a test event notification to your SNMP console.

Starling

Integrating One Identity Safeguard with One Identity Starling allows you to take advantage of companion features from Starling services, such as Starling Two-Factor Authentication and Starling Identity Analytics & Risk Intelligence.

In order to use Starling 2FA with Safeguard's Approval Anywhere feature or as a secondary authentication provider, you must join Safeguard to Starling. This is done from the Administrative Tools | Settings | External Integration | Starling pane in the Safeguard desktop client. This pane also includes the following links, which provide assistance with Starling:

- Visit us online to learn more displays the Starling login page where you can create a new Starling account.
Trouble Joining displays the Starling support page with information on the requirements and process for joining with Starling.

**NOTE:** In previous versions of Safeguard, you had to specify a Starling API key in order to use Approval Anywhere and Starling Two-Factor Authentication as a secondary authentication provider. This is no longer necessary when you join Safeguard to Starling. If you previously configured these features, once you join to Starling, Safeguard automatically migrates your previous configurations to use the credential string generated by the join process.

It is the responsibility of the Appliance Administrator to join One Identity Safeguard to Starling.

**Prerequisites**

In order to use the companion features from Starling services, first configure the following:

- A valid license for Safeguard with One Identity Hybrid subscription included.
  
  **NOTE:** You must have a valid license for at least one of the Safeguard modules: Privileged Passwords or Privileged Sessions.

- A Starling Organization Admin account or a Collaborator account associated with the One Identity Hybrid subscription. For more information on Starling, see the One Identity Starling User Guide.

- If your company requires the use of a proxy to access the internet, you must configure the web proxy to be used. For more information on configuring a web proxy to be used by Safeguard for outbound web requests to integrated services, see Networking.

**To join Safeguard with Starling**

1. Navigate to Administrative Tools | Settings.
2. Select External Integration | Starling.
3. Click (or tap) Join to Starling.

  **NOTE:** The following additional information may be required:
  
  - If you do not have an existing session with Starling, you will be prompted to authenticate.
  - If your Starling account belongs to multiple organizations, you will be prompted to select which organization Safeguard will be joined with.

After the join has successfully completed, you will be returned to the Safeguard desktop client and the Starling settings pane will now show Joined to Starling.
To unjoin Safeguard from Starling

1. In Settings, select External Integration | Starling.
2. Click (or tap) Unjoin Starling.

Safeguard will no longer be joined to Starling, which means that Approval Anywhere and two-factor authentication as a secondary authentication provider are also disabled in Safeguard. A Starling Organization Admin account or Collaborator account associated with the Starling One Identity Hybrid subscription can rejoin Safeguard to Starling at any time.

Syslog

Safeguard allows you to define one or more syslog servers to be used for logging Safeguard event messages. Using this feature, Appliance Administrators can specify to send different types of messages to different syslog servers.

The Syslog pane displays the following about each syslog server defined.

### Table 197: Syslog server: Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Address</td>
<td>The IP address or FQDN of the syslog server.</td>
</tr>
<tr>
<td>Port</td>
<td>The UDP port number for syslog server.</td>
</tr>
<tr>
<td>Facility</td>
<td>The type of program being used to create syslog messages.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the syslog server configuration.</td>
</tr>
<tr>
<td># of Events</td>
<td>The number of events selected to be logged to the syslog server.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage the syslog server configurations.

### Table 198: Syslog server: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ New</td>
<td>Add a new syslog server configuration. For more information, see Configuring a syslog server on page 337.</td>
</tr>
<tr>
<td>Delete Selected</td>
<td>Remove the selected syslog server configuration from Safeguard.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of syslog server configurations.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modify the selected syslog server configuration.</td>
</tr>
<tr>
<td>Copy</td>
<td>Clone the selected syslog server configuration.</td>
</tr>
</tbody>
</table>
Configuring a syslog server

It is the responsibility of the Appliance Administrator to configure Safeguard to log event messages to a syslog server.

**To configure a syslog server**

1. In **Settings**, select **External Integration | Syslog**.
2. Click (or tap) **+ New** to display the **Syslog** dialog.
3. In the **Syslog** dialog, enter the following:
   a. **Network Address**: Enter the IP address or FQDN of the syslog server.
      Limit: 255 characters
      Required
   b. **UDP Port**: Enter the UDP port number for the syslog server.
      Default: 514
      Range: between 1 and 32767
      Required
   c. **Description**: Enter a description for the syslog server configuration.
      Limit: 255 characters
   d. **Events**: Click (or tap) **Browse** to select the events to be included in the syslog.
      On the **Event** selection dialog, select the events to be included, then click **OK**.
   e. **Facility**: Choose the type of program to be used to log syslog messages.
      Default: User-level messages
4. Click (or tap) **OK** to save your selection and add the syslog server configuration.

Verifying syslog server configuration

Use the **Send Test Event** link located below the Syslog configuration table on the **Settings | External Integration | Syslog** pane to verify your syslog server configuration.

**To validate your setup**

1. When configuring your syslog server, on the **Syslog** dialog add the "test" event.
2. Back on the **Syslog** pane, select the syslog server configuration from the table, then select **Send Test Event**.
   Safeguard logs a test message to the designated syslog server.

**NOTE**: To log event messages to a syslog server, you must configure Safeguard to send alerts. For more information, see **Configuring alerts** on page 72.
Ticketing

Safeguard allows you to integrate with your company's external ticket system. The Ticketing pane displays the following about the ticket systems defined.

Table 199: Ticketing: Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name assigned to the ticket system when it was added to Safeguard.</td>
</tr>
<tr>
<td>URL</td>
<td>The web site address of the ticket system.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage the ticketing systems defined to integrate with Safeguard.

Table 200: Ticketing: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✯ New</td>
<td>Add a new ticket system.</td>
</tr>
<tr>
<td>⌫ Delete Selected</td>
<td>Remove the selected ticket system from Safeguard.</td>
</tr>
<tr>
<td>⌬ Refresh</td>
<td>Update the list of ticket systems.</td>
</tr>
<tr>
<td>✎ Edit</td>
<td>Modify the selected ticket system configuration.</td>
</tr>
</tbody>
</table>

Configuring integration with external ticket system

It is the responsibility of the Appliance Administrator to configure Safeguard to integrate with your company's external ticket system. The Security Policy Administrator configures the access request policy to require that users provide a ticket number when requesting an account password or session access. For more information, see Requester tab on page 217.

To configure Safeguard to integrate with an external ticket system

1. In Settings, select External Integration | Ticketing.
2. Click (or tap) ✯ Add to open the Ticket System dialog.
3. Provide the following:
   a. **Name**: Enter the name of your ticketing system.
      Required
   b. **Type**: Select the type of ticketing tracking system:
- **ServiceNow**: A cloud-based issue tracking system.
- **Remedy**: A request-for-service problem tracking system.

**c. URL**: Enter the website address to the ticketing system.
- **Required**

**d. User Name**: Enter an account for Safeguard to use to access the ticketing system.
- **Required**

**e. Password**: Enter the user account’s password.
- **Required**

**f. Client Identifier**: Enter the ServiceNow Client ID.

**g. Client Secret**: Enter the ServiceNow secret key.

**h. Authentication String**: Enter the authentication credential for the Remedy AR (Action Request) system server.

### Messaging settings

Safeguard allows you to set the following notifications.

**Table 201: Messaging settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Notification</td>
<td>Where you enable a login banner that users must acknowledge before they can access Safeguard.</td>
</tr>
<tr>
<td>Message of the Day</td>
<td>Where you set the <strong>Message of the Day</strong> which displays on the Home page.</td>
</tr>
</tbody>
</table>

### Login Notification

It is the responsibility of the Appliance Administrator to configure the login notification displayed when a user logs into One Identity Safeguard.

**To configure the login notification**

1. In **Settings**, select **Messaging | Login Notification**.
2. Select the **Message** check box and enter a message.
3. Click (or tap) **OK**.
Message of the Day

It is primarily the responsibility of the Appliance Administrator to configure the message of the day displayed on the Home page, however any user with administrator permissions has the ability to set the message of the day.

To configure the message of the day

1. In Settings, select Messaging | Message of the Day.
2. Choose either the RSS or Subject Line option.
3. When the RSS option is selected, enter a web address.
4. When the Subject line option is selected, enter the following information:
   - Subject Line: Enter a short description.
   - Message: Enter the text of up to 255 characters.
5. Click (or tap) OK.

Profile settings

Use the Profile settings to define the profile configuration settings, including account password rules and password check and change schedules, which can then be used in partition or directory profile definitions.

Table 202: Profile settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Password Rules</td>
<td>Where you define the complexity rules used by Safeguard when constructing new passwords during an automatic account password change.</td>
</tr>
<tr>
<td>Change Password</td>
<td>Where you define the rules Safeguard uses to reset account passwords.</td>
</tr>
<tr>
<td>Check Password</td>
<td>Where you define the rules Safeguard uses to verify account passwords.</td>
</tr>
<tr>
<td>Directory Account Password Rules</td>
<td>Where you defined the complexity rules used by Safeguard when constructing new passwords during automatic directory account password change.</td>
</tr>
<tr>
<td>Directory Change Password</td>
<td>Where you define the rules Safeguard uses to reset directory account passwords.</td>
</tr>
<tr>
<td>Directory Check Password</td>
<td>Where you define the rules Safeguard uses to verify directory account passwords.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password Sync Groups</td>
<td>Where you define the password sync groups and associated accounts so Safeguard can synchronize passwords across accounts.</td>
</tr>
</tbody>
</table>

## Account Password Rules

Account password rules govern the construction of a new password created by Safeguard during an automatic account password change. Some companies impose requirements on passwords, such as:

- The use of both upper- and lower-case letters
- Inclusion of one or more numerical digits
- Inclusion of special characters, such as @, #, $ and so forth

![NOTE: You select an account password rule set when defining a partition's profile. For more information, see Creating a partition profile on page 239. An account password rule applies to all accounts governed by the profile.](image)

Use these toolbar buttons to manage your account password rules.

**Table 203: Account Password Rules: Toolbar**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✌️ Add Account Password Rule</td>
<td>Add an account password complexity rule. For more information, see Adding an account password rule on page 341.</td>
</tr>
<tr>
<td>🗑️ Delete Selected</td>
<td>Remove the selected rule.</td>
</tr>
<tr>
<td>⌛️ Refresh</td>
<td>Update the list of account password rules.</td>
</tr>
<tr>
<td>✒️ Edit</td>
<td>Modify the selected rule.</td>
</tr>
<tr>
<td>🖨 Copy</td>
<td>&quot;Clone&quot; the selected rule.</td>
</tr>
</tbody>
</table>

### Adding an account password rule

It is the responsibility of the Asset Administrator, or a partition's delegated administrator, to configure account password complexity rules.
To add an account password rule

1. In Settings, select Profile | Account Password Rules.
2. Click (or tap) + Add Account Password Rule to open the Account Password Rule dialog.
3. Browse to select the partition.
4. Enter a Name of up to 50 characters for the account password rule.
5. Enter a Description of up to 255 characters for the password rule.
6. Set the Password Length from 3 to 255 characters.
   Default: 6 to 10 characters

   **NOTE:** The maximum length must be equal to or greater than the sum of minimum characters described in the next step.

   **IMPORTANT:**
   Some Unix systems silently truncate passwords to their maximum allowed length. For example, Macintosh OS X only allows a password of 128 characters. If an Asset Administrator creates a profile with an Account Password Rule that sets the password length to 136 characters, when Safeguard changes the password for an account governed by that profile, the asset's operating system truncates the new password to the allowable length and does not return an error; however, the full 136-character password is stored in Safeguard. This causes the following issues:

   - Check Password for that account will fail. When Safeguard compares the password on the Unix host with the password in Safeguard, they never match because the Unix host truncated the password generated by Safeguard.
   - A user will not be able to log into the Unix host account successfully with the password provided by Safeguard unless he truncates the password to the allowable length imposed by the operating system.

7. Set the character Requirements:

<table>
<thead>
<tr>
<th>First Character Type</th>
<th>Choose one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>All</strong>: Alphabetical, numeric, or symbols</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alphabetic</strong>: Alphabetical or numeric</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alphabetic</strong>: Only alphabetical characters</td>
</tr>
<tr>
<td></td>
<td>Default: All</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Last Character Type</th>
<th>Choose one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>All</strong>: Alphabetical, numeric, or symbols</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Alphanumeric</td>
<td>Alphabetical or numeric</td>
</tr>
<tr>
<td>Alphabetic</td>
<td>Only alphabetical characters</td>
</tr>
<tr>
<td>Default: All</td>
<td></td>
</tr>
<tr>
<td>Allow Consecutively Repeated Characters</td>
<td>Select this option to allow Safeguard to create a password with consecutively repeated characters.</td>
</tr>
<tr>
<td>NOTE: Clear this option to disallow consecutively repeated characters.</td>
<td></td>
</tr>
<tr>
<td>Default: Not allowed</td>
<td></td>
</tr>
<tr>
<td>Allow Uppercase</td>
<td>Select this option to allow Safeguard to create a password with uppercase characters.</td>
</tr>
<tr>
<td>Set the minimum number of required uppercase characters, or set it to zero if there is no minimum requirement.</td>
<td></td>
</tr>
<tr>
<td>NOTE: Clear this option to disallow uppercase characters.</td>
<td></td>
</tr>
<tr>
<td>Default: Require a minimum of 1</td>
<td></td>
</tr>
<tr>
<td>Allow Lowercase</td>
<td>Select this option to allow Safeguard to create a password with lowercase characters.</td>
</tr>
<tr>
<td>Set the minimum number of required lowercase characters, or set it to zero if there is no minimum requirement.</td>
<td></td>
</tr>
<tr>
<td>NOTE: Clear this option to disallow lowercase characters.</td>
<td></td>
</tr>
<tr>
<td>Default: Require a minimum of 1</td>
<td></td>
</tr>
<tr>
<td>Allow Numeric (0-9)</td>
<td>Select this option to allow Safeguard to create a password with numeric characters.</td>
</tr>
<tr>
<td>Set the minimum number of required numeric characters, or set it to zero if there is no minimum requirement.</td>
<td></td>
</tr>
<tr>
<td>NOTE: Clear this option to disallow numeric characters.</td>
<td></td>
</tr>
<tr>
<td>Default: Require a minimum of 1</td>
<td></td>
</tr>
<tr>
<td>Allow Symbols (e.g @ # $ % &amp; )</td>
<td>Select this option to allow Safeguard to create a password with special characters.</td>
</tr>
<tr>
<td>Set the minimum number of required symbolic characters, or set it to zero if there is no minimum requirement.</td>
<td></td>
</tr>
<tr>
<td>NOTE: Clear this option to disallow special characters.</td>
<td></td>
</tr>
<tr>
<td>Default: Not allowed</td>
<td></td>
</tr>
</tbody>
</table>
Valid Symbols: Enter allowable special characters, such as: `~!@#$%^*()_+-=;'?\|><,.\["]{}.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Change Password Setting</td>
<td>Add a change password rule. For more information, see Adding change password settings on page 344.</td>
</tr>
<tr>
<td>Delete Selected</td>
<td>Remove the selected rule.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of change password rules.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modify the selected rule.</td>
</tr>
<tr>
<td>Copy</td>
<td>&quot;Clone&quot; the selected rule.</td>
</tr>
</tbody>
</table>

Change Password

Change password settings are the rules Safeguard uses to reset account passwords.

The Change Password pane displays the following about the listed change password setting rules.

Table 204: Change Password: Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the rule.</td>
</tr>
<tr>
<td>Partition</td>
<td>The partition that uses the rule.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the rule.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Displays the selected rule's schedule.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage the change password setting rules.

Table 205: Change Password: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Change Password Setting</td>
<td>Add a change password rule. For more information, see Adding change password settings on page 344.</td>
</tr>
<tr>
<td>Delete Selected</td>
<td>Remove the selected rule.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of change password rules.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modify the selected rule.</td>
</tr>
<tr>
<td>Copy</td>
<td>&quot;Clone&quot; the selected rule.</td>
</tr>
</tbody>
</table>

Adding change password settings

It is the responsibility of the Asset Administrator or the partition's delegated administrator to configure the rules Safeguard uses to reset account passwords.
IMPORTANT: Passwords for accounts associated with a password sync group are managed based on the profile change schedule and processed via the sync group. If synchronization fails for an individual account in the sync group, the account is retried multiple times and, if failing after that, the sync task halts and is rescheduled. The administrator must correct the cause of the failure for the sync task to continue. For more information, see Password Sync Groups on page 354.

To add a password reset schedule

1. In Settings, select Profile | Change Password.
2. Click (or tap) + Add Change Password Setting to open the Change Password Settings dialog.
3. Browse to select a partition.
4. Enter a Name of up to 50 characters for the rule.
5. Enter a Description of up to 255 characters for the rule.
   For more information, see How do I manage accounts on unsupported platforms on page 483.
7. Click (or tap) the Schedule button and choose an interval.
8. In the Schedule dialog,
   a. Interval: Choose Never, Minute, Hour, Day, Week, or Month.
      NOTE: Best Practice: Do not use the Minute interval.
   b. Time of day: Set the start time.
   c. Repeat interval: Select the interval you would like to repeat the password reset task.
      - If Weekly, select which days of the week you want to repeat the change password task.
      - If Monthly, set the task recurrence pattern: Day of month or week of month and day of week.
   d. Time Zone: Select the time zone.
9. Optionally select any of these options:
   a. Change the Password Even if a Release is Active: Select this option to allow a password change even when a password release is active.
   b. Update Service on Password Change (Windows Only): For service accounts that run system services, select this option to ensure that the password change is also applied to each service the account runs.
   c. Restart Service on Password Change (Windows Only): For service accounts that run system services, select this option to ensure that the services automatically restart after the password is changed.
d. **Update Task on Password Change (Windows Only):** For service accounts that run scheduled system tasks, select this option to ensure that the password change is also applied to each task the account runs.

e. **Suspend account when not checked out (supported platforms):** Select this option to automatically suspend managed accounts that are not in use. That is, the account on a managed asset is suspended until a request is made for it through Safeguard, at which time Safeguard restores the account. Once the request is checked in or closed, the account is again suspended.

Click (or tap) the **supported platforms** link to display a list of platforms that support this feature.

NOTE: When managing passwords for Windows service accounts, do not select this option. Create a separate Profile with Change Password settings that do not have this option selected for managing Windows service accounts.

f. **Manage SSH Key:** Select this option to allow Safeguard to rotate the SSH key it uses to communicate with an asset configured to use SSH Key Authentication. For more information, see [SSH Key](#) on page 142.

NOTE: Clear this option to only manage passwords.

## Check Password

Check password settings are the rules Safeguard uses to verify account passwords. The Check Password pane displays the following about the listed check password setting rules.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the check password rule.</td>
</tr>
<tr>
<td>Partition</td>
<td>The partition that uses the rule.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the rule.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Displays the selected rule's schedule.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage the check password setting rules.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✚ Add Check Password Setting</td>
<td>Add a check password rule. For more information, see <a href="#">Adding check password settings</a> on page 347.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>🗑 Delete Selected</td>
<td>Remove the selected rule.</td>
</tr>
<tr>
<td>⌚ Refresh</td>
<td>Update the list of check password rules.</td>
</tr>
<tr>
<td>✍ Edit</td>
<td>Modify the selected rule.</td>
</tr>
<tr>
<td>✍️ Copy</td>
<td>&quot;Clone&quot; the selected rule.</td>
</tr>
</tbody>
</table>

**Adding check password settings**

It is the responsibility of the Asset Administrator or the partition’s delegated administrator to define the rules Safeguard uses to verify account passwords.

**To add a password validation schedule**

1. In **Settings**, select **Profile | Check Password**.
2. Click (or tap) **ioneer Add Check Password Setting** to open the **Check Password Settings** dialog.
3. **Browse** to select a partition.
4. Enter a **Name** of up to 50 characters for the rule.
5. Enter a **Description** of up to 255 characters for the rule.
6. Click (or tap) the **Schedule** button and choose an interval.
7. In the **Schedule** dialog, 
   a. **Interval**: Choose **Never, Minute, Hour, Day, Week, or Month**.
   
   ![NOTE: Best Practice: Do not use the Minute interval.]
   b. **Time of day**: Set the start time.
   c. **Repeat Interval**: Select the interval you would like to repeat the password check task.
      
      - If **Weekly**, select which days of the week you want to repeat the password check task.
      - If **Monthly**, set the task recurrence pattern: Day of month or week of month and day of week.
   d. **Time Zone**: Select the time zone.
8. Optionally select either of these options:
   - **Change Password on Mismatch**: Select this option to automatically change a password when Safeguard detects the password in the appliance database differs from the password on the asset.
   - **Notify Delegated Owners on Mismatch**: Select this option to trigger a notification when Safeguard detects a password mismatch.
NOTE: To send event notifications to a user, you must configure Safeguard to send alerts. For more information, see Configuring alerts on page 72. Set up an email template for the Password Check Mismatch event type.

Directory Account Password Rules

Directory account password rules govern the construction of a new password created by Safeguard during an automatic directory account password change. Some companies impose requirements on passwords, such as:

- The use of both upper- and lower-case letters
- Inclusion of one or more numerical digits
- Inclusion of special characters, such as @, #, $ and so forth

NOTE: You select a directory account password rule set when defining a directory’s profile. For more information, see Creating a directory profile on page 199. A directory account password rule applies to all accounts governed by the profile.

Use these toolbar buttons to manage your directory account password rules.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Directory Account Password Rule</td>
<td>Add a directory account password complexity rule. For more information, see Adding a directory account password rule on page 348.</td>
</tr>
<tr>
<td>Delete Selected</td>
<td>Remove the selected rule.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of directory account password rules.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modify the selected rule.</td>
</tr>
<tr>
<td>Copy</td>
<td>&quot;Clone&quot; the selected rule.</td>
</tr>
</tbody>
</table>

Adding a directory account password rule

It is the responsibility of the Asset Administrator, or a partition's delegated administrator, to configure directory account password complexity rules.
To add a directory account password rule:

1. In Settings, select Profile | Directory Account Password Rules.
2. Click (or tap) + Add Account Password Rule to open the Directory Account Password Rule dialog.
3. Enter a Name of up to 50 characters for the account password rule.
4. Enter a Description of up to 255 characters for the password rule.
5. Set the Password Length from 33 to 255 characters.
   Default: 6 to 10 characters
   
   **NOTE:** The maximum length must be equal to or greater than the sum of minimum characters described in the next step.

6. Set the character Requirements:

<table>
<thead>
<tr>
<th>First Character Type</th>
<th>Choose one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>All</strong>: Alphabetical, numeric, or symbols</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alphanumeric</strong>: Alphabetical or numeric</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alphabetic</strong>: Only alphabetical characters</td>
</tr>
<tr>
<td>Default: All</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Last Character Type</th>
<th>Choose one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>All</strong>: Alphabetical, numeric, or symbols</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alphanumeric</strong>: Alphabetical or numeric</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alphabetic</strong>: Only alphabetical characters</td>
</tr>
<tr>
<td>Default: All</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allow Consecutively Repeated Characters</th>
<th>Select this option to allow Safeguard to create a password with consecutively repeated characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>NOTE:</strong> Clear this option to disallow consecutively repeated characters.</td>
</tr>
<tr>
<td>Default: Not allowed</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allow Uppercase</th>
<th>Select this option to allow Safeguard to create a password with uppercase characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set the minimum number of required uppercase characters, or set it to zero if there is no minimum requirement.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Clear this option to disallow uppercase characters.</td>
</tr>
<tr>
<td>Default: Require a minimum of 1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allow Lowercase</th>
<th>Select this option to allow Safeguard to create a password</th>
</tr>
</thead>
</table>
with lowercase characters. Set the minimum number of required lowercase characters, or set it to zero if there is no minimum requirement.

| NOTE: Clear this option to disallow lowercase characters. |
| Default: Require a minimum of 1 |

Allow Numeric (0-9)
Select this option to allow Safeguard to create a password with numeric characters. Set the minimum number of required numeric characters, or set it to zero if there is no minimum requirement.

| NOTE: Clear this option to disallow numeric characters. |
| Default: Require a minimum of 1 |

Allow Symbols (e.g @ # $ % &)
Select this option to allow Safeguard to create a password with special characters. Set the minimum number of required symbolic characters, or set it to zero if there is no minimum requirement.

| NOTE: Clear this option to disallow special characters. |
| Default: Not allowed |

Valid Symbols
Enter allowable special characters, such as: ~!@#$%^*()_+-=';?\<><.,\]['\].

| NOTE: You must have the Allow Symbols option selected to enable this box. |

## Directory Change Password

Directory change password settings are the rules Safeguard uses to reset directory account passwords.

The **Directory Change Password** page displays the following about the listed directory change password setting rules.

**Table 209: Directory Change Password: Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the rule.</td>
</tr>
<tr>
<td>Directory</td>
<td>The directory that uses the rule.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the rule.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Displays the selected rule’s schedule.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage the directory change password setting rules.

**Table 210: Directory Change Password: Toolbar**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Add Change Password Setting</td>
<td>Add a directory account change password rule. For more information, see Adding directory change password settings on page 351.</td>
</tr>
<tr>
<td>Delete Selected</td>
<td>Remove the selected rule.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of directory account password change rules.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modify the selected rule.</td>
</tr>
<tr>
<td>Copy</td>
<td>&quot;Clone&quot; the selected rule.</td>
</tr>
</tbody>
</table>

**Adding directory change password settings**

It is the responsibility of the Asset Administrator or the partition's delegated administrator to configure the rules Safeguard uses to reset directory account passwords.

**To add a password reset schedule for directory accounts**

1. In Settings, select **Profile | Directory Change Password**.
2. Click (or tap) **+ Add Change Password Setting** to open the **Change Password Settings** dialog.
3. **Browse** to select a directory.
4. Enter a **Name** of up to 50 characters for the rule.
5. Enter a **Description** of up to 255 characters for the rule.
6. Click (or tap) the **Schedule** button and choose an interval.
7. In the **Schedule** dialog,
   a. **Interval**: Choose **Never, Minute, Hour, Day, Week, or Month**.
      
      **NOTE**: Best Practice: Do not use the **Minute** interval.
   b. **Time of day**: Set the start time.
   c. **Repeat interval**: Select the interval you would like to repeat the password reset task.
If **Weekly**, select which days of the week you want to repeat the change password task.

- If **Monthly**, set the task recurrence pattern: Day of month or week of month and day of week.

d. **Time Zone**: Select the time zone.

8. Optionally select this option:
   a. **Change the Password Even if a Release is Active**: Select this option to allow a password change even when a password release is active.
   b. **Require Current Password**: Select this option to require Safeguard to use the current password to change the directory account password. If you clear this option, Safeguard will change the account password without requiring the current password.
   c. **Suspend account when not checked out (supported platforms)**: Select this option to automatically suspend managed accounts that are not in use. That is, the account on a managed asset is suspended until a request is made for it through Safeguard, at which time Safeguard restores the account. Once the request is checked in or closed, the account is again suspended.

   Click (or tap) the **supported platforms** link to display a list of platforms that support this feature.

---

**Directory Check Password**

Directory check password settings are the rules Safeguard uses to verify directory account passwords.

The **Directory Check Password** page displays the following about the listed directory account check password setting rules.

**Table 211: Directory Check Password: Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the rule.</td>
</tr>
<tr>
<td>Directory</td>
<td>The directory that uses the rule.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the rule.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Displays the selected rule’s schedule.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage the directory account check password setting rules.
Table 212: Directory Check Password: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Add Check Password Setting] Add Check Password Setting</td>
<td>Add a directory account check password rule. For more information, see Adding directory check password settings on page 353.</td>
</tr>
<tr>
<td>![Delete Selected] Delete Selected</td>
<td>Remove the selected rule.</td>
</tr>
<tr>
<td>![Refresh] Refresh</td>
<td>Update the list of directory account check password rules.</td>
</tr>
<tr>
<td>![Edit] Edit</td>
<td>Modify the selected rule.</td>
</tr>
<tr>
<td>![Copy] Copy</td>
<td>&quot;Clone&quot; the selected rule.</td>
</tr>
</tbody>
</table>

Adding directory check password settings

It is the responsibility of the Asset Administrator or the partition’s delegated administrator to configure the rules Safeguard uses to verify directory account passwords.

To add a password validation schedule for directory accounts

1. In Settings, select Profile | Directory Check Password.
2. Click (or tap) ![Add Check Password Setting] Add Check Password Setting to open the Check Password Settings dialog.
3. Browse to select a directory.
4. Enter a Name of up to 50 characters for the rule.
5. Enter a Description of up to 255 characters for the rule.
6. Click (or tap) the Schedule button and choose an interval.
7. In the Schedule dialog,
   a. Interval: Choose Never, Minute, Hour, Day, Week, or Month.
      
      NOTE: Best Practice: Do not use the Minute interval.
   b. Time of day: Set the start time.
   c. Repeat interval: Select the interval you would like to repeat the password check task.
      
      • If Weekly, select which days of the week you want to repeat the password check task.
      • If Monthly, set the task recurrence pattern: Day of month or week of month and day of week.
   d. Time Zone: Select the time zone.
8. Optionally select this option:
Password Sync Groups

A password sync group is used to control password validation and reset across all associated accounts. The same password is used for one or more accounts associated with the same or different assets. For example, synchronized passwords can be used for accounts that support clusters or systems that sync between development, test, and production. An account can belong to only one password sync group. Multiple password sync groups can be added to a partition profile.

The profile change schedule is applied to the sync group. The sync group controls the tasks to change the passwords for the accounts in the sync group. Change tasks occur in the order of password sync group priority. If synchronization fails for an individual account in the sync group, the account is retried multiple times and, if failing after that, the sync task halts and is rescheduled. The administrator must correct the cause of the failure for the sync task to continue.

If an account is associated with a profile with a daily check schedule and also associated with a password sync group, a mismatch on the daily check will trigger a task to set the account password to the current sync group password.

For more information, see Creating a partition profile on page 239.

Password sync group priority

When an account is added to a password sync group, the default priority is 0 which is the highest priority. Subsequent numbers are lower priority (for example, 0, 1, 2, where 0 is the highest priority and 2 is the lowest). Priority determines the order in which account passwords are changed. If all accounts have the same priority, they are synchronized simultaneously. When different priorities are set, passwords at the highest priority (for example, 0) are synchronized first. If priority 0 is successful, accounts at the next priority are synchronized. If any account at a priority fails, the synchronization processing stops and the group is scheduled for synchronization retry. For example, a cluster of systems may have an admin account with the same password. If one master system is set at priority 0 and the subordinates are set at priority 1, the password change on the master must be successful before the passwords on the subordinates are changed. If the master password change fails, the subordinates are unaffected, the cluster continues to function, password change is rescheduled, and the error is logged.

The Password Sync Groups pane displays the following for each sync group.

Table 213: Sync Groups: Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>If Enable is selected, the sync runs with the Partition Profile</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Status</td>
<td>The <strong>Status</strong> displays if all account passwords are in sync with the password sync group. The <strong>Status</strong> is if any password for any account within the sync group does not match the common password.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the password sync group.</td>
</tr>
<tr>
<td>Partition</td>
<td>The partition that uses the rule.</td>
</tr>
<tr>
<td>Profile</td>
<td>The profile that uses the rule.</td>
</tr>
<tr>
<td>Accounts</td>
<td>The number of accounts to synchronize with a common password.</td>
</tr>
<tr>
<td>Next Sync Date</td>
<td>The date the sync group password will be synchronized across all accounts.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the rule.</td>
</tr>
</tbody>
</table>

Use the following toolbar buttons to manage password sync groups.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add a password sync group. For more information, see <a href="#">Adding a password sync group</a> on page 355.</td>
</tr>
<tr>
<td>Delete Selected</td>
<td>Permanently remove the selected password sync group.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of password sync groups.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modify the selected password sync group rule. For more information, see <a href="#">Modifying a password sync group</a> on page 356.</td>
</tr>
<tr>
<td>Change Sync Group Password</td>
<td>Change the password for the selected sync group. All accounts in the password sync group synchronize with the new password.</td>
</tr>
</tbody>
</table>

### Adding a password sync group

The Asset Administrator or a partition's delegated administrator defines the password sync group. An account can belong to only one password sync group. To assign sync groups and related accounts when adding the profile to a partition, see [Creating a partition profile](#).
To create a password sync group

1. In Settings, select Profile | Password Sync Group.
2. Click (or tap) + Add to open the Password Sync Group dialog.
3. Click (or tap) Browse to select a Profile. The Profile name displays.

   NOTE: Multiple password sync groups can be added to a profile. The profile change schedule is applied to the sync group. The sync group controls the tasks to change the passwords for the accounts in the sync group. Change tasks occur in the order of password sync group priority. For more information, see Password sync group priority on page 354.
4. Enter a Name of up to 100 characters.
5. Enter a Description of up to 255 characters.
6. Click (or tap) + Add and select one or more Accounts to be synchronized.
   The Accounts list displays with the following information about the account: Name, Parent, Service Account, Needs a Password (⚠️ if yes or ✅ if no), and Description. Click (or tap) any columns to sort the accounts.
7. Click (or tap) OK. The following values display:
   - Status: Displayed as ⚠️ if the password is not the same as the sync group, ✅ if the password is the same, or ⬜️ if the account is ignored and possibly should not be in the sync group.
   - Priority: The default is priority 0 (the highest). To change the priority, double-click the Priority value, enter the new priority, and click (or tap) OK. For more information, see Password sync group priority on page 354.
   - System Name: Name of the system (asset) assigned that is associated with the account.
   - Account Name: Name of the account.
   - Last Sync Time: The date and time of the last sync.
8. Click OK.

Modifying a password sync group

You can make modifications to the priority of a password sync group, the accounts assigned to a password sync group, or sync the selected account password.

To modify the priority of a password sync group or perform other modifications

1. In the Password Sync Group dialog, select the password sync group then click (or tap) ⌁ Edit.
2. Modify the Name or Description, if desired.
3. Click (or tap) any column in the account list to sort the accounts.
4. To modify an account priority, select the account then click (or tap) Edit.

5. Enter the Priority then click (or tap) OK. For more information, see Password sync group priority on page 354.

6. Perform any of the following account modifications:
   - Click (or tap) Add to add an account to the password sync group.
   - Click (or tap) Remove Selected to remove the selected account from the password sync group. This does not delete the account from Safeguard.
   - Click (or tap) Refresh to update the account list.
   - Click (or tap) Sync Now to sync the selected account password to match the sync group password. The Status follow:
     - ✓ displays when the account password is in sync with the password sync group.
     - ⚠ displays if the password is not in sync.

**Safeguard Access settings**

Safeguard allows you to configure these settings related to accessing One Identity Safeguard.

**Table 215: Safeguard Access settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Control</td>
<td>Where you configure the user login control settings.</td>
</tr>
<tr>
<td>Password Rules</td>
<td>Where you configure user password complexity rules.</td>
</tr>
</tbody>
</table>

**Login Control**

It is the responsibility of the Appliance Administrator to configure the Safeguard user login control settings, such as the number of failed sign-in attempts before locking out an account.

*To configure the login controls*

1. In Settings, select Safeguard Access | Login Control.
2. Provide the following information:
   - Token Lifetime: Set the number of minutes a user can stay logged into
**Safeguard.**

Range: 10 minutes to 28800 minutes (20 days)
Default: 1440 minutes (1 day)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lockout Duration</strong></td>
<td>Set the number of minutes a locked out account remains locked. Range: 1 to 9999 minutes; A setting of 9999 requires an administrator to manually unlock the account. Default: 15 minutes</td>
</tr>
<tr>
<td><strong>Lockout Threshold</strong></td>
<td>Set the number of consecutive failed sign-in attempts within the Lockout Window required to lock a user account. If a user submits an incorrect password for the maximum number of times specified by the account Lockout Threshold settings within the Lockout Window, Safeguard locks the account until the Lockout Duration period has been met. Range: 0 to 100 failed sign-in attempts; A value of 0 (zero) indicates the user’s account will never be locked due to failed log ins. Default: 5 consecutive failures</td>
</tr>
<tr>
<td><strong>Lockout Window</strong></td>
<td>Set the duration (in minutes) in which Safeguard increments the number of failed sign-in attempts. Range: 0 to 15 minutes; A value of 0 (zero) means that there is no time limit to tracking failed log on attempts. Default: 10 minutes</td>
</tr>
<tr>
<td><strong>Disable After</strong></td>
<td>Set the number of days to wait before automatically disabling an inactive user account. If a user has not logged onto Safeguard this number of days, Safeguard disables the user account. NOTE: The Authorizer Administrator must also reset the user's password when re-enabling a disabled account. Range: 14 to 365 days Default: 365 days</td>
</tr>
<tr>
<td><strong>Inform User of Disabled Account</strong></td>
<td>Select this option to inform users when Safeguard has disabled their account when they attempt to log in. When TIP: Set the Lockout Threshold to a high enough number that authorized users are not locked out of their user accounts simply because they mistype a password.</td>
</tr>
</tbody>
</table>
cleared, Safeguard tells the user that his or her access has been denied.

NOTE: For security reasons, One Identity recommends leaving this option cleared, unless you are troubleshooting login and authentication problems.

A disabled user cannot sign into Safeguard until an administrator has re-enabled his or her account. For more information, see Enabling or disabling a user on page 390.

Default: Not set

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inform User of Locked Account</td>
<td>Select this option to inform users when Safeguard has locked their account when they attempt to log in. When cleared, Safeguard tells the user that his or her access has been denied.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum Password Age</td>
<td>Set the number of days a user must wait before changing his or her password.</td>
<td>0 to 14 days</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Password Age</td>
<td>Set the number of days users can use their current password before they must change it.</td>
<td>0 to 180 days; A value of 0 (zero) indicates passwords never expire.</td>
<td>42 days</td>
</tr>
<tr>
<td>Password Age Reminder</td>
<td>Set the period of time (in days) before the Maximum Password Age limit is met and Safeguard begins to remind the user that their password is about to expire.</td>
<td>0 to 30 days</td>
<td>14 days</td>
</tr>
<tr>
<td>Password History</td>
<td>Enter the number of old passwords stored by Safeguard for user accounts. Stored passwords cannot be reused, and are replaced on a first-in first-out basis.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
NOTE: Administrators are not restricted by the password history setting.

Range: 0 to 24 old passwords; A value of 0 (zero) disables password history restrictions allowing users to always reuse old passwords.

Default: 5 stored passwords

Password Rules

Password rules define the complexity requirements for user authentication to Safeguard. Some companies suggest or impose requirements on what type of password a user can create, such as:

- The use of both upper- and lower-case letters.
- Inclusion of one or more numerical digits.
- Inclusion of special characters, such as @, #, $ and so forth.

NOTE: These rules only apply to local users; they do not impact users accessing Safeguard from an external provider such as Microsoft Active Directory. The password rules are listed in the Set password dialog. For more information, see Setting a local user's password on page 389.

Related Topics

Account Password Rules

Modifying user password requirements

It is the responsibility of the Authorizer Administrator to configure the user password rules.

To configure user password rules

1. In Settings, select Safeguard Access | Password Rules.
2. Set the Password Length from 3 to 255 characters.
   - Default: 6 to 64 characters

NOTE: The maximum length must be equal to or greater than the sum of minimum characters described in the next step.
3. Set the character **Requirements:**

<table>
<thead>
<tr>
<th>First Character Type</th>
<th>Choose one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- <strong>All</strong>: Alphabetical, numeric, or symbols</td>
</tr>
<tr>
<td></td>
<td>- <strong>Alphanumeric</strong>: Alphabetical or numeric</td>
</tr>
<tr>
<td></td>
<td>- <strong>Alphabetic</strong>: Only alphabetical characters</td>
</tr>
<tr>
<td>Default: <strong>All</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Last Character Type</th>
<th>Choose one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- <strong>All</strong>: Alphabetical, numeric, or symbols</td>
</tr>
<tr>
<td></td>
<td>- <strong>Alphanumeric</strong>: Alphabetical or numeric</td>
</tr>
<tr>
<td></td>
<td>- <strong>Alphabetic</strong>: Only alphabetical characters</td>
</tr>
<tr>
<td>Default: <strong>All</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allow Consecutively Repeated Characters</th>
<th>Select this option to allow a user to create a password with consecutively repeated characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>NOTE</strong>: Clear this option to disallow consecutively repeated characters.</td>
</tr>
<tr>
<td>Default: <strong>Allowed</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allow Uppercase</th>
<th>Select this option to allow Safeguard to create a password with uppercase characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set the minimum number of required uppercase characters, or set it to zero if there is no minimum requirement.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: Clear this option to disallow uppercase characters.</td>
</tr>
<tr>
<td>Default: <strong>Require a minimum of 1.</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allow Lowercase</th>
<th>Select this option to allow a user to create a password with lowercase characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set the minimum number of required lowercase characters, or set it to zero if there is no minimum requirement.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: Clear this option to disallow lowercase characters.</td>
</tr>
<tr>
<td>Default: <strong>Require a minimum of 1.</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Allow Numeric (0-9)</th>
<th>Select this option to allow a user to create a password with numeric characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set the minimum number of required numeric characters, or set it to zero if there is no minimum requirement.</td>
</tr>
</tbody>
</table>
Sessions settings

One Identity Safeguard enables you to issue privileged access to users for a specific period or session and gives you the ability to record, archive, and replay user sessions so that your company can meet its auditing and compliance requirements.

It is the responsibility of the Appliance Administrator to configure the One Identity Safeguard Privileged Sessions settings.

Table 216: Sessions settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Recordings Storage Management</td>
<td>Where you assign an archive server to an appliance for storing session recordings produced by that appliance.</td>
</tr>
<tr>
<td>Sessions Module</td>
<td>Where you can view the current status of the sessions module, enable debug logging and reset the sessions module if the Privileged Sessions module is not responding and users cannot connect to their target systems.</td>
</tr>
<tr>
<td>SSH Banner</td>
<td>Where you define the banner text shown to session users notifying them that they are being recorded.</td>
</tr>
<tr>
<td>SSH Host Key</td>
<td>Where you specify the SSH key to be used for authentication to an SSH session.</td>
</tr>
</tbody>
</table>
Session Recordings Storage Management

One Identity Safeguard provides the ability to immediately archive session recordings from a specific Safeguard appliance to a specified archive target. When an archive server is configured, session recordings for that appliance are removed from the Safeguard appliance and stored on the archive server. Use the **Session Recordings Storage Management** pane to assign archive servers to your Safeguard appliances.

**IMPORTANT:** When storing session recordings locally, once the local storage reaches capacity, the oldest recordings will be deleted. When storing session recordings to an archive server, the session recording is archived to the designated server immediately upon completion. As soon as the recording is copied to the archive server, it is removed from the appliance storage. Safeguard allows you to play back a recording that is stored locally or on the archive server. However, if you are playing back a recording that is stored on an archive server you will need to download it before you can play it. For more information, see [Replaying a session](#) on page 91.

### Table 217: Session Recordings Storage Management: Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance ID</td>
<td>The ID assigned to an appliance.</td>
</tr>
<tr>
<td>Archive Server Name</td>
<td>The name of the designated archive server.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage archive server configurations for session recordings.

### Table 218: Session Recordings Storage Management: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Refresh]</td>
<td>Update the list of designated archive servers being used to archive session recordings.</td>
</tr>
<tr>
<td>![Assign Archive Server to Appliance]</td>
<td>Specify the archive server to be associated with the selected appliance. Clicking this button displays the <strong>Archive Servers</strong> dialog allowing you to select the archive server where session recordings are to be stored for the selected appliance. For more information, see <a href="#">Assigning an archive server to an appliance</a> on page 364.</td>
</tr>
<tr>
<td>![Unassign Archive Server from Appliance]</td>
<td>Unassign the specified archive server from the selected appliance.</td>
</tr>
</tbody>
</table>
Assigning an archive server to an appliance

It is recommended that you assign an archive server to each appliance in your Safeguard deployment to store that appliance’s session recordings. This best practice will prevent you from filling up the appliance’s local disk space.

**IMPORTANT: Clustered environment:** It is highly recommended that you assign an archive server to at least the primary appliance in a clustered environment. You may also want to consider assigning an archive server to each individual appliance in the cluster.

If a replica in the cluster does not have an archive server assigned to it for its session recordings, the primary appliance will act as a proxy for archiving any recordings for that replica. If the primary appliance does not have an archive server assigned for session recordings, the following will happen:

- Any recorded session produced by the primary appliance will remain on the primary appliance.
- All recorded sessions produced by any replica in the cluster without an assigned archive server will also remain on the primary appliance.
- Each of these recordings will be replicated to every cluster member and therefore consume a lot of disk space throughout the cluster.

Therefore, in order to avoid filling up the appliances’ disk space, not only on the primary appliance but also on the replica appliances, is to ensure that at least the primary appliance has an archive server assigned for storing session recordings.

**To assign an archive server to an appliance**

**NOTE: Clustered environment:** Log into the primary appliance to assign archive servers to your primary appliance and replica appliances.

1. In **Settings**, select **Backup and Retention | Archive Servers** to configure your archive servers. For more information, see Adding an archive server on page 290.

2. In **Settings**, select **Sessions | Session Recordings Storage Management** to assign an archive server to the appliance.
   a. Select the appliance from the grid.
   b. Click (or tap) the **Assign Archive Server to Appliance** toolbar button.
   The name of the target archive server will appear in the **Archive Server Name** column.

**Sessions Module**

From the Sessions Module pane, an Appliance Administrator can view the current status of the One Identity Safeguard Privileged Sessions module and reset the sessions module.
### Table 219: Sessions Module controls

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✂️ Refresh</td>
<td>Click (or tap) to retrieve and update the session module's status.</td>
</tr>
</tbody>
</table>
| ⚖️ Health Check | Click (or tap) to run and display the results of the health check run against the sessions module. An additional pane appears, displaying results for the following:  
  - HTTP: Checks whether Safeguard can communicate with the sessions module via the internal web interface.  
  - SSH: Checks whether Safeguard can communicate with the sessions module via the internal SSH channel.  
  - SNMP: Checks whether Safeguard can communicate with the sessions module via the SNMP channel. It also checks whether the sessions module can report significant events back to Safeguard via SNMP.  
  - Keys: Checks whether the proper keys are in place in order for the sessions module to communicate back to Safeguard.  
  - Internal: Checks whether the sessions module can interact with Safeguard once a session request has been made.  
  
  ❧ **NOTE:** The background of the Session Module Health pane changes colors indicating the current health of the sessions module:  
    - Green: All components of the sessions module are healthy (OK).  
    - Red: An error was encountered with at least one of the components. The error message is displayed.  
  
  Click X in the upper right corner to close the Session Module Health pane. |

<table>
<thead>
<tr>
<th>Module Status</th>
<th>Displays the current status of the Privileged Sessions module.</th>
</tr>
</thead>
</table>

| Reset Sessions Module | When the Privileged Sessions module is not responding and users cannot connect to their target systems, click the **Reset Sessions Module** button to reboot the sessions module. Click (or tap) **Reset Now** in the **Reset Sessions Module** confirmation dialog.  
  
  ❧ **NOTE:** Resetting the sessions module will terminate all active sessions. |

### SSH Banner

It is the responsibility of the Appliance Administrator to define the banner text shown to session users when they initiate a privileged session. The SSH banner notifies session users that One Identity Safeguard will record the current session.
To define the SSH banner text

1. In **Settings**, select **Sessions | SSH Banner**.
2. In the **Banner Text** box, enter the text to be displayed to session users.
3. Click (or tap) **OK** to save the message.

**SSH Host Key**

The SSH Host Key pane allows the Appliance Administrator to verify or specify the SSH host key presented to the user's SSH client whenever an SSH session is started.

**Table 220: SSH Host Key settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint</td>
<td>Displays the SSH key fingerprint identifying the host to which you are currently connected.</td>
</tr>
<tr>
<td><strong>Set New Key</strong></td>
<td>Click (or tap) <strong>Set New Key</strong> to set a new SSH private key for authenticating to an SSH session.</td>
</tr>
<tr>
<td><strong>Generate New Key Pair</strong></td>
<td>If you do not have an SSH key, click (or tap) <strong>Generate New Key Pair</strong> to generate a new SSH key to use for authentication to an SSH session.</td>
</tr>
<tr>
<td><strong>Download Public Key</strong></td>
<td>Click (or tap) <strong>Download Public Key</strong> to download a public SSH key for authenticating to an SSH session.</td>
</tr>
</tbody>
</table>
Users

A user is a person who can log into Safeguard. You can add both local users and directory users. Directory users are users from an external identity store such as Microsoft Active Directory. For more information, see Adding directory accounts to a directory on page 193.

NOTE: Users displayed in a faded color are disabled.
To search for a particular user, see Search box on page 65.

Your administrator permissions determine what you can view in Users. The following table shows you the tabs that are available to each type of administrator.

Table 221: Administrator permission affect what you see in Users

<table>
<thead>
<tr>
<th>Administrator</th>
<th>Available tabs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorizer Administrator</td>
<td>General, History</td>
</tr>
<tr>
<td>User Administrator</td>
<td>General, User Groups (directory users only), History</td>
</tr>
<tr>
<td>Help Desk Administrator</td>
<td>General, History*</td>
</tr>
<tr>
<td>Auditor</td>
<td>General, User Groups, Partitions, Entitlements, Linked Accounts, History (Read only)</td>
</tr>
<tr>
<td>Asset Administrator</td>
<td>General, Partitions, History*</td>
</tr>
<tr>
<td>Security Policy Admin.</td>
<td>General, User Groups, Entitlements, Linked Accounts, History*</td>
</tr>
</tbody>
</table>

* This administrator can only view the user object history for his or her own account.

The Authorizer Administrator typically controls the Enabled/Disabled state. For more information, see Enabling or disabling a user on page 390.
The **Users** view displays the following information about a selected user:

### Table 222: Users: Tabs

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td>Displays the authentication, contact information, location, and permissions for the selected user.</td>
</tr>
<tr>
<td>User Groups tab</td>
<td>Displays the user groups in which the selected user is a member.</td>
</tr>
<tr>
<td>Partitions tab</td>
<td>Displays the partitions over which the selected user is a delegated partition administrator.</td>
</tr>
<tr>
<td>Entitlements tab</td>
<td>Displays the entitlements in which the selected user is a member; that is, an entitlement &quot;user&quot;.</td>
</tr>
<tr>
<td>Linked Accounts tab</td>
<td>Displays the directory accounts linked to the selected user.</td>
</tr>
<tr>
<td>History tab</td>
<td>Displays the details of each operation that has affected the selected user.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage users:

### Table 223: Users: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✚ Add User</td>
<td>Add users to Safeguard. For more information, see Adding a user on page 375.</td>
</tr>
<tr>
<td>⏪ Delete Selected</td>
<td>Remove the selected user. For more information, see Deleting a user on page 387.</td>
</tr>
<tr>
<td>⌛ Refresh</td>
<td>Update the list of users.</td>
</tr>
<tr>
<td>☐ Import Users</td>
<td>Add users to Safeguard. For more information, see Importing objects on page 388.</td>
</tr>
<tr>
<td> User Security</td>
<td>Menu options include: <strong>Set Password</strong> and <strong>Unlock</strong> accounts. For more information about these options, refer to Setting a local user’s password and Unlocking a user’s account.</td>
</tr>
<tr>
<td> Permissions</td>
<td>Display the <strong>Permissions</strong> dialog showing what administrative permissions apply to the selected user.</td>
</tr>
</tbody>
</table>
General tab

The **General** tab lists information about the selected user.

Large tiles at the top of the tab display the number of **User Groups, Partitions, Entitlements, and Linked Accounts** associated with the selected user. Clicking a tile heading opens the corresponding tab.

**NOTE:** The tiles visible depend on your administrator permissions:

- All tiles are visible to the Auditor.
- **Partitions** tile is visible to Asset Administrator.
- **User Groups, Entitlements and Linked Accounts** tiles are visible to Security Policy Administrator.

### Table 224: Users General tab: Authentication properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>A user’s display name.</td>
</tr>
<tr>
<td>Authentication Provider</td>
<td>How the user authenticates with Safeguard:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Certificate</strong>: with a certificate</td>
</tr>
<tr>
<td></td>
<td>- <strong>Local</strong>: with a user name and password</td>
</tr>
<tr>
<td></td>
<td>- <strong>Directory name</strong>: with directory credentials</td>
</tr>
<tr>
<td>Domain Name</td>
<td>If the primary <strong>Authentication Provider</strong> is a directory, this indicates the directory's domain name.</td>
</tr>
<tr>
<td>Secondary Authentication</td>
<td>If you set up a user to require secondary authentication, this indicates the name of this user's secondary authentication service provider.</td>
</tr>
<tr>
<td>Username</td>
<td>The name of the user account on the secondary authentication service provider required at log in.</td>
</tr>
</tbody>
</table>

### Table 225: Users General tab: Contact Information properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>The user's first name.</td>
</tr>
<tr>
<td>Last Name</td>
<td>The user's last name.</td>
</tr>
<tr>
<td>Work Phone</td>
<td>The user's work telephone number.</td>
</tr>
<tr>
<td>Mobile Phone</td>
<td>The user's mobile telephone number.</td>
</tr>
<tr>
<td>Email Address</td>
<td>The user's email address.</td>
</tr>
</tbody>
</table>
Table 226: Users General tab: Location properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Zone</td>
<td>The user's regional location on Earth.</td>
</tr>
</tbody>
</table>

Table 227: Users General tab: Permissions properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permissions</td>
<td>Lists the user's administrator permissions or &quot;Standard User&quot; if user does not have administrative permissions.</td>
</tr>
</tbody>
</table>

**Description**: Information about the selected user.

**Related Topics**

Modifying a user

**User Groups tab**

The **User Groups** tab displays the user groups in which the selected user is a member.

**NOTE**: The **User Groups** tab is available to a user with Auditor or Security Policy Administrator permissions and to the User Administrator for directory users (not for local users).

Click (or tap) + **Add User Group** from the details toolbar to add the selected user to one or more user groups.

**Search**: For more information, see Search box on page 65.

Table 228: Users: Users Groups tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The user group name.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of group: <strong>User Group</strong> or <strong>Directory Group</strong>.</td>
</tr>
<tr>
<td>Distinguished Name</td>
<td>The distinguished name of the group.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the selected user group.</td>
</tr>
</tbody>
</table>

**Related Topics**

Adding a user to user groups
Partitions tab

The **Partitions** tab displays the partitions over which the selected user is a delegated partition administrator.

### NOTE: The **Partitions** tab is available to a user with Auditor or Asset Administrator permissions.

Click (or tap) **Add Partition(s)** from the details toolbar to delegate the selected user as an administrator to one or more partitions.

**Search:** For more information, see **Search box** on page 65.

**Table 229: Users: Partitions tab properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The partition name.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the selected partition.</td>
</tr>
</tbody>
</table>

**Related Topics**

Assigning a user to partitions

Entitlements tab

The **Entitlements** tab displays the entitlements in which the selected user is a member.

### NOTE: The **Entitlements** tab is only available to a user with Auditor or Security Policy Administrator permissions.

Click (or tap) **Add Entitlement** to add the selected user as a "user" of one or more entitlement.

**Table 230: Users: Entitlements tab properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the entitlements in which the selected user is a &quot;user&quot;.</td>
</tr>
<tr>
<td>Access Request Policies</td>
<td>The number of unique access request policies in the entitlement.</td>
</tr>
<tr>
<td>Accounts</td>
<td>The number of unique accounts in the selected entitlement.</td>
</tr>
<tr>
<td>Users</td>
<td>The number of unique users in the entitlement.</td>
</tr>
</tbody>
</table>
### Users: Entitlements tab toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✚ Add Entitlement</td>
<td>Add the selected user to one or more entitlements. For more information, see Adding a user to entitlements on page 385.</td>
</tr>
<tr>
<td>Remove Selected</td>
<td>Remove the user from the selected entitlement.</td>
</tr>
<tr>
<td>☛ Refresh</td>
<td>Update the list of entitlements.</td>
</tr>
<tr>
<td>☁ Details</td>
<td>View additional details about the selected entitlement.</td>
</tr>
<tr>
<td>🔍 Search</td>
<td>To locate a specific entitlement or set of entitlements in this list, enter the character string to be used to search for a match. For more information, see Search box on page 65.</td>
</tr>
</tbody>
</table>

### Linked Accounts tab

The **Linked Accounts** tab displays the directory accounts linked to the selected user that can be used in session request policies to access the assets or accounts defined within the scope of the policy.

Click (or tap) **✚ Add Linked Account** from the details toolbar to link a directory account to the selected user.

**Search:** For more information, see Search box on page 65.
### Table 232: Users: Linked Accounts tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The account name.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The name of the domain where the linked account resides.</td>
</tr>
<tr>
<td>Service Account</td>
<td>A check in this column indicates that the account is a service account.</td>
</tr>
<tr>
<td>Password Request</td>
<td>A check in this column indicates that password release requests are enabled for the account.</td>
</tr>
<tr>
<td>Session Request</td>
<td>A check in this column indicates that session access requests are enabled for the account.</td>
</tr>
<tr>
<td>Needs a Password</td>
<td>Displays 🔐 if a password is not set for the account. For more information, see Checking, changing, or setting an account password on page 110.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the selected account.</td>
</tr>
</tbody>
</table>

### Related Topics

- Linking a directory account to a user

### History tab

The History tab allows you to view or export the details of each operation that has affected the selected user.

- **NOTE:** Help Desk Administrators, Asset Administrators, and Security Policy Administrators can only view the user object history for their own account.

The History tab contains the following information:

- **Items**: Total number of entries in the history log.
- **Search**: For more information, see Search box on page 65.
- **Time Frame**: By default the history details are displayed for the last 24 hours. Click (or tap) one of the time intervals at the top of the grid to display history details for a different time frame. If the display does not refresh after selecting a different time interval, click (or tap) **Refresh**.

### Table 233: Users: History tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>The date and time of the event.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User</td>
<td>The display name of the user that triggered the event.</td>
</tr>
<tr>
<td>Source IP</td>
<td>The network DNS name or IP address of the managed system that triggered the event.</td>
</tr>
<tr>
<td>Object Name</td>
<td>The name of the selected user.</td>
</tr>
<tr>
<td>Event</td>
<td>The type of operation made to the selected user:</td>
</tr>
<tr>
<td></td>
<td>- Create</td>
</tr>
<tr>
<td></td>
<td>- Delete</td>
</tr>
<tr>
<td></td>
<td>- Update</td>
</tr>
<tr>
<td></td>
<td>- Add Membership</td>
</tr>
<tr>
<td></td>
<td>- Remove Membership</td>
</tr>
</tbody>
</table>

**NOTE:** A membership operation indicates a "relationship" change with a related or parent object such as the selected user was added or removed from the membership of a user group or entitlement.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related Object</td>
<td>The name of the related object.</td>
</tr>
<tr>
<td>Related Object Type</td>
<td>The type of the related object.</td>
</tr>
<tr>
<td>Parent</td>
<td>The name of the object to which the selected user is a child.</td>
</tr>
<tr>
<td>Parent Object Type</td>
<td>The parent object type.</td>
</tr>
</tbody>
</table>

Select an event to display this additional information for some types of events (for example, create and update events).

**Table 234: Additional History tab properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>The property that was updated.</td>
</tr>
<tr>
<td>Old Value</td>
<td>The value of the property before it was updated.</td>
</tr>
<tr>
<td>New Value</td>
<td>The new value of the property.</td>
</tr>
</tbody>
</table>

**Managing users**

Use the controls and tabbed pages on the Users page to perform the following tasks to manage Safeguard users:
Adding a user

It is the responsibility of either the Authorizer Administrator or the User Administrator to add Safeguard users.

**To add a user**

1. Navigate to Administrative Tools | Users.
2. In Users, click (or tap) + Add User from the toolbar.
3. In the User dialog, provide information in each of the tabs:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity tab</td>
<td>Where you define the authentication provider, user name and password.</td>
</tr>
<tr>
<td>Authentication tab</td>
<td>Where you define the authentication provider, user name and password.</td>
</tr>
<tr>
<td>Contact Information tab</td>
<td>Where you add the user's contact information.</td>
</tr>
<tr>
<td>Location tab</td>
<td>Where you set the user's time zone.</td>
</tr>
<tr>
<td>Permissions tab</td>
<td>Where you set the user's administrator permissions.</td>
</tr>
</tbody>
</table>

**Related Topics**

Adding users or user groups to an entitlement

Adding users to a user group
Authentication tab

On the Authentication tab, specify the authentication settings for the user.

Table 235: User: Authentication tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Provider</td>
<td>Indicate how this user is to authenticate to Safeguard:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Certificate</strong>: with a certificate</td>
</tr>
<tr>
<td></td>
<td>️</td>
</tr>
<tr>
<td></td>
<td>- <strong>Local</strong>: With a user name and password (default)</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;Directory name&gt;</code>: with directory account credentials (only available if one or more directories have been added to Safeguard.)</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;External Federation service provider name&gt;</code>: With external federation authentication (only available if an external federation service provider has been configured in Safeguard)</td>
</tr>
<tr>
<td>User Name</td>
<td>If using <strong>Certificate</strong> or <strong>Local</strong> authentication, enter the user's display name.</td>
</tr>
<tr>
<td></td>
<td>If using directory authentication, <strong>Browse</strong> to select a user name. For more information, see Adding a directory user account on page 382.</td>
</tr>
<tr>
<td></td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>Limit: 255 characters</td>
</tr>
<tr>
<td><strong>Set Password</strong></td>
<td>Click (or tap) this button to change a user's password.</td>
</tr>
<tr>
<td></td>
<td>️</td>
</tr>
<tr>
<td>Certificate Thumb-print (SHA-1)</td>
<td>If adding a <strong>Certificate</strong> user, enter the unique hash value (40 hexadecimal characters) of the certificate.</td>
</tr>
<tr>
<td></td>
<td>️</td>
</tr>
<tr>
<td>Password</td>
<td>If adding a <strong>Local</strong> user, enter a password for the user.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>You must comply with the password requirements specified in the dialog. For more information, see Password Rules on page 360. Required limit: 64 characters</td>
</tr>
</tbody>
</table>
| Email Address or Name Claim | If adding an external federation user account, enter the email address or name claim that will be returned from the IdP-STS of an authenticated user.  
  | NOTE: A case-insensitive comparison will be performed on the value when the user is logging in.                                               |
|                          | NOTE: You must configure or ensure that the IdP-STS includes either the email address claim or name claim. Safeguard will first look for the email address claim in the claims token. If that claim does not exist, it will use the name claim. You must create the user account in Safeguard according to what claim is returned by your IdP-STS, with precedence given to the email address claim. |
| Require Certificate Authentication | Select this check box to require that the user logs into Safeguard using their domain issued user certificate or SmartCard.  
  | NOTE: This option is only available when the Authentication Provider is a Microsoft Active Directory.                                                                                                   |
| Require Secondary Authentication | Select this check box to require that this user logs into Safeguard with two-factor authentication. For more information, see Requiring user to log in using secondary authentication on page 380. |
| Authentication Provider   | When Require Secondary Authentication is selected, choose the secondary authentication provider for this user.  
<p>| - When the primary authentication provider is Active Directory, the secondary authentication provider can be LDAP, Radius, or Starling Two-Factor Authentication. |
|                          | - When the primary authentication provider is LDAP, the secondary authentication provider can be Active Directory, Radius, or Starling Two-Factor Authentication. |
|                          | - When the primary authentication provider is Local, the secondary authentication provider can be Active Directory, LDAP, Radius, or Starling Two-Factor Authentication. |
|                          | Depending on the type of authentication provider selected, additional information is required.                                                                                           |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>When a directory is selected, <strong>Browse</strong> to select the account on the secondary authentication provider this user must use when logging into Safeguard with two-factor authentication.</td>
</tr>
<tr>
<td></td>
<td>If Radius is selected, enter the name of the account on the secondary authentication provider this user must use when logging into Safeguard with two-factor authentication.</td>
</tr>
<tr>
<td>Use alternate mobile phone number</td>
<td>When Starling Two-Factor Authentication is selected, this option is available to enter an alternate mobile phone number.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The Approval Anywhere and one-touch approval features require a valid mobile phone number for the user. If the user does not have their mobile number published in Active Directory, use this option to specify a valid mobile phone number for the user.</td>
</tr>
<tr>
<td>Mobile phone number</td>
<td>If the <strong>Use alternate mobile phone number</strong> check box is selected, enter the mobile phone number to be used.</td>
</tr>
<tr>
<td>Number on file</td>
<td>This field displays the mobile phone number specified on the <strong>Contact Information</strong> tab of a user's record.</td>
</tr>
</tbody>
</table>

**Contact Information tab**

**NOTE:** When adding a user from an external provider such as Microsoft Active Directory, Safeguard imports read-only contact information from the source; however, you can change the photo for these users.

On the Contact Information tab, enter the user's contact information.

**Table 236: User: Contact Information tab properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>Enter the user's first name. Limit: 30 characters; no double quotes.</td>
</tr>
<tr>
<td>Last Name</td>
<td>Enter the user's last name. Limit: 30 characters; no double quotes.</td>
</tr>
<tr>
<td>Work Phone</td>
<td>Enter the user's work telephone number. Limit: 30 characters</td>
</tr>
<tr>
<td>Mobile Phone</td>
<td>Enter the user's mobile telephone number. Limit: 30 characters</td>
</tr>
</tbody>
</table>
NOTE: A valid mobile phone number in E.164 format is required for approvers using the Approval Anywhere feature and for two-factor authentication using Starling. However, you can use the **Use alternate mobile phone number** option on the **Authentication** tab to specify a valid mobile phone number, instead of adding it here.

E.164 format: +<country code><area code><phone number>

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email Address</strong></td>
<td>Enter the user's email address.</td>
</tr>
<tr>
<td></td>
<td>Limit: 255 characters</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Enter information about this user.</td>
</tr>
<tr>
<td></td>
<td>Limit: 255 characters</td>
</tr>
</tbody>
</table>

### Location tab

On the Location tab, specify the user's time zone.

**Table 237: User: Location tab properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Zone</strong></td>
<td>Select the user's time zone.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Because Microsoft Active Directory does not have a Time Zone attribute, when you add a directory group, Safeguard sets the default time zone for all imported accounts to (UTC) Coordinated Universal Time. To reset the time zone, open each imported account in <strong>Users</strong> and modify the Time Zone on the <strong>Location</strong> tab. Required</td>
</tr>
</tbody>
</table>

### Permissions tab

On the Permissions tab, select the user's Administrator permissions, if applicable. When assigning permissions to a user, you set the following access controls:
- Authorizer: Allow the user to grant permissions to other users.
  
  **NOTE:** This permission allows the user to change their own permissions.

- User: Allow the user to create new users, unlock and reset passwords for non-administrative users.

- Help Desk: Allow the user to unlock and set passwords for non-administrative users.

- Appliance: Allow the user to edit and update the appliance and to configure external integration settings, such as email, SNMP, Syslog, Ticketing, and Approval Anywhere.

- Operations: Allow the user to reboot and monitor the appliance.

- Auditor: Allow the user read-only access.

- Asset: Allow the user to add, edit and delete partitions, assets and accounts.

- Directory: Allow the user to add, edit and delete directories.

- Security Policy: Allow the user to add, edit and delete entitlements and polices that control access to accounts and assets.

For a more detailed list of permissions available, see Administrator permissions.

### Requiring user to log in using secondary authentication

You can require a user to log in using two-factor authentication by enabling the **Require Secondary Authentication** option in the user record.

**To require a user to log in using secondary authentication**

1. Setup a secondary authentication provider in **Settings | Secondary Authentication**.

2. Configure the Safeguard user to **Require Secondary Authentication**. For more information, see **Authentication tab** on page 376.
   a. On the Authentication tab of a user's properties, select the **Require Secondary Authentication** check box.
   b. Choose the **Authentication Provider**.
   c. Depending on the type of authentication provider selected, specify the additional information this user must use when logging into Safeguard with two-factor authentication.

3. Log in with secondary authentication.

   When you log into Safeguard with a user account that requires secondary authentication, you log in as usual, using the password that is set for the Safeguard user account. Safeguard then displays one or more additional login screens. Depending on how the system administrator has configured the secondary authentication provider, you must enter additional authenticators for your secondary
authentication service provider account, such as a secure password and/or security token code.

**NOTE:** The type and configuration of the secondary authentication provider (RSA SecureID, One Identity Starling Two-Factor Authentication, Microsoft Azure, etc.) determines what you must provide for secondary authentication. Check with your system administrator for more information about how to log into Safeguard with secondary authentication.

## Configuring user to use Starling Two-Factor Authentication when logging into Safeguard

It is the responsibility of the Authorizer Administrator or the User Administrator to configure a user account to use two-factor authentication when logging into Safeguard.

**TIP:** If you want to use one-touch approvals, download and install the Starling 2FA app onto your mobile device.

### To configure users to use Starling Two-Factor Authentication when logging into Safeguard

1. Log into Safeguard as an Authorizer Administrator or User Administrator.
2. Navigate to Administrative Tools | Users.
3. Add or edit users, ensuring the following settings are configured:
   a. Authentication tab:
      - **Require Secondary Authentication**: Select this check box.
      - **Authentication Provider**: Select the Starling 2FA service provider.

      **NOTE:** If the Starling 2FA service provider is not listed, you must first join Safeguard to Starling. For more information, see Starling on page 334.

      - **Use alternate mobile phone number**: Optionally, select this check box and enter an alternate mobile number to be used for two-factor authentication notifications.

      **NOTE:** If you want to use one-touch approvals, this feature requires a valid mobile phone number for the user. If the user does not have their mobile number published in Active Directory, use this option to specify a valid mobile phone number for the user.

   b. Contact Information tab:
      - **Mobile Phone**: Enter a valid mobile phone number in E.164 format.
      - **Email Address**: Enter a valid email address.
Now whenever any of these users attempt to log into Safeguard, after entering their password, a message appears on the login screen informing them that an additional authentication step is required.

| NOTE: If the Safeguard user is required to use Starling Two-Factor Authentication and has the Starling 2FA mobile app installed, Safeguard sends a push notification to their mobile device where they can complete the login by pressing a button in the app. If the user does not have the Starling 2FA app, they have the option to receive a one-time password via SMS or a phone call. |

## Adding a directory user account

It is the responsibility of either the Authorizer Administrator or User Administrator to add directory users to Safeguard.

| NOTE: You must add directories (Active Directory or LDAP) to Safeguard before you can add directory user accounts. |

| IMPORTANT: Safeguard must be able to communicate with the global catalog for directory management tasks including the addition of a directory account, a directory user account, or a directory user group. Standard global catalog ports are 3268 (LDAP) and 3269 (LDAPS). |

### To add a directory user account

1. Navigate to Administrative Tools | Users.
2. In Users, click (or tap) + Add User from the toolbar.
3. In the User dialog, provide information in each of these tabs:

<table>
<thead>
<tr>
<th>Authentication tab</th>
<th>Where you define the authentication provider, user name and password.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Information tab</td>
<td>Where you add the user's contact information.</td>
</tr>
<tr>
<td>Location tab</td>
<td>Where you set the user's time zone.</td>
</tr>
<tr>
<td>Permissions tab</td>
<td>Where you set the user's administrator permissions.</td>
</tr>
</tbody>
</table>

### Authentication tab

When adding a directory user account, specify the following information on the Authentication tab:

1. In the Authentication Provider field, select a directory.
2. Browse to select a user name.
3. In the **User** dialog,
   a. **Browse** to select a container within the directory as the **Filter Search Location**.
   b. The **Include objects from sub containers** check box is selected by default indicating that child objects will be included in your search. Clear this check box to exclude child objects from your search.
   c. In the **Contains** field, enter a full or partial account name and press **Search**. Safeguard searches the entire forest root using the global catalog. You can search on partial strings. For example, if you enter "ad" in the search box, it will find any user **Name** or **Distinguished Name** that contains "ad".

   **NOTE:** The text search is not case sensitive and does not allow wild cards.
   
d. The results of the search displays in the **Select the user to add** grid. Select a user account to add to Safeguard.
   e. Click (or tap) **OK** to save the selected account and close the dialog.

4. Select the **Require Certificate Authentication** check box to require that the user logs into Safeguard using their domain issued user certificate or Smart Card.

   **NOTE:** This option is only available when the **Authentication Provider** is a Microsoft Active Directory.

5. Select the **Require Secondary Authentication** check box to require that this user logs into Safeguard with two-factor authentication. For more information, see **Requiring user to log in using secondary authentication** on page 380.

6. Choose the secondary authentication provider for this user.

7. Once the secondary authentication provider is specified, choose or enter the information required for two-factor authentication based on the type. For more information, see **Authentication tab** on page 376.

## Adding a user to user groups

**NOTE:** It is the responsibility of the Security Policy Administrator to add users to user groups to assign to password policies.

### To add a user to one or more user groups

1. Navigate to **Administrative Tools | Users**.
2. In **Users**, select a user from the object list and open the **User Groups** tab.
3. Click (or tap) **+ Add User Groups** from the details toolbar.
4. Select one or more groups from the list in the **User Groups** dialog and click (or tap) **OK**.
NOTE: You can also double-click (or double-tap) a group name to add it.

If you do not see the user group you are looking for, depending on your Administrator permissions, you can create it in the User Groups selection dialog. (You must have Security Policy Administrator permissions to create user groups.)

To create a new user group from the selection dialog

1. Click (or tap) + Create New.
   For more information about creating user groups, see Adding a user group.
2. Create additional user groups, as required.
3. Click (or tap) OK in the User Groups selection dialog to add the selected user to the user groups.

Assigning a user to partitions

Assigning a user to a partition makes that user the "Delegated Owner" of that partition, giving that person authorization to manage the assets and accounts in that partition. A delegated partition owner has a subset of the permissions that an Asset Administrator has. For more information, see Administrator permissions on page 421.

NOTE: It is the responsibility of the Asset Administrator to select one or more users to manage the assets and accounts in a partition.

To assign a user to one or more partitions

1. Navigate to Administrative Tools | Users.
2. In Users, select a user from the object list and open the Partitions tab.
3. Click (or tap) + Assign Partition(s) from the details toolbar.
4. Select one or more partitions from the list in the Partitions selection dialog and click (or tap) OK.

NOTE: You can also double-click (or double-tap) a partition name to add it.

If you do not see the partition you are looking for, depending on your Administrator permissions, you can create it in the Partitions selection dialog. (You must have Asset Administrator permissions to create partitions.)

To create a new partition in the Partitions selection dialog

1. Click (or tap) + Create New.
   For more information about creating partitions, see Adding a partition.
2. Create additional partitions, as required.
3. Click (or tap) OK in the Partition selection dialog to add the selected user to the partitions.
Adding a user to entitlements

When you add users to an entitlement, you are specifying which people can request access governed by the entitlement's policies.

NOTE: It is the responsibility of the Security Policy Administrator to add users to entitlements.

To add a user to one or more entitlements

1. Navigate to Administrative Tools | Users.
2. In Users, select a user from the object list and open the Entitlements tab.
3. Click (or tap) + Add Entitlement from the details toolbar.
4. Select one or more entitlements from the list in the Entitlements selection dialog and click (or tap) OK.

NOTE: You can also double-click (or double-tap) an entitlement name to add it.

If you do not see the entitlement you are looking for, depending on your Administrator permissions, you can create it in the Entitlements selection dialog. (You must have Security Policy Administrator permissions to create entitlements.)

To create a new entitlement from the Entitlements selection dialog

1. Click (or tap) + Create New.
   The Entitlement dialog displays. For more information about creating entitlements, see Adding an entitlement.
2. Create additional entitlements, as required.
3. Click (or tap) OK in the Entitlements selection dialog to add the selected user to the entitlements.

Linking a directory account to a user

NOTE: It is the responsibility of the Security Policy Administrator to link directory accounts to a user. Once linked, these linked accounts can be used to access assets and accounts within the scope of an access request policy.

To link a directory account to a user

1. Navigate to Administrative Tools | Users.
2. In Users, select a user from the object list and open the Linked Accounts tab.
3. Click (or tap) + Add Linked Account from the details toolbar.
The **Directory Account** dialog displays, listing the directory accounts available in Safeguard. This dialog includes the following details about each directory account listed:

- **Name**: Displays the name of the directory account.
- **Domain Name**: Displays the name of the domain where this account resides.
- **Password Request**: Indicates whether password release requests are allowed.
- **Needs a Password**: Indicates whether the account needs a password.
- **Description**: Displays descriptive text about the directory account.

4. Select one or more accounts from the list in the **Directory Account** selection dialog and click (or tap) **OK**.

## Modifying a user

The Authorizer Administrator and the User Administrator can modify the general information for a user.

**To modify a user's information**

1. Navigate to **Administrative Tools | Users**.
2. In **Users**, select a user from the object list.
3. Double-click (or double-tap) the user's name to open the **User** settings edit window.

   **NOTE:** You can also double-click (or double-tap) the **Authentication**, **Contact Information**, **Location**, or **Permissions** edit box on the **General** tab (or click (or tap) the ✎ Edit icon) to go directly to that view.

   **For example:**
   
   - To modify a user's authentication provider, change the user's password, or enter an alternate mobile phone number, double-click (or double-tap) the **Authentication** box, or click (or tap) the ✎ Edit icon.

     **NOTE:** Once you add a user, you cannot modify the user's name. If you change a user's authentication provider from **Local** to directory authentication, Safeguard will attempt to validate the local user name against the directory user names. If it does not match, you can **Browse** to select the correct user name.

   - To change a local user's contact information, double-click (or double-tap) the **Contact Information** box on the **General** tab or click (or tap) the ✎ Edit icon.

     **NOTE:** You cannot modify a directory user's contact information that is managed in the directory, such as Active Directory. If you need to add a valid mobile phone number, use the alternate mobile phone number option on the **Authentication** tab instead.
To modify the administrator permissions, double-click (or double-tap) the Permissions box on the General tab or click (or tap) the Edit icon.

**TIP:** As a best practice, to prevent users from gaining access to information after you change their administrative permissions, ensure that the user closes all connections to the appliance (or reboot the appliance).

**NOTE:** Help Desk Administrators, Asset Administrators, and Security Policy Administrators can only view the user object history for their own account.

4. The Security Policy Administrator can modify a user’s group membership on the user’s User Groups tab.

**NOTE:** You can multi-select user groups to add or remove more than one user on a user’s group membership.

5. The Asset Administrator can delegate partition ownership to a user on the user’s Partitions tab.

6. The Security Policy Administrator can add the selected user to an entitlement on the user’s Entitlements tab.

7. The Security Policy Administrator can add (or remove) linked accounts to an entitlement on the user’s Linked Accounts tab.

8. The Authorizer Administrator and the User Administrator can view or export the details of each operation that has affected the selected user on the History tab.

**NOTE:** Help Desk Administrators, Asset Administrators, and Security Policy Administrators can only view the user object history for their own account.

### Deleting a user

Typically, it is the responsibility of the Authorizer Administrator to delete administrator users and the User Administrator to delete non-administrator users.

**IMPORTANT:** When you delete a local user, Safeguard deletes it permanently. If you delete a directory user that is part of a directory group, next time it synchronizes its database with the directory, Safeguard will add it back in.

**To delete a user**

1. Navigate to Administrative Tools | Users.
2. In Users, select a user from the object list.
3. Click (or tap) Delete Selected.
4. Confirm your request.

**TIP:** As a best practice, disable the directory user instead of deleting the account. For more information, see Enabling or disabling a user on page 390.
Importing objects

Safeguard allows you to import a .csv file containing a set of accounts, assets, or users.

To import a set of objects

1. Click (or tap) Import from the toolbar.
2. In the Import dialog, Browse to select an existing .csv file containing a list of objects to import.
   
   **NOTE:** For assistance in creating an import file, click (or tap) CSV Template Assistant. For more information, see Creating an import file on page 109.

3. When importing assets, the Discover SSH Host Keys option is selected by default indicating that Safeguard will retrieve the required SSH host key for the assets specified in the CSV file.
4. Click (or tap) OK.

   Safeguard imports the objects into its database.

   **NOTE:** Safeguard does not add an object if any column contains invalid data in the .csv file with the follow exceptions:
   
   - **Assets PlatformDisplayName property.**
     a. If Safeguard does not find an exact match, it looks for a partial match. If it finds a partial match it supplies the `<platform>` Other platform, such as "Other Linux".
     b. If it does not find a partial match, it supplies the Other platform type.
   - **Users TimeZoneId property.**
     a. If Safeguard does not find a valid TimeZoneId property (that is, does not find an exact match or no timezone was provided), it uses the local workstation's current timezone.

   **NOTE:** Do not enter numbers or abbreviations for the TimeZoneId.
   - **Users Password property.**
     a. Safeguard adds a user without validating the password you provide.

5. Navigate to the Tasks pane in the Toolbox for details about the import process and invalid data messages. For more information, see Viewing task status on page 93.
Setting a local user's password

It is primarily the responsibility of the Authorizer Administrator to set passwords for administrators; and the User Administrator and Help Desk Administrator to set passwords for non-administrator local users.

NOTE: These administrators can only set passwords for local user accounts. Directory user account passwords are maintained in an external provider, such as Microsoft Active Directory.

There are three ways to set a password.

To set a local user's password

1. Navigate to Administrative Tools | Users.
2. In Users, select a local user from the object list, right-click (or press and hold) and select Set Password from the context menu.
   - OR-
   Click (or tap) the User Security menu and select Set Password.
   - OR-
   Open the Authentication box on the General tab and click (or tap) Set Password.
3. In the Set Password dialog, enter the new password and click (or tap) OK.

   NOTE: You must comply with the password requirements specified in the dialog. For more information, see Password Rules on page 360.

Unlocking a user's account

If you are unable to log in, your account may have become disabled or "locked". For example, if you enter a wrong password for the maximum number of times specified by the account Lockout Threshold settings, Safeguard locks your account. For more information, see Login Control on page 357.

Typically, it is the responsibility of the Authorizer Administrator to unlock administrator accounts; and the User Administrator and Help Desk Administrator to unlock non-administrator local users.

There are two ways to unlock a user account.

To unlock a user's account

- In Users, select a "locked" user, right-click (or press and hold) and select Unlock from the context menu.
  - OR-
  - Click (or tap) the User Security menu and select Unlock.
Enabling or disabling a user

Typically, it is the responsibility of the Authorizer Administrator to enable or disable administrator users and the User Administrator to enable or disable non-administrator users.

To enable or disable a user

1. Navigate to Administrative Tools | Users.
2. In Users, select a user from the object list.
3. Click (or tap) Enabled or Disabled.

   This icon, located in the upper-right corner of the console, toggles between the two settings.

   ![NOTE: You configure the number of days you want Safeguard to wait before automatically disabling an inactive user account in the Disable After Login Control Setting. For more information, see Login Control on page 357.](image)

   ![NOTE: The Authorizer Administrator must also reset the user's password when re-enabling a disabled account. Simply enabling the account does not permit the user to login with his previous password.](image)

Disabling a user prevents him or her from logging into Safeguard; however, if you disable a directory user, that does not prevent that user from logging into the directory. You can modify a disabled user's information.
User Groups

Safeguard allows you to add both user groups (a set of local users) and directory groups (a set of directory accounts) to User Groups. The Security Policy Administrator can add a group of users to an entitlement to authorize them to request access to the accounts and assets governed by the entitlement’s access request policies.

NOTE: User Groups is available to the Authorizer Administrator, User Administrator, Security Policy Administrator, and the Auditor. However, it is only available to the Authorizer Administrator and User Administrator if a directory has been added to Safeguard. For more information, see Adding a directory on page 188.

The User Groups view displays the following information about the selected user or directory group.

Table 238: User Groups: Tabs

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td>Displays general information about the selected user group.</td>
</tr>
<tr>
<td>Users tab</td>
<td>Displays the members of the selected group.</td>
</tr>
<tr>
<td>Entitlements tab</td>
<td>Displays the entitlements to which the users associated with the selected user group are &quot;users&quot;.</td>
</tr>
<tr>
<td>History tab</td>
<td>Displays the details of each operation that has affected the selected group.</td>
</tr>
</tbody>
</table>

Use these toolbar buttons to manage users.

Table 239: User Groups: Toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Add User Groups</td>
<td>Add user groups to Safeguard. For more information, see Adding a user group on page 396.</td>
</tr>
<tr>
<td>- Delete Selected</td>
<td>Remove the selected user group. For more information, see Deleting a user group on page 399.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the list of user groups.</td>
</tr>
</tbody>
</table>
Related Topics

- Modifying a user group
- Adding users or user groups to an entitlement
- Adding a directory user group

General tab

The General tab lists information about the selected user group.

Large tiles at the top of the tab display the number of Users in the selected group and, when applicable, the number of Entitlements to which the selected group is an entitlement member or "user". Clicking a tile heading opens the corresponding tab.

**NOTE:** The Entitlements tile is only visible to the Auditor and Security Policy Administrator.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The group name.</td>
</tr>
</tbody>
</table>

Description: Information about the selected group.

Related Topics

- Modifying a user group

Users tab

The Users tab displays the members of the selected group.

Click (or tap) + Add User from the details toolbar to add one or more users to the selected local user group.

**NOTE:** For directory groups, group membership is read-only. That is, you cannot add or remove users from a directory group using the Users tab.
**Table 241: User Groups: Users tab properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The user's display name.</td>
</tr>
<tr>
<td>Name</td>
<td>The user's first and last name, if the information exists in the user's properties; otherwise, the user's display name.</td>
</tr>
<tr>
<td>Provider</td>
<td>The name of the authentication provider: <strong>Local, Certificate</strong>, or the name of an external provider such as a Microsoft Active Directory domain name.</td>
</tr>
<tr>
<td>Distinguished Name</td>
<td>The distinguished name of the user.</td>
</tr>
</tbody>
</table>

Use these buttons on the details toolbar to manage the users in your user groups.

**Table 242: User Groups: Users tab toolbar**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✚ Add User</td>
<td>Add one or more users to the selected user group. For more information, see Adding users to a user group on page 397.</td>
</tr>
<tr>
<td>✖ Remove Selected</td>
<td>Remove the selected user from the user group.</td>
</tr>
<tr>
<td>☰ Refresh</td>
<td>Update the list of users in the user groups.</td>
</tr>
<tr>
<td>☰ Details</td>
<td>View additional details about the selected user.</td>
</tr>
<tr>
<td>🔍 Search</td>
<td>To locate a specific user or set of users in this list, enter the character string to be used to search for a match. For more information, see Search box on page 65.</td>
</tr>
</tbody>
</table>

**Related Topics**

Adding users to a user group
Modifying a user group

**Entitlements tab**

The **Entitlements** tab displays the entitlements to which the users associated with the selected user group are "users".

![NOTE:](https://example.com) The Entitlements tab is only available to a user with Auditor or Security Policy Administrator permissions.

Click (or tap) ✚ Add Entitlement to add the selected user group as a "user" of one or more entitlements.
Table 243: User Groups: Entitlements tab properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name assigned to the entitlement.</td>
</tr>
<tr>
<td>Accounts</td>
<td>The number of unique accounts in this entitlement.</td>
</tr>
<tr>
<td>Users</td>
<td>The number of unique users and user groups in this entitlement.</td>
</tr>
<tr>
<td>Access Request Policies</td>
<td>The number of unique policies in this entitlement.</td>
</tr>
</tbody>
</table>

Use these buttons on the details toolbar to manage the entitlements associated with the selected user group.

Table 244: User Groups: Entitlements tab toolbar

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Add Entitlement</td>
<td>Add the selected user group to one or more entitlements. For more information, see Adding a user group to an entitlement on page 398.</td>
</tr>
<tr>
<td>− Remove Selected</td>
<td>Remove the user group from the selected entitlement.</td>
</tr>
<tr>
<td>☀ Refresh</td>
<td>Update the list of entitlements.</td>
</tr>
<tr>
<td>☰ Details</td>
<td>View additional details about the selected entitlement.</td>
</tr>
<tr>
<td>☐ Search</td>
<td>To locate a specific entitlement or set of entitlements in this list, enter the character string to be used to search for a match. For more information, see Search box on page 65.</td>
</tr>
</tbody>
</table>

Related Topics
Adding a user group to an entitlement
Modifying a user group

History tab

The History tab allows you to view or export the details of each operation that has affected the selected group.

The History tab contains the following information:

- **Items**: Total number of entries in the history log.
- **Search**: For more information, see Search box on page 65.
**Time Frame**: By default the history details are displayed for the last 24 hours. Click (or tap) one of the time intervals at the top of the grid to display history details for a different time frame. If the display does not refresh after selecting a different time interval, click (or tap) **Refresh**.

**Table 245: User Groups: History tab properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>The date and time of the event.</td>
</tr>
<tr>
<td>User</td>
<td>The display name of the user that triggered the event.</td>
</tr>
<tr>
<td>Source IP</td>
<td>The network DNS name or IP address of the managed system that triggered the event.</td>
</tr>
<tr>
<td>Object Name</td>
<td>The name of the selected group.</td>
</tr>
<tr>
<td>Event</td>
<td>The type of operation made to the selected user group:</td>
</tr>
<tr>
<td></td>
<td>• Create</td>
</tr>
<tr>
<td></td>
<td>• Delete</td>
</tr>
<tr>
<td></td>
<td>• Update</td>
</tr>
<tr>
<td></td>
<td>• Add Membership</td>
</tr>
<tr>
<td></td>
<td>• Remove Membership</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: A membership operation indicates a &quot;relationship&quot; change with a related or parent object such as a user was added or removed from the membership of the selected user group or the selected group was added or removed from an entitlement.</td>
</tr>
<tr>
<td>Related Object</td>
<td>The name of the related object.</td>
</tr>
<tr>
<td>Related Object Type</td>
<td>The type of the related object.</td>
</tr>
<tr>
<td>Parent</td>
<td>The name of the object to which the selected user group is a child.</td>
</tr>
<tr>
<td>Parent Object Type</td>
<td>The parent object type.</td>
</tr>
</tbody>
</table>

Select an event to display this additional information for some types of events (for example, create and update events).

**Table 246: Additional History tab properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>The property that was updated.</td>
</tr>
<tr>
<td>Old Value</td>
<td>The value of the property before it was updated.</td>
</tr>
<tr>
<td>New Value</td>
<td>The new value of the property.</td>
</tr>
</tbody>
</table>
Management user groups

Use the controls and tabbed pages on the User Groups page to perform the following tasks to manage Safeguard user groups:

- Adding a user group
- Adding a directory user group
- Adding users to a user group
- Adding a user group to an entitlement
- Modifying a user group
- Deleting a user group

Adding a user group

It is the responsibility of the Security Policy Administrator to add groups of local users to Safeguard.

NOTE: It is the responsibility of the Authorizer Administrator or the User Administrator to add directory groups. For more information, see Adding a directory user group on page 396.

To add a user group

1. Navigate to Administrative Tools | User Groups.
2. Click (or tap) + Add User Groups from the toolbar.
3. In the User Groups dialog, enter the following information:
   a. Name: Enter a unique name for the user group.
      Limit: 50 characters
   b. Description: (Optional) Enter information about this user group.
      Limit: 255 characters

Related Topics

Adding users to a user group

Adding a directory user group

It is the responsibility of the Authorizer Administrator or the User Administrator to add directory groups to Safeguard. However, a Directory Administrator must first add a directory to Safeguard before an administrator has the ability to add directory groups.
NOTE: It is the responsibility of the Security Policy Administrator to add local user groups. For more information, see Adding a user group on page 396.

IMPORTANT: Safeguard must be able to communicate with the global catalog for directory management tasks including the addition of a directory account, a directory user account, or a directory user group. Standard global catalog ports are 3268 (LDAP) and 3269 (LDAPS).

To add a directory user group

1. Navigate to Administrative Tools | User Groups.
2. Click (or tap) + Add Directory Group from the toolbar.
3. In the Directory Group dialog, select a directory.
4. Browse to select a container within the directory as the Filter Search Location.
5. The Include objects from sub containers check box is selected by default indicating that child objects will be included in your search. Clear this check box to exclude child objects from your search.
6. In the Contains field, enter a full or partial directory group name and click (or tap) Search.
   To search for a directory group, you must enter text into the search box. Safeguard searches the entire forest root using the global catalog. You can search on partial strings. For example, if you enter "ad" in the search box, it will find any directory group that contains "ad".

   NOTE: The text search is not case sensitive and does not allow wild cards.
7. The results of the search displays in the Select the group to add grid. Select a group name and click (or tap) OK, or double-click (or double-tap) a name to add a directory group.

NOTE: Because Microsoft Active Directory does not have a Time Zone attribute, when you add a directory group, Safeguard sets the default time zone for all imported accounts to (UTC) Coordinated Universal Time. To reset the time zone, open each imported account in Users and modify the Time Zone on the Location tab.

Adding users to a user group

It is the responsibility of the Security Policy Administrator to add both local or directory users to local user groups.

NOTE: Directory group membership is maintained in the directory, such as Active Directory.
To add users to a user group

1. Navigate to Administrative Tools | User Groups.
2. In User Groups, select a user group from the object list and open the Users tab.
3. Click (or tap) + Add User from the details toolbar.
4. Select one or more users from the list in the Users selection dialog and click (or tap) OK.

   NOTE: You can also double-click (or double-tap) a user name to add it.

   IMPORTANT: You cannot add a group to a user group’s membership; group membership cannot be nested.

If you do not see the user you are looking for, depending on your Administrator permissions, you can create it in the Users selection dialog. (You must have Authorizer Administrator or User Administrator permissions to create users.)

To create a new user in the Users selection dialog

1. Click (or tap) + Create New.

   For more information, see Adding a user on page 375.
2. Create additional users, as required.
3. Click (or tap) OK in the Users selection dialog to add the users to the user group.

Adding a user group to an entitlement

When you add user groups to an entitlement, you are specifying which people can request access to the accounts and assets governed by an entitlement’s policies.

   NOTE: It is the responsibility of the Security Policy Administrator to add user groups to entitlements.

To add a user group to entitlements

1. Navigate to Administrative Tools | User Groups.
2. In User Groups, select a user group from the object list and open the Entitlements tab.
3. Click (or tap) + Add Entitlement from the details toolbar.
4. Select one or more entitlements from the Entitlements selection dialog and click (or tap) OK.

   NOTE: You can also double-click (or double-tap) an entitlement name to add it.

If you do not see the entitlement you are looking for, depending on your Administrator permissions, you can create it in the Entitlements selection dialog. (You must have Security Policy Administrator permissions to create entitlements.)
To create a new entitlement in the Entitlements selection dialog

1. Click (or tap) **Create New**.
   The Entitlement dialog appears. For more information about creating entitlements, see Adding an entitlement.
2. Create additional entitlements, as required.
3. Click (or tap) **OK** in the Entitlements selection dialog to add the selected user group to the entitlements.

Modifying a user group

Only the Security Policy Administrator can modify user groups.

To modify a user group

1. Navigate to Administrative Tools | User Groups.
2. In User Groups, select a user group.
3. Select the view of the user group's information you want to modify (General, Users, or Entitlements).
   **For example:**
   - To change a local user group's name or description, double-click (or double-tap) the General information box on the General tab or click (or tap) the Edit icon.
     **NOTE:** You can double-click (or double-tap) a user group name to open the General settings edit window.
   - To add (or remove) users to the selected local user group, switch to the Users tab.
     **NOTE:** You can multi-select members to add or remove more than one from a user group.
   - To add (or remove) the selected user group to an entitlement, switch to the Entitlements tab.
4. To view or Exporting data the details of each operation that has affected the selected user group, switch to the History tab.

Deleting a user group

It is the responsibility of the Security Policy Administrator to delete groups of local users from Safeguard. It is the responsibility of the Authorizer Administrator or the User Administrator to delete directory groups.
NOTE: When you delete a user group, Safeguard does not delete the users associated with it.

To delete a user group

1. Navigate to Administrative Tools | User Groups.
2. In User Groups, select a user group from the object list.
3. Click (or tap) Delete Selected.
4. Confirm your request.
Disaster recovery

To enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster, Safeguard provides a solution for disaster recovery scenarios by allowing you to configure a cluster of appliances.

A Safeguard cluster consists of two or more Safeguard appliances configured to communicate over TCP port 655. One appliance in the cluster is designated as the "primary". Non-primary appliances are referred to as "replicas".

All vital data stored on the primary appliance is also stored on the replicas. In the event of a disaster, where the primary appliance is no longer functioning, you can promote a replica to be the new primary appliance. This reduces downtime and data loss. While you can only have one primary, you can have up to four replicas. The replicas provide a read-only view of the security policy configuration; however, users can log into replicas to request access, generate reports or audit the data.

Enrolling and unjoining cluster members

Keep the following considerations in mind when performing the enroll replica and unjoin replica operations to create a Safeguard cluster.

Enroll cluster members

- Update all appliances to the same appliance build (patch) prior to building your cluster.
- In order to enroll an appliance into a cluster, appliances must be able to communicate over TCP port 655 and port 443. In addition, all members of a cluster must all have IPv4 or IPv6 network addresses. That is, if one appliance has only IPv4, all appliances in the cluster must have IPv4; same with IPv6. An appliance with only IPv4 cannot communicate with an appliance with only IPv6.
- Appliances can only belong to a single cluster.
You can only enroll replica appliances to a cluster when logged into the primary appliance (using an account with Appliance Administrator permissions).

You can only add one appliance at a time - the maintenance operation must be complete before adding additional replicas.

Enrolling a replica can take as little as 5 minutes or as long as 24 hours depending on the amount of data to be replicated and your network.

During an "enroll replica" operation, Safeguard puts the replica appliance in Maintenance mode and locks down the remaining appliances in the cluster. On the primary appliance, you will see an "enrolling" notice in the status bar of the cluster view, indicating that a cluster-wide operation is in progress. While a cluster-wide operation is occurring, all appliances in the cluster are locked down meaning that no modifications, password change or check requests, or access requests can be performed on any of the appliances in the cluster.

Once the maintenance operation (enroll replica operation) is complete, the diagram in the cluster view (left pane) shows the link latency on the connector. The appliances in the cluster are unlocked and users can once again use the features available in Safeguard.

TIP: The Activity Center contains events for the start and the completion of the enrollment process.

The primary appliance's objects and security policy configuration are replicated to all replica appliances in the cluster. If a replica has objects (such as users, assets, and so on) or security policy configuration defined, they will be replaced with the objects and configuration defined on the primary.

Some of the maintenance tasks available require that the cluster has consensus (that is, the majority of the remaining members are online and able to communicate). When half (or 50%) of your appliances in the cluster are online and able to communicate this is NOT the majority. Therefore, it is highly recommended that you create clusters with an odd number of appliances.

For detailed instructions, see Enrolling replicas into a cluster on page 403.

Unjoin cluster members

You can only unjoin replica appliances from a cluster.

To remove a primary appliance, you can failover to a replica making the replica the new primary and then unjoin the 'old' primary appliance. For more information, see Failing over to a replica by promoting it to be the new primary on page 406.

NOTE: If the cluster has consensus (that is, the majority of the remaining members are online and able to communicate), you can use the Failover option to promote a replica to be the new primary and then unjoin the 'old' primary appliance. However, if the cluster does not have consensus (that is, the majority of the remaining members are offline/unable to communicate), you must use the Cluster Reset option to rebuild your cluster. For more information, see Resetting a cluster that has lost consensus on page 412.
To perform an unjoin operation, the replica appliance to be unjoined can be in any state; however, the remaining appliances in the cluster must achieve consensus.

You can unjoin a replica appliance when logged into any appliance in the cluster that is online (using an account with Appliance Administrator permissions).

When you unjoin a replica appliance from a cluster, the appliance is removed from the cluster as a stand-alone appliance that retains all of the data and security policy configuration information it contained prior to being unjoined. After the replica is unjoined, the appliance is placed in a Read-Only mode. You can however activate the appliance so you can add, delete and modify data, apply access request workflow, and so on. For more information, see Activating a read-only appliance on page 407.

NOTE: When a replica is activated, it will start to manage the assets and accounts in its own configuration.

For detailed instructions, see Unjoining replicas from a cluster on page 404.

### Enrolling replicas into a cluster

Safeguard allows the Appliance Administrator to create a cluster of up to five appliances, one primary and four replicas.

Prior to enrolling cluster members into a Safeguard cluster, review the enrollment considerations; see Enrolling and unjoining cluster members

NOTE: It is highly recommended that you take a backup of your primary appliance before enrolling replicas to a cluster.

#### To enroll a replica

1. Log into the primary appliance as an Appliance Administrator.
2. In Administrative Tools, navigate to Settings | Cluster | Cluster Management.
3. Click (or tap) + Add Replica to join a Safeguard appliance to a cluster.
4. In the Add Replica dialog, enter a network DNS name or the IP address of the replica appliance into the Network Address field and click (or tap) Connect.
5. Safeguard connects to the replica and displays the login screen for the replica appliance.
   a. Enter a valid account with Appliance Administrator permissions.
   b. In the Add Replica confirmation dialog, enter the words Add Replica and click (or tap) OK to proceed with the operation.

Safeguard displays ⌛ (synchronizing icon) and ⌒ (lock icon) next to the appliance it is enrolling and puts the replica appliance in Maintenance mode while it is enrolling into the cluster.
On all of the appliances in the cluster, you will see an "enrolling" banner at the top of the cluster view, indicating that a cluster-wide operation is in progress and all appliances in the cluster are locked down.

Once the maintenance operation (enroll replica operation) is complete, the diagram in the cluster view (left pane) shows the link latency on the connector. The appliances in the cluster are unlocked and users can once again make access requests.

**NOTE:** Enrolling a replica can take up to 24 hours depending on the amount of data to be replicated and your network.

6. Log into the replica appliance as the Appliance Administrator.

Notice that the appliance has a state of Replica (meaning it is in a Read-Only mode); and contains the objects and security policy configuration defined on the primary appliance.

**NOTE:** You cannot add, delete or modify the objects or security policy configuration on a replica appliance; however, you can perform password change and check operations and make password release and session access requests. Network configuration is done on each unique appliance, whether it is the primary or a replica.

### Unjoining replicas from a cluster

Safeguard allows the Appliance Administrator to unjoin replica appliances from a cluster. Prior to unjoining a replica from a Safeguard cluster, review the unjoin considerations: See [Enrolling and unjoining cluster members](#).

**NOTE:** After a replica appliance is unjoined from a cluster, it remains in a Read-Only mode. See [Activating a read-only appliance](#) for instructions on how to bring this appliance back online.

**To unjoin a replica from a cluster**

1. Log into an appliance in the cluster, as an Appliance Administrator.
2. In **Administrative Tools**, navigate to **Settings | Cluster | Cluster Management**.
3. In the cluster view (left pane), select the replica node to be unjoined from the cluster.
4. In the details view (right pane), click (or tap) ⚡ Unjoin.
5. In the Unjoin confirmation dialog, enter the word **Unjoin** and click (or tap) **OK** to proceed.

   Safeguard displays ⌁ (synchronizing icon) and ⚐ (lock icon) next to the appliance it is unjoining and puts the replica appliance in Maintenance mode while it is unjoining from the cluster.
Once the operation has completed, the replica appliance no longer appears in the cluster view (left pane).

**NOTE:** If you log into the replica appliance using the desktop client while Safeguard is processing an unjoin operation, you will see the maintenance mode screen. At the end of the maintenance mode, you will see a **Restart Desktop Client** button indicating that the unjoin operation completed successfully.

### Maintaining and diagnosing cluster members

When a node is selected in the Cluster view (left pane) of the **Cluster** settings page, the appliance details and cluster health view (right pane) displays details about the selected appliance. From this pane you can run the following maintenance and diagnostic tasks against the selected appliance.

**Table 247: Cluster health toolbar buttons**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Unjoin](image) | Click (or tap) ![Unjoin](image) to remove a replica from the cluster. For more information, see [Unjoining replicas from a cluster](#) on page 404.  

**NOTE:** This option is only available for replica appliances. |

| ![Failover](image) | Click (or tap) ![Failover](image) to promote a replica to the primary appliance. For more information, see [Failing over to a replica by promoting it to be the new primary](#) on page 406.  

**NOTE:** This option is only available for replica appliances. |

| ![Activate](image) | Click (or tap) ![Activate](image) to activate a read-only appliance so it can add, modify and delete data. For more information, see [Activating a read-only appliance](#) on page 407.  

**CAUTION:** Activating this appliance will take it out of the read-only state and enable password check and change for managed accounts. Ensure that no other Safeguard appliance is actively monitoring these accounts, otherwise access to managed accounts could be lost. |
### Diagnose

Click (or tap) **Diagnose** to open the Diagnostics pane where you can perform the following:

- View appliance information. For more information, see [Appliance Information on page 251](#).
- Run diagnostic tests against the appliance. For more information, see [Diagnostics on page 254](#).
- Perform a factory reset. For more information, see [Factory Reset from the desktop client on page 258](#).
- View or edit networking settings. For more information, see [Networking on page 261](#).
- Generate a support bundle. For more information, see [Support Bundle on page 263](#).
- View or edit time settings. For more information, see [Time on page 264](#).

### Check Health

Click (or tap) **Check Health** to capture and display the current state of the selected appliance.

### Restart

Click (or tap) **Restart** to restart the selected appliance. Confirm your intentions by entering a **Reason** and clicking (or tapping) **Restart**.

To fix more serious issues with a cluster, you can perform additional operations depending on the state of the cluster members. Some such operations include:

- Patching cluster members
- Using a backup to restore a clustered appliance
- Performing a factory reset
- Resetting a cluster that has lost consensus

## Failing over to a replica by promoting it to be the new primary

Safeguard allows you to failover to a replica appliance by promoting it to be the new primary.
NOTE: You can promote a replica to be the new primary anytime the cluster has consensus (that is, the majority of the cluster nodes are online and able to communicate). If you have a quorum failure (that is, the majority of the cluster members do not achieve consensus), you must perform a cluster reset instead. For more information, see Resetting a cluster that has lost consensus on page 412.

To promote a replica to be the new primary in a cluster

1. Log into a healthy cluster member as an Appliance Administrator.
3. In the cluster view (left pane), select the replica node that is to become the new primary.
4. In the details view (right pane), click (or tap) Failover.
5. In the Failover confirmation dialog, enter the word Failover and click (or tap) OK to proceed.
   During the failover operation, all of the appliances in the cluster are placed in Maintenance mode.
   Once the failover operation completes, the selected replica appliance appears as the primary with a state of online. All other appliances (including the "old" primary) in the cluster appear as replicas with a state of online.

Activating a read-only appliance

Appliances that have been unjoined from a Safeguard cluster or restored from a backup remain in a Read-Only mode after they have been unjoined/restored. This procedure explains how to activate a read-only appliance so you can add, delete and modify data, apply access request workflow, and so on.

CAUTION: Activating this appliance will take it out of the read-only state and enable password check and change for managed accounts. Ensure that no other Safeguard appliance is actively monitoring these accounts, otherwise access to managed accounts could be lost.

NOTE: The read-only appliance must be online in order to use the Activate task. If it is offline or the cluster does not have consensus (that is, the majority of the remaining members are offline/unable to communicate), you must use the Cluster Reset option to rebuild your cluster. For more information, see Resetting a cluster that has lost consensus on page 412.

To activate a read-only appliance

1. Log into the read-only appliance as an Appliance Administrator.
2. In Administrative Tools, navigate to Settings | Cluster | Cluster Management.
The cluster view (left pane) displays one primary appliance with a yellow warning icon indicating the appliance is in a Read-Only mode.

3. In the cluster view (left pane), select the read-only node to be activated.
4. In the details view (right pane), click (or tap) **Activate**.
5. In the Activate confirmation dialog, enter the word **Activate** and click (or tap) **OK** to proceed.

The appliance’s node in the cluster view (left pane) no longer displays the yellow warning icon and the state is now **Online**.

**Diagnosing a cluster member**

The diagnostic tools are available to an Appliance Administrator or Operations Administrator for the currently connected appliance and any other appliances (replicas) in the cluster.

**To run diagnostics on a clustered appliance**

1. In **Settings**, select **Cluster | Cluster Management**.
2. From the cluster view (left pane), select the appliance to be diagnosed.
3. In the details pane (right pane), click (or tap) **Diagnose**.

   The Appliance Information view displays.
4. Select **Diagnostics** and choose the type of test to be performed.

<table>
<thead>
<tr>
<th>Test</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping</td>
<td>To verify your network connectivity and response time.</td>
</tr>
<tr>
<td>NS Lookup</td>
<td>To obtain your domain name or IP address.</td>
</tr>
<tr>
<td>Trace Route</td>
<td>To obtain your router information; trace route determines the paths packets take from one IP address to another.</td>
</tr>
<tr>
<td>Telnet</td>
<td>To access remote computers over TCP/IP networks like the Internet.</td>
</tr>
<tr>
<td>Show Routes</td>
<td>To retrieve routing table information.</td>
</tr>
</tbody>
</table>

5. Enter the requested information in the test dialog that displays.
Patching cluster members

When an appliance update is released, apply the patch so all appliances in the cluster are on the same version. See About cluster patching for more information on how Safeguard handles access requests and system failures during the cluster patching process.

Prior to installing an update patch to a cluster:

- Ensure all appliances in the cluster are online and healthy. Any warnings or problems should be addressed before cluster patching. The patch install process will fail if any of the cluster members are unhealthy or cannot be contacted.

  IMPORTANT: The primary appliance orchestrates the cluster upgrade; therefore, the primary appliance must stay online and have a solid network connection with all of the replica appliances in the cluster. If this cannot be reasonably assured, you should unjoin the replica appliances from the cluster, individually upgrade them, and then re-enroll them into cluster.

- It is highly recommended to take a backup of your primary appliance before applying a patch.

- You may want to unjoin a replica from the cluster to serve as a backup appliance. In case of a catastrophic failure, you can activate the unjoined replica to be the primary. If the cluster patching process is successful, upgrade the unjoined replica, and then re-enroll it back into the cluster.

To patch appliances in a cluster

IMPORTANT: The following procedure applies to Safeguard appliances running version 2.1.x and later. If you need to patch appliances running an earlier version, you will need to unjoin replica appliances, install the patch on each appliance, and then enroll the replica appliances to rebuild your cluster. For more information, see Patching cluster members in the One Identity Safeguard 2.0 Administration Guide.

1. Log into the primary appliance, as an Appliance Administrator.
2. In Administrative Tools, select Settings | Appliance | Updates.
3. Click (or tap) Upload a File and browse to select an update file.

   The patch will be uploaded and distributed to all of the appliances in the cluster.

   NOTE: If you make changes to the cluster, such as adding a new replica, while a patch is staged, the update file must be distributed to the new cluster member before the patch install process can begin. Safeguard will not allow the patch install process to begin until all of the cluster members report that they have the update file stored locally.
NOTE: Clicking the **Cancel** button during the distribution process stops the distribution of the update file to the replicas. At this point, you can click (or tap) one of the following buttons:

- **Remove** to remove the update file from all of the appliances in the cluster.
- **Distribute to Cluster** to continue distributing the update file to each replica in the cluster.

4. Once the file has been successfully distributed to all of the replicas in the cluster, click (or tap) the **Install Now** button.

The primary appliance will go into Maintenance mode to begin the update operation. Once the primary appliance is successfully updated, Safeguard will perform the update operation on each replica, one at a time. During an update operation, the cluster will be locked so that no other cluster operations can interfere with the update operation. Once the update operation is completed on all cluster members, the cluster will automatically unlock so normal operations can resume.

The **Cluster** view (**Settings | Cluster | Cluster Management**) shows that an update operation is in progress and the cluster members that are locked, awaiting to install the update file.

In addition, the **Updates** view (**Settings | Appliance | Updates**) shows the cluster members involved in the update operation and the progress as cluster members are successfully updated.

### About cluster patching

The following information provides some insight into how Safeguard processes access requests during the cluster patching process. It also describes what happens if a cluster member loses power or network connectivity during the patching process.

### Service guarantees:

During a cluster upgrade, the cluster is split logically into the current version (side A) and the upgrade version (side B). Access request workflow is only enabled on one side at a time. Audit logs run on both sides and merge when the cluster patch completes. Initially, access request workflow is only enabled on side A and replicas in PatchPending state can perform access requests. As appliances upgrade and move to side B, the access workflow migrates to side B when side B has a majority of the appliances. At this point in the upgrade process, replicas in PatchPending state can no longer perform access requests; however, all of the upgraded cluster members can perform access requests. There is a small window where access request workflow is unavailable as the data migrates from one side to the other.

### Failure scenarios:

If the primary appliance loses power or loses network connectivity during the upgrade process, it will try to resume the upgrade on restart.
If a replica is disconnected or loses power during an upgrade process, the replica will most likely go into quarantine mode. The primary appliance will skip that appliance and remove it from the cluster. This replica will need to be reset, upgraded, and then re-enrolled into the cluster manually to recover.

**Using a backup to restore a clustered appliance**

In a clustered environment, the objective of a cluster backup is to preserve and allow the restoration of all operational data, including access request workflow, users/accounts, audit logs and so on. All appliances in a cluster (primary and replicas) can be backed up. However, a backup should only be restored to an appliance in the worst-case scenario where no appliance can be restored using the failover operation.

When a backup is restored to an appliance, all of the cluster configuration data is purged. The appliance is restored as a stand-alone primary appliance in Read-Only mode with no replicas. However, all the access request workflow, user/account, and audit log data that existed when the backup was taken is retained. This primary appliance can then be activated and replicas can be joined to recreate a cluster.

**To take a backup of an appliance**

1. Log into the appliance as an Appliance Administrator.
2. In **Administrative Tools**, select **Settings | Backup and Restore**.
3. Click (or tap) **Run Now** to create a copy of the data currently on the primary appliance.
   - For more information, see [Run Now](#) on page 294.
   - Or you can click (or tap) **Backup Settings**, in the upper right corner of the Backups page, to configure an automatic backup schedule.
   - For more information, see [Safeguard Backup and Restore](#) on page 292.

**To restore an appliance from a backup**

1. Log into the appliance to be restored as an Appliance Administrator.
2. In **Administrative Tools**, select **Settings | Backup and Restore**.
3. Select the backup to be used and click (or tap) **Restore**.
   - **NOTE:** If you want to use a backup file taken on a different appliance, that backup file must first be downloaded on the appliance where the backup was taken. The downloaded backup file will then need to be uploaded to the appliance that wants to use it before you can use the **Restore** option.
4. In the **Restore** dialog, enter the word **Restore** and click (or tap) **OK**.
   
   For more information, see **Restore** on page 296.

   The appliance is restored as a stand-alone primary appliance in Read-Only mode with no replicas.

**To rebuild a cluster**

1. Log into the primary appliance as an Appliance Administrator.
2. Activate the Read-Only primary appliance.
   a. In **Administrative Tools**, navigate to **Settings | Cluster | Cluster Management**.
   b. Select the node to be activated from the cluster view (left pane).
   c. Click (or tap) **Activate**.
   d. Confirm the activate operation.

   For more information, see **Activating a read-only appliance** on page 407.
3. One at a time, enroll the replica appliances to rebuild your cluster.
   a. In **Administrative Tools**, select **Settings | Cluster**.
   b. Click (or tap) ✗ **Add Replica** to join a replica appliance to the cluster.

   Once the enroll operation completes, repeat to add your appliances back into the cluster as replicas.

   **NOTE:** Enrolling a replica can take up to 24 hours depending on the amount of data to be replicated and your network.

   For more information, see **Enrolling replicas into a cluster** on page 403.

### Resetting a cluster that has lost consensus

Resetting the cluster configuration allows you to recover a cluster that has lost consensus.

**CAUTION:** Resetting a cluster should be your last resort. It is recommended that you restore from a backup rather than reset a cluster.

A cluster has consensus when the majority of the nodes in the cluster are online and able to communicate. If a cluster loses consensus (also known as a quorum failure), the following automatically happens:

- The primary appliance goes into Read-Only mode.
- Password check and change is disabled.

If the cluster regains consensus automatically after connectivity is restored, the primary will return to Read-Write mode and password check and change will be re-enabled. However, if it does not regain consensus automatically, the Appliance Administrator must perform a cluster reset to force-remove nodes from the cluster.
IMPORTANT: Only reset the cluster if you are certain that consensus has been lost; otherwise, you could introduce a split-brain scenario. (Split-brain scenario is where a cluster gets divided into smaller clusters. Each of these smaller clusters believes it is the only active cluster and may then access the same data which could lead to data corruption.)

TIP: If you are concerned about network issues, reset the cluster with only the new primary appliance. Once the cluster reset operation is complete, enroll appliances one by one to create a new cluster.

To reset a cluster

1. In Settings, select Cluster.
2. Click (or tap) the Reset Cluster button.
   The Reset Cluster dialog displays listing the appliances (primary and replicas) in the cluster.
3. In the Reset Cluster dialog, select the nodes to be included in the reset operation and use the Set Primary button to designate the primary appliance in the cluster.
   NOTE: Nodes must have an Appliance State of Online or Online Read-Only and be able to communicate to be included in the reset operation. If you select a node that is not online or not available, you will get an error and the reset operation will fail.
4. Click (or tap) Reset Cluster.
5. In the confirmation dialog, enter the words Reset Cluster and click (or tap) OK.
   When connected to the new primary appliance, the Configuring Safeguard Appliance progress page displays showing the steps being performed as part of the maintenance task to reset the cluster.
6. Once the maintenance tasks have completed, click (or tap) Restart Desktop Client.

Once reset, the cluster only contains the appliances that were included in the reset operation.

Performing a factory reset

As an Appliance Administrator, you can use the Factory Reset feature to reset a Safeguard appliance to recover from major problems or to clear the data and configuration settings on the appliance.
**CAUTION:** Care should be taken when performing a factory reset against an appliance, because this operation removes all data and audit history, returning it to its original state when it first came from the factory. The appliance must go through configuration again as if it had just come from the factory. For more information, see Setting up One Identity Safeguard for the first time on page 37.

In addition, performing a factory reset may change the default SSL certificate and default SSH host key.

**IMPORTANT:** When performing a factory reset from the recovery kiosk, this is a challenge response operation, where Safeguard generates a challenge that is then sent to One Identity Support to get a response back. You must then copy and paste this challenge response into the kiosk screen in order to proceed. Please keep the following information in mind when performing a challenge response operation:

- A challenge response is only good for 24 hours.
- Do not navigate away from the kiosk or refresh the kiosk during a challenge response operation. Doing so will invalidate the challenge response.

**NOTE:** Clustered environment: Performing a factory reset on a clustered appliance will not automatically remove the appliance from a cluster. You will need to unjoin an appliance that has been factory reset from the cluster. The factory reset appliance must be configured again. For more information, see Setting up One Identity Safeguard for the first time on page 37.

A factory reset of an appliance may be initiated from the Appliance Information settings page in the desktop client, from the recovery kiosk or using the API.

**To perform a factory reset from the desktop client**

1. In Settings, select **Appliance | Factory Reset**.
2. Click (or tap) **Factory Reset**.
3. In the Factory Reset confirmation dialog, enter the words **Factory Reset** and click (or tap) **OK**.

The appliance will go into Maintenance mode to revert the appliance. Once completed, you will be prompted to restart the desktop client. If the appliance had been in a cluster, you may need to unjoin the factory reset appliance. The factory reset appliance must be configured again. For more information, see Setting up One Identity Safeguard for the first time on page 37. In addition, when you log into the appliance, you will be prompted to add your Safeguard licenses.

**To perform a factory reset from the recovery kiosk**

**NOTE:** You must contact One Identity Technical Support to perform a **Factory Reset** from the recovery kiosk.

1. From the recovery kiosk, select the **Factory Reset** option.
2. Right arrow.
3. At **id**, enter your identification and press the **Tab** key (or down arrow).

4. At **Get Challenge**, press the **Enter** key.
   Safeguard produces a challenge.

5. Copy and paste the challenge and send it to One Identity Support.

6. When you get the response from One Identity Support, copy and paste the response into the kiosk screen and select **Factory Reset**.

**Unlocking a locked cluster**

In order to maintain consistency and stability, only one cluster operation can run at a time. To ensure this, Safeguard locks the cluster while a cluster operation is running, such as enroll, unjoin, failover, patch, reset, and routine maintenance. The Cluster view shows that the cluster is locked and that any changes to the cluster configuration are not allowed until the operation completes. The banner that appears at the top of the screen explains the operation in progress and a red lock icon (🔒) next to an appliance indicates that the appliance is locking the cluster.

**To unlock a locked cluster**

1. Click (or tap) the 🔒 lock icon in the upper right corner of the warning banner.

2. In the Unlock Cluster confirmation dialog, enter **Unlock Cluster** and click (or tap) **OK**.
   This will release the cluster lock that was placed on all of the appliances in the cluster and terminate the operation.

**IMPORTANT:** Care should be taken when unlocking a locked cluster. It should only be used when you are sure that one or more appliances in the cluster are offline and will not finish the current operation. If you force the cluster unlock, you may cause instability on an appliance requiring a factory reset and possibly the need to rebuild the cluster. If you are unsure about the operation in progress, do NOT unlock the cluster. Most often, it will eventually time out and unlock on its own.

**Troubleshooting tips**

If there is a problem with a Safeguard cluster, follow these guidelines:

1. Ensure that the hardware is powered on and online.

2. Check for networking problems. For more information, see Diagnosing a cluster member on page 408.

3. Attempt to reboot the appliance.
4. Unjoin and re-enroll replica appliances. For more information, see Unjoining replicas from a cluster and Enrolling replicas into a cluster.

5. Restore from a backup and recreate your cluster. For more information, see Using a backup to restore a clustered appliance on page 411.

6. Perform a factory reset and recreate your cluster. For more information, see Performing a factory reset on page 413.

**TIP:** Please consider the following before contacting One Identity support for assistance:

- Check the events in the Activity Center as all cluster operations are logged.
- Errors and warnings may resolve on their own. If an error persists for more than 15 minutes it probably won't resolve itself. Try restarting the appliance to see if the error or warning clears.
- For connectivity errors/warnings, check for network disruptions. Ensure the appliances can ping one another. Ensure that ports 443 and 655 are not blocked between appliances.
- If an appliance goes into quarantine mode, connect to the recovery kiosk and contact support. For more information, see Recovery kiosk on page 462.
- If you are requesting assistance from One Identity support, generate a support bundle prior to contacting support. For more information, see Support Bundle on page 263.

### Appliance states

The following table lists the appliance states and what actions are available when the appliance is in a particular state.

<table>
<thead>
<tr>
<th>Appliance state and description</th>
<th>Actions available</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EnrollingReplica</strong></td>
<td></td>
</tr>
<tr>
<td>A transitional state where a replica appliance is being added to a cluster and is not available for access. From this state, the appliance goes into maintenance mode to complete the enroll operation.</td>
<td>Wait for operation to complete before logging into appliance.</td>
</tr>
</tbody>
</table>

**NOTE:** Only applies to replica appliances in a cluster.
<table>
<thead>
<tr>
<th>Appliance state and description</th>
<th>Actions available</th>
</tr>
</thead>
<tbody>
<tr>
<td>A transitional state where the appliance is initializing to start, but is not yet available for access.</td>
<td>Wait for operation to complete before logging into appliance.</td>
</tr>
<tr>
<td><strong>Maintenance</strong></td>
<td>Wait for maintenance tasks to complete before logging into appliance.</td>
</tr>
<tr>
<td>Appliance is performing maintenance tasks and is not available for access.</td>
<td></td>
</tr>
<tr>
<td><strong>LeavingCluster</strong></td>
<td>Wait for operation to complete before logging into appliance.</td>
</tr>
<tr>
<td>A transitional state where a replica appliance is being unjoined from a cluster and is not available for access. From this state, the appliance goes into maintenance mode to complete the unjoin operation.</td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> Only applies to replica appliances in a cluster.</td>
<td></td>
</tr>
<tr>
<td><strong>Offline</strong></td>
<td>Wait for appliance to come back online before logging in.</td>
</tr>
<tr>
<td>Appliance is not available for access.</td>
<td></td>
</tr>
<tr>
<td><strong>Online</strong></td>
<td>Log into appliance.</td>
</tr>
<tr>
<td>Appliance is online and available for access and the remaining nodes in the cluster have reached consensus.</td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> In this state, access request workflow is available from all clustered appliances that are online and able to communicate.</td>
<td></td>
</tr>
<tr>
<td><strong>PatchPending</strong></td>
<td>You can log into a replica with a PatchPending state.</td>
</tr>
<tr>
<td>A transitional state where a replica appliance is waiting to be upgraded. The primary appliance patches first, then instructs each replica to enter the PatchPending state. From this state, the appliance goes into maintenance mode to complete the upgrade operation.</td>
<td>You can initially perform access request workflow on a replica in PatchPending state; however, during the cluster upgrade, when the majority of the cluster members have upgraded, access request workflow migrates from the PatchPending side of the cluster to the upgraded side of the cluster. During this time, access request workflow is unavailable on any appliance still in the PatchPending state.</td>
</tr>
<tr>
<td><strong>PrimaryNoQuorum</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Appliance state and description</td>
<td>Actions available</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>The primary appliance is in a Read-Only mode while attempting to get the lease, but can't because the cluster does not have consensus. The appliance continues to attempt getting the lease and when it does, the appliance state goes back to Online.</td>
<td>If the appliance is powered on, you can log into an appliance with a PrimaryNoQuorum state; however, it will be in a Read-Only mode.</td>
</tr>
<tr>
<td><strong>NOTE</strong>: Only applies to the primary appliance in a cluster.</td>
<td><strong>NOTE</strong>: In this state, access request workflow is not available from the primary appliance, but may be available from other appliances in the cluster. For example, if the primary cannot communicate with the rest of the nodes in the cluster, but the rest of the nodes can communicate between themselves (ReplicaWithQuorum state), then access request workflow will be available from these replica appliances even though it is not available from the primary appliance.</td>
</tr>
</tbody>
</table>

**Quarantine**  
Appliance is broken or in an unknown state.  
Requires manual intervention to recover.  
Go to recovery kiosk to recover. For more information, see Recovery kiosk on page 462.

**ReplicaDisconnected**  
A replica appliance is available for access; however, both of the following conditions apply:  
- the replica appliance cannot communicate with the primary appliance in the cluster.  
- the remaining nodes in the cluster that the replica appliance can communicate with do not have consensus.  
**NOTE**: Applies to replica appliances in a cluster.  
You can log into a replica with a ReplicaDisconnected state, but access request workflow is disabled.  
**NOTE**: If the replica appliance cannot communicate with the other nodes in the cluster, but the remaining nodes can communicate with each other, then access request workflow will be available from those appliances even though it is not available from the appliance that cannot communicate with them.

**ReplicaNoQuorum**  
A replica appliance can communicate.  
You can log into a replica with a ReplicaNoQuorum state, but access request
### Appliance state and description

<table>
<thead>
<tr>
<th>Appliance state and description</th>
<th>Actions available</th>
</tr>
</thead>
<tbody>
<tr>
<td>With the primary appliance; however, the remaining nodes in the cluster do not reach consensus. Once the cluster regains consensus, the replica appliance will go into the Online state.</td>
<td>Workflow is disabled.</td>
</tr>
</tbody>
</table>

**NOTE:** Applies to replica appliances in a cluster.

### ReplicaWithQuorum

- A replica appliance cannot communicate with the primary appliance; however, the remaining nodes in the cluster have reached consensus.

**NOTE:** Applies to replica appliances in a cluster.

### TransitioningToPrimary

- A transitional state where a replica appliance is being promoted to be the new primary and is not available for access.

**NOTE:** Only applies to replica appliances in a cluster.

### TransitioningToReplica

- A transitional state where a primary appliance is being demoted to a replica and is not available for access.

**NOTE:** In this state, access request workflow is not available from the primary appliance, but may be available from other replicas. For example, in a cluster of five appliances, if the primary and a single replica cannot communicate with the remaining replicas in the cluster, but the other three replicas can communicate between themselves (ReplicaWithQuorum state), then access request workflow will be available from the replicas that are online and communicating even though it is not available from the primary and replica that cannot communicate.

**NOTE:** In this state, access request workflow is not available from the primary appliance, but may be available from other replicas. For example, in a cluster of five appliances, if the primary and a single replica cannot communicate with the remaining replicas in the cluster, but the other three replicas in the cluster can communicate between themselves (ReplicaWithQuorum state), then access request workflow will be available from the replicas that are online and communicating even though it is not available from the primary and replica that cannot communicate.

**NOTE:** In this state, access request workflow is not available from the primary appliance, but may be available from other replicas. For example, in a cluster of five appliances, if the primary and a single replica cannot communicate with the remaining replicas in the cluster, but the other three replicas in the cluster can communicate between themselves (ReplicaWithQuorum state), then access request workflow will be available from the replicas that are online and communicating even though it is not available from the primary and replica that cannot communicate.

**NOTE:** In this state, access request workflow is available from any clustered appliance that is online and able to communicate.

**NOTE:** In this state, access request workflow is available from any clustered appliance that is online and able to communicate.
<table>
<thead>
<tr>
<th>Appliance state and description</th>
<th>Actions available</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOTE:</strong> Only applies to the primary appliance in a cluster.</td>
<td></td>
</tr>
<tr>
<td><strong>ShuttingDown</strong>&lt;br&gt;A transitional state where an appliance is shutting down and is not available for access.</td>
<td>Wait for appliance to come back online before logging in.</td>
</tr>
<tr>
<td><strong>StandaloneReadOnly</strong>&lt;br&gt;State used for replicas removed from a cluster (unjoined and restored replicas). Appliance is online and available for access.</td>
<td>Log into appliance. See Activating a read-only appliance for how to activate a Read-Only appliance so you can add, delete and modify data, apply access request workflow, and so on.</td>
</tr>
<tr>
<td><strong>Unknown</strong>&lt;br&gt;Appliance is broken or in an unknown state.</td>
<td>Requires manual intervention to recover. Go to recovery kiosk to recover. For more information, see Recovery kiosk on page 462.</td>
</tr>
</tbody>
</table>
Administrator permissions

To secure control of your IT department’s assets (that is, “managed systems”), Safeguard uses a role-based access control hierarchy. Safeguard’s various permission sets restrict the amount of control each type of user has.

NOTE: It is the responsibility of a user with Authorizer Administrator permissions to grant administrator permissions to other Safeguard users; however, the User Administrator can grant Help Desk Administrator permissions to non-administrative users.

Administrator permissions include:

- Appliance administrator permissions
- Asset administrator permissions
- Auditor permissions
- Authorizer administrator permissions
- Directory administrator permissions
- Help Desk administrator permissions
- Operations administrator permissions
- Security Policy administrator permissions
- User administrator permissions

Appliance administrator permissions

The appliance administrator is responsible for configuring and maintaining the appliance, including the following tasks:

- Racks and stacks the appliance
- Configures the appliance.
- Troubleshoots performance, hardware, and networking.
- Creates and monitors the status of a clustered environment.
- Manages licenses, certificates, backups, and sessions settings.
- Enables and disables access request and password management services.

**Table 250: Appliance administrator: Permissions**

<table>
<thead>
<tr>
<th>Safeguard view/page</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Center</td>
<td>View and export appliance activity events.</td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>Toolbox</td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>Settings:</td>
</tr>
<tr>
<td>- Access Request</td>
<td>Enable or Disable Services</td>
</tr>
<tr>
<td>- Appliance</td>
<td>Monitor the status of the appliance.</td>
</tr>
<tr>
<td></td>
<td>Shutdown or restart the appliance.</td>
</tr>
<tr>
<td></td>
<td>Run diagnostics on the appliance.</td>
</tr>
<tr>
<td></td>
<td>Enable or disable Lights Out Management (BMC).</td>
</tr>
<tr>
<td></td>
<td>Configure networking settings.</td>
</tr>
<tr>
<td></td>
<td>Perform a factory reset to recover from major problems or clear the data and configuration settings on the appliance.</td>
</tr>
<tr>
<td></td>
<td>Generate a support bundle to assist technical support.</td>
</tr>
<tr>
<td></td>
<td>Manage appliance time.</td>
</tr>
<tr>
<td></td>
<td>Install update files (patches).</td>
</tr>
<tr>
<td>- Backup and Retention</td>
<td>Configure backup and retention settings, define archive servers, and manage backups.</td>
</tr>
<tr>
<td>- Certificates</td>
<td>Manage the certificates used by Safeguard.</td>
</tr>
<tr>
<td>- Cluster</td>
<td>Create and manage a clustered environment.</td>
</tr>
<tr>
<td></td>
<td>Monitor the status of the clustered environment.</td>
</tr>
<tr>
<td></td>
<td>Diagnose cluster members.</td>
</tr>
<tr>
<td>- External Integration</td>
<td>Configure Approval Anywhere service for access request approvals.</td>
</tr>
<tr>
<td></td>
<td>Configure Safeguard to send event notifications to external systems.</td>
</tr>
<tr>
<td></td>
<td>Configure external federation.</td>
</tr>
<tr>
<td></td>
<td>Configure secondary authentication service provider.</td>
</tr>
<tr>
<td></td>
<td>Configure Safeguard to send SNMP traps to the SNMP console.</td>
</tr>
</tbody>
</table>

Table 250: Appliance administrator: Permissions
Safeguard view/page | Permissions
----------------------|---------------------------------------------------------------
Join Safeguard to Starling.
Configure Safeguard to send event notifications to a syslog server.
Configure the integration with an external ticketing system.

- **Licensing**
  Add and manage Safeguard module licenses.

- **Messaging**
  Configure login notifications.
  Set message of the day.

- **Safeguard Access | Login Control**
  Configure the user login control settings.

- **Sessions**
  Configure session recording storage management.
  Configure the sessions module settings.
  Reset the sessions module.
  Generate or download an SSH host key.

### Asset administrator permissions

An asset administrator manages all partitions, assets, and accounts:

- Creates (or imports) local assets and accounts.
- Creates partitions and partition profiles.
- Delegates partition ownership to users.

  **NOTE:** A delegated partition owner has a subset of permissions that an Asset Administrator has. That is, the delegated partition owner is authorized to manage a specific partition and the assets and accounts assigned to that partition.

- Assigns assets to partitions.
- Manages account password rules.

  **NOTE:** Asset Administrators can only view the user object history for their own account.

### Table 251: Asset administrator: Permissions

<table>
<thead>
<tr>
<th>Safeguard view</th>
<th>page</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>Account</td>
<td>Full control for accounts related to all Safeguard</td>
</tr>
<tr>
<td>Safeguard view</td>
<td>page</td>
<td>Permissions</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Automation</td>
<td></td>
<td>assets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>![NOTE] Delegated partition owners have control for accounts related to the assets and directories managed through delegated partition profile.</td>
</tr>
<tr>
<td>Activity Center</td>
<td>View and export asset activity events.</td>
<td></td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>Accounts</td>
<td>Add, modify, delete and import accounts. Check, change, and set account passwords. Access password archive. Enable or disable the access request services for an account.</td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>Assets</td>
<td>Add, modify, delete and import assets. Configure and manage asset discovery jobs. Download SSH Key.</td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>Partitions</td>
<td>Add, modify and delete partitions and partition profiles. Set partition as default. Add assets to the scope of a partition profile.</td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>Settings</td>
<td>Add, modify and delete account discovery settings. Add, modify and delete account password complexity rules. Add, modify and delete change password settings. Add, modify and delete check password settings. Add, modify, and delete password sync groups.</td>
</tr>
</tbody>
</table>
Auditor permissions

The Auditor administrator has read-only access to all features, giving him the ability to review all access request activity:

- Monitors appliance information.
- Reviews everything.
- Exports object history.
- Runs entitlement reports.

<table>
<thead>
<tr>
<th>Auditor administrator: Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>**Safeguard view</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>**Safeguard Access</td>
</tr>
<tr>
<td>**Administrative Tools</td>
</tr>
</tbody>
</table>

### Table 252: Auditor administrator: Permissions

<table>
<thead>
<tr>
<th>Safeguard view</th>
<th>page</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>View only.</td>
<td></td>
</tr>
<tr>
<td>Activity Center</td>
<td>View and export activity events. Audit access request workflow.</td>
<td></td>
</tr>
<tr>
<td>Reports</td>
<td>View and export entitlement reports.</td>
<td></td>
</tr>
<tr>
<td>**Administrative Tools</td>
<td>Toolbox**</td>
<td>Access to all Administrative Tools views and the Tasks pane.</td>
</tr>
<tr>
<td>**Administrative Tools</td>
<td>Accounts**</td>
<td>View only.</td>
</tr>
<tr>
<td>**Administrative Tools</td>
<td>Account Groups**</td>
<td>View only.</td>
</tr>
<tr>
<td>**Administrative Tools</td>
<td>Assets**</td>
<td>View asset discovery jobs.</td>
</tr>
<tr>
<td>**Administrative Tools</td>
<td>Asset Groups**</td>
<td>View only.</td>
</tr>
<tr>
<td>**Administrative Tools</td>
<td>Directories**</td>
<td>View only.</td>
</tr>
<tr>
<td>**Administrative Tools</td>
<td>Entitlements**</td>
<td>View only.</td>
</tr>
<tr>
<td>**Administrative Tools</td>
<td>Partitions**</td>
<td>View only.</td>
</tr>
<tr>
<td>Safeguard view</td>
<td>page</td>
<td>Permissions</td>
</tr>
<tr>
<td>----------------</td>
<td>---------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>Settings:</td>
<td></td>
</tr>
<tr>
<td>• Access Request</td>
<td>View only.</td>
<td></td>
</tr>
<tr>
<td>• Appliance</td>
<td>View Appliance Information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Run diagnostics on appliance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View licensing information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View Lights Out Management (BMC) settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View Networking settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View Time settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View update history.</td>
<td></td>
</tr>
<tr>
<td>• Backup and Retention</td>
<td>View only.</td>
<td></td>
</tr>
<tr>
<td>• Certificates</td>
<td>View only.</td>
<td></td>
</tr>
<tr>
<td>• Cluster</td>
<td>View only.</td>
<td></td>
</tr>
<tr>
<td>• Asset Management</td>
<td>View only.</td>
<td></td>
</tr>
<tr>
<td>• External Integration</td>
<td>View only.</td>
<td></td>
</tr>
<tr>
<td>• Messaging</td>
<td>Login notification: View only.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set message of the day.</td>
<td></td>
</tr>
<tr>
<td>• Profile</td>
<td>View only.</td>
<td></td>
</tr>
<tr>
<td>• Safeguard Access</td>
<td>View only.</td>
<td></td>
</tr>
<tr>
<td>• Sessions</td>
<td>View only.</td>
<td></td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>Users</td>
<td>View only.</td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>User Groups</td>
<td>View only.</td>
</tr>
</tbody>
</table>

**Authorizer administrator permissions**

The "permissions" administrator:

- Creates (or imports) Safeguard users.
- Adds directory groups, including the associated directory users, if a directory has been added to Safeguard.
- Grants administrator permissions to users.
• Sets passwords, unlocks, and enables or disables both local and directory user accounts.
• Creates and maintains the Password Rules.

**NOTE:** Also has User Administrator and Help Desk Administrator permissions.

**IMPORTANT:** Authorizer Administrators can change the permissions for their own account which may affect their ability to grant permissions to other users. When you make changes to your own permissions, they take effect next time you log in.

<table>
<thead>
<tr>
<th><strong>Table 253: Authorizer administrator: Permissions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Safeguard view/page</strong></td>
</tr>
<tr>
<td><strong>Activity Center</strong></td>
</tr>
<tr>
<td>**Administrative Tools</td>
</tr>
<tr>
<td>**Administrative Tools</td>
</tr>
<tr>
<td>• **External Integration</td>
</tr>
<tr>
<td>• <strong>Messaging</strong></td>
</tr>
<tr>
<td>• **Safeguard Access</td>
</tr>
<tr>
<td>**Administrative Tools</td>
</tr>
</tbody>
</table>

**Directory administrator permissions**

The Directory administrator configures and manages directory integration and synchronization including adding directory accounts to make them available for password request policies. This administrator also manages the profiles that govern the password
validation and reset settings for the accounts assigned to each directory and which account password rule to use.

- Adds directories and their associated accounts.
- Creates directory profiles.
- Defines directory account password rules.
- Configures directory account password settings.

Table 254: Directory administrator: Permissions

<table>
<thead>
<tr>
<th>Safeguard view</th>
<th>Permissions</th>
</tr>
</thead>
</table>
| Dashboard | Full control for accounts related to the directories managed by Safeguard.  
<i>Note: Delegated partition owners have control for accounts related to the assets and directories managed through delegated partition profile.</i> |
| Activity Center | View and export directory activity events. |
| Administrative Tools | Access to the Directories view.  
Access to the Tasks pane. |
| Administrative Tools | Add, modify or delete directories.  
Add directory accounts to directories.  
Enable or disable access request services for directory accounts.  
Set directory account passwords.  
Access password archive.  
Define and maintain directory account discovery jobs.  
Add and maintain directory profiles. |

Administrative Tools | Settings:

- **Messaging**  
Login notification: View only.  
Set message of the day.
- **Profile | Directory Account Password Rules**  
Add, modify or delete directory account password rules.
- **Profile | Directory Change Password**  
Add, modify or delete directory change password settings.
- **Profile | Directory Check Password**  
Add, modify or delete directory check password settings.
Help Desk administrator permissions

A help desk administrator:

- Sets passwords for non-administrative user accounts.
- Unlocks accounts for all user accounts.

**NOTE:** Help Desk Administrators can only view the user object history for their own account.

### Table 255: Help Desk administrator: Permissions

<table>
<thead>
<tr>
<th>Safeguard view</th>
<th>page</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Center</td>
<td></td>
<td>View and export user activity events.</td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>Toolbox</td>
<td>Access to the Users view and the Tasks pane.</td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>Settings:</td>
<td></td>
</tr>
<tr>
<td>Messaging</td>
<td></td>
<td>Login notification: View only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set message of the day.</td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>Users</td>
<td>Set passwords and unlock accounts for non-administrator users.</td>
</tr>
</tbody>
</table>

Operations administrator permissions

The Operations administrator monitors the status of the appliance and can reboot the appliance.

**NOTE:** This user can be a non-interactive user; that is, an automated script or external monitoring system.
Table 256: Operations administrator: Permissions

<table>
<thead>
<tr>
<th>Safeguard view</th>
<th>page</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Center</td>
<td>View and export appliance activity events.</td>
<td></td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>Toolbox</td>
<td>Access to the Tasks pane.</td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>Settings:</td>
<td></td>
</tr>
<tr>
<td>• Access Request</td>
<td>Enable or Disable Services</td>
<td>View only.</td>
</tr>
<tr>
<td>• Appliance</td>
<td>Monitor status of the appliance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Shutdown or restart the appliance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Run diagnostics on the appliance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Generate a support bundle to assist technical support.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View licensing information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View Networking settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View Time settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View update history.</td>
<td></td>
</tr>
<tr>
<td>• Backup and Retention</td>
<td>Configure backup and retention settings, define archive servers, and manage backups.</td>
<td></td>
</tr>
<tr>
<td>• Certificates</td>
<td>View only.</td>
<td></td>
</tr>
<tr>
<td>• Cluster</td>
<td>View only - monitor the status of the clustered environment.</td>
<td></td>
</tr>
<tr>
<td>• External Integration</td>
<td>View only.</td>
<td></td>
</tr>
<tr>
<td>• Messaging</td>
<td>Login notification: View only.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set message of the day.</td>
<td></td>
</tr>
<tr>
<td>• Safeguard Access</td>
<td>Login Control</td>
<td>View only.</td>
</tr>
<tr>
<td>• Sessions</td>
<td>View only.</td>
<td></td>
</tr>
</tbody>
</table>

Security Policy administrator permissions

The Security Policy administrator configures the security policies that govern the access rights to accounts and assets, including the requirements for checking out passwords, such
as the maximum duration, if password reasons are required, if emergency access is allowed, and so forth.

This user configures time restrictions for entitlements and who can request, approve and review access requests.

- Creates account groups, asset groups and user groups.
- Creates entitlements.
- Configures access request policies.
- Adds users or user groups to entitlements to authorize those accounts to request passwords.

> NOTE: This user may not know any details about the assets.

> NOTE: Security Policy Administrators can only view the user object history for their own account.

**Table 257: Security Policy administrator: Permissions**

<table>
<thead>
<tr>
<th>Safeguard view</th>
<th>page</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>Access Requests</td>
<td>Full control to manage access requests.</td>
</tr>
<tr>
<td>Activity Center</td>
<td></td>
<td>View and export security-related activity events, including access request events.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Audit access request workflow.</td>
</tr>
<tr>
<td>Reports</td>
<td></td>
<td>View and export entitlement reports.</td>
</tr>
<tr>
<td>Administrative</td>
<td>Account Groups</td>
<td>Add, modify or delete account groups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Add accounts to account groups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assign policies to account groups.</td>
</tr>
<tr>
<td>Administrative</td>
<td>Asset Groups</td>
<td>Add, modify or delete asset groups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Add assets to asset groups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assign policies to asset groups.</td>
</tr>
<tr>
<td>Administrative</td>
<td>Entitlements</td>
<td>Add, modify or delete entitlements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Add users or user groups to entitlements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Define and maintain access request policies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assign policies to entitlements.</td>
</tr>
<tr>
<td>Safeguard view</td>
<td>Permissions</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>Access Request</td>
<td>Add, modify, or delete reason codes.</td>
<td></td>
</tr>
<tr>
<td>External Integration</td>
<td>Add, modify, or delete application registrations.</td>
<td></td>
</tr>
<tr>
<td>External Integration</td>
<td>Configure Approval Anywhere service for access request approvals.</td>
<td></td>
</tr>
<tr>
<td>Messaging</td>
<td>Login notification: View only. Set message of the day.</td>
<td></td>
</tr>
</tbody>
</table>

**Administrative Tools | Users**

- Add users to user groups.
- Add users to entitlements.
- Link directory accounts to a user.

**Administrative Tools | User Groups**

- Add, modify or delete local user groups.
- Add local or directory users to user groups.
- Assign entitlements to user groups.

## User administrator permissions

The user administrator:

- Creates (or imports) Safeguard users.
- Grants Help Desk Administrator permissions to users.
- Sets passwords, unlocks, and enables or disables non-administrator user accounts.
- Adds directory groups, including the associated directory users, if a directory has been added to Safeguard.

**NOTE:** Also has Help Desk Administrator permissions.

**NOTE:** User Administrators cannot modify administrator passwords, including their own.

**IMPORTANT:** User Administrators can change the permissions for their own account which may affect their ability to grant Help Desk Administrator permissions to other users. When you make changes to your own permissions, they take effect next time you log in.
Table 258: User administrator: Permissions

<table>
<thead>
<tr>
<th>Safeguard view</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Center</td>
<td>View and export user activity events.</td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>Settings:</td>
</tr>
<tr>
<td>• External Integration</td>
<td>View only.</td>
</tr>
<tr>
<td>Secondary Authentication</td>
<td></td>
</tr>
<tr>
<td>• Messaging</td>
<td>Message of the Day: Login notification: View only. Set message of the day.</td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>Users: Add, modify, delete or import local and directory users. Set passwords and unlock accounts for non-administrator users. Enable or disable non-administrative users. Set Help Desk Administrator permissions.</td>
</tr>
<tr>
<td>Administrative Tools</td>
<td>User Groups: Add or delete directory groups, if a directory has been added to Safeguard.</td>
</tr>
</tbody>
</table>
Preparing systems for management

Before you add systems to Safeguard (Adding an asset on page 136), you must ensure they are properly configured.

Generally, to prepare an asset for Safeguard:

1. Create a functional account (called a "service" account in Safeguard) on the asset and assign it a password.

   **NOTE:** To add an asset to Safeguard, it must have a service account. For more information, see About service accounts on page 140.

2. Grant the service account sufficient permissions.

3. Test the service account connectivity.

4. Configure the security protocol.

5. For platforms that support SSL server certificate validation, add the server’s signing authority certificate to the Trusted Certificates store in Safeguard. For more information, see Trusted Certificates on page 309.

The following topics can help you prepare your hosts for management by Safeguard:

- Prepare ACF - Mainframe systems
- Prepare Amazon Web Services platforms
- Prepare Cisco devices
- Prepare Dell iDRAC devices
- Prepare VMware ESXi hosts
- Prepare Facebook hosts
- Prepare Fortinet FortiOS devices
- Prepare F5 Big-IP devices
- Prepare HP iLO servers
- Prepare HP iLO MP (Management Processors)
- Prepare IBM i (AS/400) systems
- Prepare JunOS Juniper Networks systems
- Prepare MongoDB
Prepare MySQL servers
Prepare Oracle databases
Prepare PAN-OS (Palo Alto) networks
Prepare PostgreSQL
Prepare RACF - Mainframe systems
Prepare SAP HANA
Prepare SAP Netweaver Application Servers
Prepare Sybase (Adaptive Server Enterprise) servers
Prepare SonicOS devices
Prepare SonicWALL SMA or CMS appliances
Prepare SQL Servers
Prepare Top Secret - Mainframe systems
Prepare Unix-based systems
Prepare Windows systems

Safeguard supports a variety of platforms. For more information, see Supported platforms on page 31.

Prepare ACF - Mainframe systems

This applies to both ACF2 - Mainframe and ACF2 - Mainframe LDAP platforms.

To prepare IBM ACF-mainframe systems for Safeguard

1. Create a service account on the asset and assign it a password.
2. Grant the service account the privileges required to use the ALTERUSER command on other profiles.
3. If not already installed, install a Telnet server on the z/OS system. If required, secure Telnet with SSL.

   **NOTE:** Please refer to your IBM z/OS system documentation for details on installing and configuring the Telnet server (and SSL).

4. Test the Telnet server using a Windows-based 3270 emulator or on Linux, use the telnet-ssl or x3270 programs to test SSL and non-SSL connections to an z/OS system.
5. In Safeguard, create the asset and accounts for the z/OS system using password authentication.
About certificate support for the TELNET protocol

Safeguard automatically accepts any server certificate that the connection offers and does not verify the trust chain on the TELNET certificate. In addition, Safeguard does not support client certificate selection so if TELNET requires that the client present a certificate that is signed by a recognized authority, Safeguard cannot support that configuration.

Prepare Amazon Web Services platforms

Safeguard supports Amazon Web Services (AWS), a secure cloud services platform.

To prepare Amazon Web Services platforms for Safeguard

1. Configure an Identity and Access Management (IAM) user to use as a service account.
2. Assign the IAM service account to the AdministratorAccess security policy.
3. In Amazon, create an access key for the IAM service account.
   
   Amazon creates a pair of data items called a "Secret Key" and a public "Access Key ID", which you will need when you add the Amazon Web Services asset to Safeguard.

   NOTE: When adding an Amazon Web Services asset, the **Network Address** must contain the AWS Account ID or Alias.

Prepare Cisco devices

Safeguard supports both Cisco Private Internet eXchange (PIX) firewall security appliances and PIX Internetwork Operating System (IOS) routers and switches. Cisco PIX and Cisco IOS use the SSH protocol to connect to the Safeguard appliance. Safeguard supports both SSH version 1 and version 2.

To prepare a Cisco device for Safeguard

1. Create a service account on the asset and assign it a password.
2. Enable and configure the SSH server to allow the service account to log in remotely.
3. Configure the **Privilege Level Password** (that is, the system enable password). This password is required when adding the asset to Safeguard.

   NOTE: Safeguard manages accounts found in the startup configuration file, not in the running configuration file.

4. Add the Cisco device to Safeguard using password authentication.
Prepare Dell iDRAC devices

Safeguard supports the Dell Remote Access Controller that is integrated with Dell PowerEdge servers. Safeguard uses the SSH protocol to connect to iDRAC devices.

To prepare an iDRAC device for Safeguard

1. Use iDRAC to create a service account with administrator privileges and assign it a password.
   The service account must have login privileges and must be able to configure users.
2. Verify that SSH is enabled in the iDRAC Network settings.
3. In Safeguard, create the asset and accounts for the iDRAC device using password authentication.

Prepare VMware ESXi hosts

IMPORTANT: Safeguard can only manage local users on a VMware host.

To prepare a VMware ESXi host for Safeguard

1. Use an existing account or create a new account as the service account on the asset and assign it a password.
   The default administrator account is suitable.
2. Grant the service account the privileges required to set user passwords using the web management API.
3. When adding a VMware ESXi host to Safeguard:
   a. Specify the network address.
   b. Specify port 443 as the HTTPS port.

Prepare Facebook hosts

Safeguard can manage Facebook account passwords. Verify that a login code for the account is not required by Facebook.

To prepare a Facebook account for Safeguard

1. Log into your Facebook account.
2. In the upper right corner of the page, click the down arrow on the right of the Quick Help question mark.
3. Click (or tap) **Settings**.
4. In the upper left corner of the page, click (or tap) **Security and Login**.
5. Scroll to **Two-Factor Authentication, Authorized Logins**.
6. Click (or tap) **View**.

Facebook displays the list of devices where you do not have to use a login code. Verify that login code is not required to access the account. If you have no registered devices, you will see the following message: You do not have any registered devices.

For details about adding a Facebook account to Safeguard, see Adding a cloud platform account on page 104.

### Prepare Fortinet FortiOS devices

Safeguard supports Fortinet Internet appliances. Safeguard uses the SSH protocol to connect to Fortinet devices.

**To prepare a Fortinet FortiOS device for Safeguard**

1. Create the service account as a local user on the managed system and assign it a password.
2. Add the service account to the Fortinet Administrators group. This allows the service account to access the device with SSH to manage users.

   ! **IMPORTANT:** Safeguard can only manage passwords for users that are members of the Fortinet Administrators group.

3. Enable and configure the SSH server to allow the service account to log in remotely.
4. Add the Fortinet device to Safeguard using password authentication.

### Prepare F5 Big-IP devices

Safeguard supports F5 Big-IP devices. Safeguard uses the SSH protocol to connect to F5 Big-IP devices.

**To prepare an F5 Big-IP device for Safeguard**

1. Create the service account as a local user on the F5 Big-IP managed system and assign it a password. Assign that service account the Administrator Role on all partitions. This allows the service account to manage users.
2. Enable console access by setting "Terminal Access" to either "Advanced" or "tmsh", which will allow the service account to log in remotely via SSH.
3. Add the F5 Big-IP device to Safeguard using password or SSH key authentication.
Prepare HP iLO servers

In Safeguard the HP iLO operating system is an HP Integrated Lights-Out (iLO) HP ProLiant server. Safeguard connects to HP iLO systems using HTTPS on port 443.

To prepare an HP iLO server for Safeguard

1. Create a service account with the Administrate User Accounts privilege and assign it a password.
   The service account must have login privileges and must be able to configure users.
2. Verify that the Web Server SSL Port is set to 443.
3. In Safeguard, create the asset and accounts for the HP iLO server using password authentication.

Prepare HP iLO MP (Management Processors)

In Safeguard the HP iLO MP operating system is an HP Integrity Integrated Lights-Out (iLO) Management Processor. Safeguard connects to HP iLO MP systems using SSH.

To prepare an HP iLO Management Processor for Safeguard

1. Create a service account with the Administer User Accounts privilege and assign it a password.
2. Verify that SSH is enabled.
3. In Safeguard, create the asset and accounts for the HP iLO MP asset type using password authentication.

Prepare IBM i (AS/400) systems

To prepare IBM i systems for Safeguard

1. Create a service account on the asset and assign it a password.
2. Grant the service account the privileges required to use the chgusrprf command on other profiles.
3. If not already installed, install a Telnet server on the IBM iSeries (AS/400) system. If required, secure Telnet with SSL.
   NOTE: Please refer to your IBM iSeries (AS/400) system documentation for details on installing and configuring the Telnet server (and SSL).
4. Test the Telnet server using a Windows-based 3270 emulator or on Linux, use the telnet-ssl or x3270 programs to test SSL and non-SSL connections to an IBM iSeries system.

5. In Safeguard, create the asset and accounts for the IBM iSeries (AS/400) system using password authentication.

About certificate support for the TELNET protocol

Safeguard automatically accepts any server certificate that the connection offers and does not verify the trust chain on the TELNET certificate. In addition, Safeguard does not support client certificate selection so if TELNET requires that the client present a certificate that is signed by a recognized authority, Safeguard cannot support that configuration.

Prepare JunOS Juniper Networks systems

Safeguard uses the Juniper Networks JunOS operating system to manage Juniper Networks routers and switches. Safeguard connects to JunOS systems using SSH.

To prepare a Juniper Networks JunOS system for Safeguard

1. Create a service account that is a member of the super-user login class and assign it a password.
2. Verify that SSH is enabled.
3. In Safeguard, create the asset and accounts for the Juniper Networks JunOS asset type using password authentication.

Prepare MongoDB

Safeguard makes an SSL connection to MongoDB using a TCP port and Bind IP address defined in the mongodb.conf file. You must enter this port number when adding a MongoDB asset to Safeguard.

To configure MongoDB for Safeguard

1. Create a service account and assign it a password.

   **NOTE:** The service account must have permissions for remote connections and permissions to change passwords. Consult your MongoDB Security Guide for the appropriate settings for your organization.

2. Verify that you can log in with the service account.
3. In Safeguard, create the asset and accounts for the MongoDB asset type using
password authentication. You must specify the **Database instance name** and the **Port** used by the database instance.

![NOTE: When you create an account of Dialog User or Communication Data type, Safeguard allows you to set the account password or reset the password. Use the **Reset Password** option to reset the password for this account. If you use the **Set Password** option and enter the same password used in MongoDB, the password check in Safeguard will fail.]

---

**Prepare MySQL servers**

To prepare a MySQL server for Safeguard, refer to the documentation for your MySQL server for information about how to setup and secure encryption.

To enable SSL server certificate validation, add the server’s signing authority certificate to the Trusted Certificates store in Safeguard. For more information, see [Trusted Certificates](#) on page 309.

For more information about how Safeguard database servers use SSL, see [How do Safeguard database servers use SSL](#) on page 492.

---

**Prepare Oracle databases**

To prepare an Oracle database for Safeguard, refer to the documentation for your Oracle database for information about how to setup and secure encryption.

To enable SSL server certificate validation, when configuring the SSL-enabled service on the Oracle server, ensure that the following security setting is configured:

```
SSL_SERVER_CERT_DN="CN=<address>" , where <address> matches the Network Address of the asset in Safeguard.
```

---

**Prepare PAN-OS (Palo Alto) networks**

In Safeguard the PAN-OS operating system is used by Palo Alto Networks appliances. Safeguard connects to PAN-OS systems using SSH.

**To prepare a Palo Alto Networks system for Safeguard**

1. Create a service account that is a Device Administrator and assign it the Superuser role and a password.
2. Verify that SSH is enabled.
3. In Safeguard, create the asset and accounts for the Palo Alto Networks asset type using password authentication.

**Prepare PostgreSQL**

Safeguard makes an SSL connection to PostgreSQL using a TCP port defined in the `postgresql.conf` file. You must enter this port number when adding a PostgreSQL asset to Safeguard.

**To configure PostgreSQL for Safeguard**

1. Create a service account and assign it a password.
   
   **NOTE:** The service account must have permissions for remote connections and permissions to change passwords. Consult your PostgreSQL Security Guide for the appropriate settings for your organization.

2. Verify that you can log in with the service account.

3. In Safeguard, create the asset and accounts for the PostgreSQL asset type using password authentication. You must specify the **Database instance name** and the **Port** used by the database instance.

   **NOTE:** When you create an account of Dialog User or Communication Data type, Safeguard allows you to set the account password or reset the password. Use the **Reset Password** option to reset the password for this account. If you use the **Set Password** option and enter the same password used in PostgreSQL, the password check in Safeguard will fail.

**Prepare RACF - Mainframe systems**

This applies to both RACF - Mainframe and RACF - Mainframe LDAP platforms.

**To prepare IBM RACF-mainframe systems for Safeguard**

1. Create a service account on the asset and assign it a password.

2. Grant the service account the privileges required to use the ALTERUSER command on other profiles.

3. If not already installed, install a Telnet server on the z/OS system. If required, secure Telnet with SSL.

   **NOTE:** Please refer to your IBM z/OS system documentation for details on installing and configuring the Telnet server (and SSL).
4. Test the Telnet server using a Windows-based 3270 emulator or on Linux, use the telnet-ssl or x3270 programs to test SSL and non-SSL connections to an z/OS system.

5. In Safeguard, create the asset and accounts for the z/OS system using password authentication.

**About certificate support for the TELNET protocol**

Safeguard automatically accepts any server certificate that the connection offers and does not verify the trust chain on the TELNET certificate. In addition, Safeguard does not support client certificate selection so if TELNET requires that the client present a certificate that is signed by a recognized authority, Safeguard cannot support that configuration.

**Prepare SAP HANA**

Safeguard makes an SSL connection to SAP HANA using a TCP port between 30015 and 39915, depending on the SAP system number (also known as the "instance number").

**To configure SAP HANA for Safeguard**

1. Create a service account and assign it a password.
   
   **NOTE:** This service account must have permissions for remote connections and permissions to change passwords. Consult your SAP security guide for the appropriate settings for your organization.

2. Verify that you can log in with the service account.

   **NOTE:** In SAP, when you create a new account of Dialog User or Communication Data type, you will be prompted to set a new password.

3. In Safeguard, create the asset and accounts for the SAP asset type using password authentication. You must specify the **SAP Client ID** number as well as the **Port** used by the SAP instance.

   **NOTE:** When you create an account of Dialog User or Communication Data type, Safeguard allows you to set the account password or reset the password. Use the **Reset Password** option to reset the password for this account. If you use the **Set Password** option and enter the same password used in SAP, the password check in Safeguard will fail.
Prepare SAP Netweaver Application Servers

Safeguard makes an SSL connection to the SAP Application Server using a TCP port between 3300 and 3399, depending on the SAP system number (also known as the "instance number").

1. **NOTE:** You can have multiple instances of SAP running on a server, each using a different network port in the range 3300-3399. The last two digits of the port are called the system number (or instance number). Also, when you assign a password to the account, the account is not usable until you log in and change the password from the admin-assigned value.

2. **NOTE:** If a privileged user for the asset is of Dialog User or Communication Data type, assign RFC authorization for the RFCPING function module for that user. This allows the user to execute its functions remotely, such as changing the password.

**To configure a SAP Netweaver Application Server for Safeguard**

1. Create a service account and assign it a password.

   **NOTE:** This service account must have permissions for remote connections and permissions to change passwords. For example, S_A.SYSTEM or SAP_ALL authorization profiles will work, but may have more permissions than are necessary. Consult your SAP security guide for the appropriate settings for your organization.

2. Verify that you can log in with the service account.

   **NOTE:** In SAP, when you create a new account of Dialog User or Communication Data type, you will be prompted to set a new password.

3. In Safeguard, create the asset and accounts for the SAP asset type using password authentication. You must specify the SAP Client ID number as well as the Port used by the SAP instance.

   **NOTE:** When you create an account of Dialog User or Communication Data type, Safeguard allows you to set the account password or reset the password. Use the Reset Password option to reset the password for this account. If you use the Set Password option and enter the same password used in SAP, the password check in Safeguard will fail.
Prepare Sybase (Adaptive Server Enterprise) servers

To prepare a Sybase ASE (Adaptive Server Enterprise) server for Safeguard, refer to the documentation for your Sybase ASE server for information about how to setup and secure encryption.

To enable SSL server certificate validation, add the server’s signing authority certificate to the Trusted Certificates store in Safeguard. For more information, see Trusted Certificates on page 309.

For more information about how Safeguard database servers use SSL, see How do Safeguard database servers use SSL on page 492.

Prepare SonicOS devices

Safeguard supports SonicOS Internet appliances. Safeguard uses the SSH protocol to connect to SonicOS devices.

To prepare a SonicOS device for Safeguard

1. Create the service account as a local user on the managed system and assign it a password.
2. Add the service account to the SonicWALL Administrators group. This allows the service account to access the device with SSH to manage users.
   
   IMPORTANT: Safeguard can only manage passwords for users that are members of the SonicWALL Administrators group.

3. Enable and configure the SSH server to allow the service account to log in remotely.
4. Add the SonicOS device to Safeguard using password authentication.

Prepare SonicWALL SMA or CMS appliances

Here are some important notes about configuring a SonicWALL SMA or CMS appliance for Safeguard:

1. Use the local "admin" account as the service account.
2. Safeguard can only manage the admin account; it cannot manage other local accounts or accounts from external providers.
Prepare SQL Servers

To prepare a Microsoft SQL Server for Safeguard, refer to the documentation for your SQL server for information about how to setup and secure encryption.

To enable SSL server certificate validation, add the server’s signing authority certificate to the Trusted Certificates store in Safeguard. For more information, see Trusted Certificates on page 309.

For more information about how Safeguard database servers use SSL, see How do Safeguard database servers use SSL on page 492.

To configure a SQL Server for Safeguard (with an authentication type of Local System Account)

1. Log into the Safeguard desktop client as an Asset Administrator.
3. Add a Windows asset that matches the OS of the server that is hosting the SQL database.
   a. On the Connection tab,
      - **Authentication Type**: Set to Password.
      - **Service Account**: Set to a local user that is a member of the Administrator’s group.
   b. Add other accounts as needed.
   Save the asset.
4. Add a SQL Server asset.
   a. On the Connection tab,
      - **Authentication Type**: Set to Local System Account.
      - **Service Account**: Click (or tap) Select Account and select a local system account from the list.
        The accounts available for selection are Windows accounts that are linked to the Windows asset you added in Step 3.
      - Run **Test Connection** and verify the connection works.
   Save the asset.
To configure a SQL Server for Safeguard (with an authentication type of Directory Account)

**NOTE:** To manage a Microsoft SQL asset with the authentication type of Directory Account, you need a domain account that is a Security Admin in SQL. In order to use this authentication type, you must add a directory and directory users to Safeguard.

1. Add a directory and directory users.
   a. Log into the Safeguard desktop client as a Directory Administrator.
   b. Navigate to Administrative Tools | Directories to add a directory for your domain.
   c. Once added, select the domain and open the Accounts tab to add domain user accounts.

   For more information, see Directories on page 177.

2. Add a SQL Server asset.
   a. Log into the Safeguard desktop client as an Asset Administrator.
   b. Navigate to Administrative Tools | Assets to add a SQL Server asset.
   c. On the Connection tab,
      - **Authentication Type:** Set to Directory Account.
      - **Service Account:** Click (or tap) Select Account and select a domain user account from the list.
        The accounts available for selection are domain user accounts that are linked to the directory you added in Step 1.
      - **Run Test Connection** and verify the connection works.

Save the asset.

Prepare Top Secret - Mainframe systems

Safeguard can manage authorized Top Secret users who have a valid accessor ID (ACID) with the facility ‘TSO’ who can log on to the TSO interface.

This applies to both Top Secret - Mainframe and Top Secret - Mainframe LDAP platforms.

To prepare CA Top Secret mainframe systems for Safeguard

1. Create a service account on the asset, assign it a password, and grant it the ‘TSO’ facility.
2. Grant the service account the following authority for ACIDs within its scope:
   a. Permission to list security record information for an ACID.
   b. MISC1(SUSPEND) authority, to remove the PSUSPEND attribute from ACIDs.
   c. Either ACID(MAINTAIN) or MISC8(PWMAINT) authority, to update the password of another ACID.
3. If not already installed, install a Telnet server on the z/OS system. If required, secure Telnet with SSL.

   **NOTE:** Please refer to your IBM z/OS system documentation for details on installing and configuring the Telnet server (and SSL).
4. Test the Telnet server using a Windows-based 3270 emulator or on Linux, use the telnet-ssl or x3270 programs to test SSL and non-SSL connections to an z/OS system.
5. In Safeguard, create the asset and accounts for the z/OS system using password authentication.

**About certificate support for the TELNET protocol**

Safeguard automatically accepts any server certificate that the connection offers and does not verify the trust chain on the TELNET certificate. In addition, Safeguard does not support client certificate selection so if TELNET requires that the client present a certificate that is signed by a recognized authority, Safeguard cannot support that configuration.

**Prepare Unix-based systems**

Safeguard uses the SSH protocol to connect to Unix-based systems.

*To prepare Unix-based systems (AIX, HP-UX, Linux, Macintosh OS X, Solaris, and FreeBSD platforms)*

1. Create a service account on the asset with sufficient permissions.

   You need to at least configure a password for the service account. If you want to use an SSH key generated and configured by Safeguard, then you also need to make sure the service account’s home directory exists.

2. Ensure that the service account can run the following list of commands with root privileges non-interactively; that is, without prompting for a password.

   For example, on a Linux system add the following line in the sudoers file:
   
   ```
   <SerAcctName> ALL=(root) NOPASSWD: /usr/bin/passwd
   ```
   
   The commands a service account must run with root privileges non-interactively are:

   **Linux and most Unix-based systems:**
egrep
grep
passwd

**AIX:**
- sed
- passwd
- pwdadm

**Mac OS X**
- dscl
- passwd

3. Enable and configure the SSH server to allow the service account to log in remotely. For example, on a Mac, enable **Remote Login** for the service account.

**NOTE:** Different versions of Linux and Unix may require slightly different parameters for SSH configuration. Consult a Linux/Unix system administrator or the system documentation for assistance.

## Prepare Windows systems

**To prepare Windows systems for Safeguard**

1. Create a service account on the asset and assign it a password:
   - **Directory Configuration:**
     If the Windows system is joined to a domain that will be managed in Safeguard, you can use a directory account, such as a Microsoft Active Directory account to manage the asset. Enable the **Password Never Expires** option; once you add the asset to Safeguard, you can have the service account password auto-managed to keep it secure.

     - **OR** -

   - **Local Configuration:**
     If the Windows system is not joined to a domain, then use a local service account that has been granted sufficient permissions.
   
2. Grant the service account sufficient permissions to change account permissions to change account passwords. For more information, see **Minimum required permissions for Windows assets** on page 450.

3. Configure the system's firewall to allow the following predefined incoming rules:
   - Windows Management Instrumentation (DCOM-In)
   - NetLogon Service (NP-In)

   These rules allow incoming traffic on TCP port 135 and TCP SMB 445 respectively.
4. Ensure the following ports are accessible: 389, 636, and 3269. When possible, RPC ephemeral ports should also be accessible. For more information, see Service overview and network port requirements for Windows.

5. Change the local security policy:
Before Safeguard can reset local account passwords on Windows systems, using a service account that is a non-built-in administrator, you must change the local security policy to disable the User Account Control (UAC) Admin Approval Mode (“Run all administrators in Admin Approval Mode”) option. For more information, see Change password fails on page 455.

Minimum required permissions for Windows assets

The following minimum permissions are required for Windows assets to perform directory password management and sessions management tasks.

Asset password management
Using a Local account or Domain account:

- Test connection, Check connection, Password check, and Account discovery tasks require the following permissions:
  - Remote Enable permission on CIMV2 Namespace
  - Enable Account permission on CIMV2 Namespace
  - Remote Activation permission on computer
**NOTE:**

**To set Remote Enable and Enable Account permissions**
1. Open wmiimgmt.
2. Right-click **WMI Control (Local)** and select **Properties**.
3. Select the **Security** tab.
4. Add user and select **Remote Enable and Enable Account**.
5. Click **OK**.

**To set Remote Activation permissions**
1. Open dcomcnfg.
2. Expand **Component Services | Computers**.
3. Right-click **My Computer** and select **Properties**.
4. Open the **COM Security** tab.
5. Under **Launch and Activation Permissions**, select **Edit Limits**.
6. Add user and select **Allow for Remote Activation**.

- Password change task requires the following permission:
  - Member of Local Administrators group

**Domain password management**

Using a Domain account:

- Test connection, Check connection, Password check, and Account discovery tasks require the following permissions:
  - Member of Domain Users
- Password change task requires that the Service account has the following delegated permissions:
  - Reset Password
  - Read All Properties
  - Write All Properties

**Asset session access**

Using a Local account:

- Member of Remote Desktop Users group
- Defined in the "Allow log on through Remote Desktop Services" policy (directly or via group membership)
- Not defined in the "Deny log on through Remote Desktop Services" policy (directly or via group membership)

Using a Domain account:
- Defined in the Remote Desktop Users group or be a member of a domain security group by a group policy update to the Remote Desktop Users group for that asset
- Defined in the "Allow log on through Remote Desktop Services" policy (directly or via group membership)
- Not defined in the "Deny log on through Remote Desktop Services" policy (directly or via group membership)
Troubleshooting

One Identity recommends the following resolutions to some of the common problems you might encounter as you deploy and use Safeguard. For more information about how to troubleshoot Safeguard, refer to the Appliance settings.

- Anti Cross-Site Request Forgery token error
- Cannot connect to remote machine through SSH or RDP
- Cannot delete account
- Cannot play session message
- Connectivity failures
- Domain user denied access to Safeguard
- LCD status messages
- My Mac keychain password was lost
- Password fails for Unix host
- Password is pending review
- Profile did not run
- Recovery kiosk
- Replica not adding
- System services did not update or restart after password change
- Test Connection failures
- Timeout errors causing operations to fail
- User locked out
- User not notified

Related Topics

Frequently asked questions
Anti Cross-Site Request Forgery token error

If you receive an Anti Cross-Site Request Forgery token error when attempting to log into Safeguard using Microsoft Internet Explorer 9 on Windows 7 SP1, this indicates that cookies are blocked.

To resolve this issue

1. In Internet Explorer, open Tools and choose Internet Options.
2. In the Privacy tab, click the Advanced button.
3. Select the Always allow session cookies option.

Cannot connect to remote machine through SSH or RDP

If you are unable to connect to a remote machine either through SSH or RDP, log into the Safeguard desktop client as an Appliance Administrator and check the following:

- Check the Activity Center and logs for additional information.
- Ensure that the Network Interface X1 is configured correctly (Administrative Tools | Settings | Appliance | Networking).
- Ensure that you have installed the Privileged Sessions module license. (Administrative Tools | Settings | Appliance | Licensing).

Cannot delete account

Wrong Account name:

As an Asset administrator, if you attempt to delete an account and receive this error, "This entity has access requests which have not yet expired or have to be reviewed. It cannot be deleted now", this could indicate that Safeguard is trying to change the password on an account that does not exist on the asset.

One reason for this error message is that the wrong account name was used when adding the account to Safeguard. So now when someone requests the password for this account, Safeguard displays the password that was manually set. However, when the requester attempts to log into the asset using the "bad" account and password, it will fail. If the access request policy specified Change password after check-in, the above error message appears when the administrator tries to delete the account from Safeguard.
**Workaround**: To delete the account with the misspelled name, first manually set the password on the account. Once the account password is reset, Safeguard will allow you to delete the account.

**Cannot play session message**

If you receive a message that says "Cannot play session...The specified executable is not a valid application for this OS platform", you are most likely attempting to run the sessions player on a 32-bit platform, which is not supported.

**Connectivity failures**

The most common causes of failure in Safeguard are either connectivity issues between the appliance and the managed system, or problems with service accounts.

> **NOTE**: Always verify network connectivity and asset power before troubleshooting.

The following topics explain some possible reasons that Check Password, Change Password, and Set Password could fail and gives you some corrective steps you can take.

**Table 259: Causes for connectivity failures**

<table>
<thead>
<tr>
<th>Cause</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change password fails</td>
<td>Learn about a possible resolution if Change Password fails.</td>
</tr>
<tr>
<td>Incorrect authentication credentials</td>
<td>Learn how to resolve incorrect service account credentials.</td>
</tr>
<tr>
<td>Missing or incorrect SSH host key</td>
<td>Learn how to resolve issues with SSH host keys.</td>
</tr>
<tr>
<td>No cipher supported error</td>
<td>Learn how to resolve cipher support issues.</td>
</tr>
<tr>
<td>Service account has insufficient privileges</td>
<td>Learn how to resolve service account privilege issues.</td>
</tr>
</tbody>
</table>

**Change password fails**

A local account password change can fail when you are using a Windows asset that is configured with a service account with Administrative privileges, other than the built-in Administrator.
NOTE: Before Safeguard can change local account passwords on Windows systems, using a member of an administrators group other than built-in Administrator, you must change the local security policy to disable User Account Control (UAC) Admin Approval Mode ("Run all administrators in Admin Approval Mode") option.

To configure Windows assets to change account passwords

1. Run secpol.msc from the Run dialog,
   - OR-
   From the Windows Start menu, open Local Security Policy.
3. Disable the "User Account Control: Run all administrators in Admin Approval Mode" option.
4. Restart your computer.

For more information, see Prepare Windows systems on page 449.

Incorrect authentication credentials

You must have the correct user name and password to authenticate to an asset.

To resolve incorrect service account credentials

1. Verify the service account credentials match the credentials in Safeguard asset information (Administrative Tools | Assets | Connection). For more information, see About service accounts on page 140.
2. Perform Test Connection to verify connection. For more information, see About Test Connection on page 142.
3. Attempt to check, change, and set password again. For more information, see Checking, changing, or setting an account password on page 110.

Missing or incorrect SSH host key

If a Safeguard asset requires an SSH host Key and does not have one, Safeguard will not be able to communicate with the asset. For more information, see Certificate issue on page 470.

To resolve missing SSH host keys

To verify that an asset has an SSH host key, select the asset and look under Connection on the General view. If there is no SSH Host Key Fingerprint displayed, you need to add one.
To add an SSH host key

1. Open the asset’s Connection tab.
2. Choose any authentication type (except None) and enter required information.
   🔄 NOTE: You must enter the service account password again.
3. Click (or tap) Test Connection.
   Test Connection verifies that the appliance can communicate with the asset.
4. Confirm that you accept the SSH host key.
   🔄 NOTE: To bypass the SSH host key verification and automatically accept the key, click (or tap) the Auto Accept SSH Host Key option.
5. Click (or tap) OK to save asset.

To resolve incorrect SSH host keys

Safeguard uses the following host key algorithms for key exchange:
- DSA
- ECDSA
- RSA

To correct a mismatched SSH host key, run Test Connection.

No cipher supported error

If you receive an error message that says, "There is no cipher supported by both: client and server", refer to Cipher support on page 470.

Service account has insufficient privileges

If you are having service account issues, consider the following:
- Is the service account properly authorized to access the system? In a common setup, sudo is used to elevate the service account’s privileges on the system.
- Has the service account been locked out or disabled?
- Is the service account configured to allow remote logon?

A service account needs sufficient permissions to edit the passwords of other accounts. For more information, see About service accounts on page 140.
To resolve incorrect or insufficient service account privileges

1. Verify that the service account has sufficient permissions on the asset.
2. Perform Test Connection to verify connection.
3. Attempt to manually check, change, and set password again on the account that failed.

If the asset is running a Windows operating system, a local account password check, change, or set can fail when you are using an asset that is configured with a service account with Administrative privileges, other than the built-in Administrator.

Before Safeguard can change local account passwords on Windows systems, using a service account that is a non-built-in administrator, you must change the local security policy to disable the "Run all administrators in Admin Approval Mode" option. For more information, see Change password fails on page 455.

Domain user denied access to Safeguard

If you add a directory user who has the "User must change password at next logon" option enabled in Active Directory, Safeguard prevents that user from logging in. There are two ways to allow the directory user to log into Safeguard successfully:

- Have the directory user use his domain account to log in to an asset joined to Active Directory. When prompted he can change his password. This fulfills the "User must change password at next logon" requirement.
-OR-

- Have the domain administrator disable the option in Active Directory for the directory user.

LCD status messages

The One Identity Safeguard 2000 Appliance has an LCD screen which displays the status of the appliance as it is starting and as it progress through certain operations.

As it proceeds through its various stages, it displays the following messages.

NOTE: First boot setup refers to the initial configuration of Safeguard, which normally happens at the factory when the appliance is deployed and after a factory reset.
Table 260: LCD Status messages

<table>
<thead>
<tr>
<th>LCD status messages</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply Update xx%</td>
<td>Shows the percentage completed as the appliance progresses through an update operation.</td>
</tr>
<tr>
<td>Factory Reset xx%</td>
<td>Shows the percentage completed as the appliance progresses through a factory reset.</td>
</tr>
<tr>
<td>First boot ... &lt;version&gt;</td>
<td>Displayed after the first boot completes while it is waiting for Safeguard to load.</td>
</tr>
<tr>
<td>First Boot Setup xx%</td>
<td>Shows the percentage completed as the appliance is being configured for the first time.</td>
</tr>
<tr>
<td>Preparing for first boot setup</td>
<td>Displayed after a factory reset and before the appliance starts configured for the first time.</td>
</tr>
<tr>
<td>Quarantine</td>
<td>Indicates the appliance in a Quarantine state. For more information, see What do I do when an appliance goes into quarantine on page 496.</td>
</tr>
<tr>
<td>Starting core</td>
<td>Indicates that Safeguard is being loaded.</td>
</tr>
<tr>
<td>Starting database</td>
<td>Indicates that the Safeguard database is being loaded.</td>
</tr>
<tr>
<td>Starting reboot</td>
<td>Indicates the appliance is being rebooted.</td>
</tr>
<tr>
<td>Starting services</td>
<td>Indicates that Safeguard services are being loaded.</td>
</tr>
<tr>
<td>Starting shut down</td>
<td>Indicates the appliance is being shut down.</td>
</tr>
<tr>
<td>Starting web</td>
<td>Indicates that the web services are being loaded.</td>
</tr>
</tbody>
</table>

When the appliance is running, the LCD home screen displays:

- Safeguard <version number>

Appliance LCD and controls

The front panel of the One Identity Safeguard 2000 appliance contains the following controls for powering on, powering off, and scrolling through the LCD display.
Table 261: Appliance LCD and controls

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green check mark button</td>
<td>Use the Green check mark button to start the appliance. Press the Green check mark button for NO more than one second to power on the appliance.</td>
</tr>
<tr>
<td></td>
<td><strong>CAUTION:</strong> Once the Safeguard appliance is booted, DO NOT press and hold the Green check mark button. Holding this button for four or more seconds will cold reset the power of the appliance and may result in damage.</td>
</tr>
<tr>
<td>Red X button</td>
<td>Use the Red X button to shut down the appliance. Press and hold the Red X button for four seconds until the LCD displays POWER OFF.</td>
</tr>
<tr>
<td></td>
<td><strong>CAUTION:</strong> Once the Safeguard appliance is booted, DO NOT press and hold the Red X button for more than 13 seconds. This will hard power off the appliance and may result in damage.</td>
</tr>
<tr>
<td>Down, up, left and right arrow buttons</td>
<td>When the appliance is running, the LCD home screen displays:</td>
</tr>
<tr>
<td></td>
<td>• Safeguard &lt;version number&gt;</td>
</tr>
<tr>
<td></td>
<td>Use the arrow buttons to scroll through the following details:</td>
</tr>
<tr>
<td></td>
<td>• Serial: &lt;appliance serial number&gt;</td>
</tr>
<tr>
<td></td>
<td>• X0: &lt;appliance IP address&gt;</td>
</tr>
<tr>
<td></td>
<td>• X1: &lt;IP address of the session module interface&gt;</td>
</tr>
<tr>
<td></td>
<td>• MGMT: &lt;management IP address&gt;</td>
</tr>
<tr>
<td></td>
<td>• MGMT MAC: &lt;media access control address&gt;</td>
</tr>
<tr>
<td></td>
<td>• IPMI: &lt;IP address for IPMI&gt;</td>
</tr>
</tbody>
</table>

My Mac keychain password was lost

The keychain in Macintosh OS X is the Apple password management system. A keychain can store all your passwords for applications, servers, and websites, or even sensitive information unrelated to your computer, such as credit card numbers or personal identification numbers (PINs) for bank accounts.

If you have added a Mac OS X system to Safeguard, you might receive a message that says, "The system was unable to unlock your login keychain." That is because Safeguard automatically updates the account passwords on all managed systems based on the policies your Security Policy Administrator has configured, but it does not update the keychain password.
Password fails for Unix host

Some Unix systems silently truncate passwords to their maximum allowed length. For example, Macintosh OS X only allows a password of 128 characters. If an Asset Administrator creates a profile with an Account Password Rule that sets the password length to 136 characters, when Safeguard changes the password for an account governed by that profile, the asset’s operating system truncates the new password to the allowable length and does not return an error; however, the full 136-character password is stored in Safeguard. This causes the following issues:

- Check Password for that account will fail. When Safeguard compares the password on the Unix host with the password in Safeguard, they never match because the Unix host truncated the password generated by Safeguard.

- A user will not be able to log into the Unix host account successfully with the password provided by Safeguard unless he truncates the password to the allowable length imposed by the operating system.

Password is pending review

Safeguard can resolve a situation when a user needs to request an account password but cannot because there is a previous password release request still in the “Pending Review” state and the designated reviewer is not available. If the request is left in this state, Safeguard prevents users from checking out the account password. In such a situation, the Security Policy Administrator can close the request without review.

To close a password without review

1. Log in as a user with Security Policy Administrator permissions.
2. On the Home page, click (or tap) Refresh.
3. Open Administrator to review the pending request.
   
   NOTE: The Administrator control is only available in the Safeguard desktop client application, not in the web client.
4. Select Close Request.
5. Type an explanation in the Comment box of up to 255 characters (required).

You can query and view all requests closed without review in the Activity Center. Filter the events by Password Request Closed, then export the search results to see the old state and new state.
Related Topics
Password is pending a reset

Password is pending a reset

If a user receives a persistent message that states, "You cannot checkout the password for this account while another request is pending password reset" or "This account has password requests which have not yet expired or have to be reviewed. It cannot be deleted now", the account password is stuck in a pending password change state.

Ensure that the service account for the asset associated with this account is working. Then manually change the account password. For more information, see Checking, changing, or setting an account password on page 110.

Or, if the service account for the asset is working properly and the policy governing the account allows emergency access and has enabled multiple users simultaneous access, you can instruct the user to request the password using Emergency Access.

Related Topics
Password is pending review

Profile did not run

The password management settings Settings | Access Request | Enable or Disable Services enable the automatic profile check and change schedules in directories and partitions.

Ensure the password management settings are enable for profiles to run on schedule:
  - Check Password Management Enabled
  - Change Password Management Enabled

For more information, see Enable or Disable Services (Access request and password management services) on page 247.

Recovery kiosk

Safeguard provides a recovery kiosk with these options.
Table 262: Recovery Kiosk options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance information</td>
<td>Allows you to view basic appliance information.</td>
</tr>
<tr>
<td>Power options</td>
<td>These options allow you to remotely restart or shut down the appliance.</td>
</tr>
<tr>
<td>Admin password reset</td>
<td>Allows you to reset the bootstrap administrator’s password to its initial value.</td>
</tr>
<tr>
<td>Factory reset</td>
<td>Allows you to recover from major problems or to clear the data and configuration settings on the appliance.</td>
</tr>
</tbody>
</table>

⚠️ **CAUTION:** Care should be taken when performing a factory reset against an appliance, because this operation removes all data and audit history, returning it to its original state when it first came from the factory. The appliance must go through configuration again as if it had just come from the factory. For more information, see Setting up One Identity Safeguard for the first time on page 37.

In addition, performing a factory reset may change the default SSL certificate and default SSH host key.

Support bundle | Allows you to generate and send a support bundle to a Windows share.

**To start the recovery kiosk**

⚠️ **NOTE:** On the terminal or laptop running the recovery kiosk, you must configure your serial port settings as follows:

1. Connect a serial cable from a laptop or terminal to the serial port on the back of the appliance marked with **[010]**.
2. On the laptop or terminal, configure the serial port settings as follows:
   - Speed: 115200
   - Data bits: 8
   - Parity: None
   - Stop bit: 1
3. These options display on the recovery kiosk screen:
   - **Appliance Information**
   - **Power Options**
- Reboot
- Shut Down
- Admin Password Reset
- Factory Reset
- Support Bundle

4. Use the up-arrow and down-arrow to select one of these options.
5. Use the right-arrow to initiate the option.
6. Use the left-arrow to return to the option.

**Kiosk keyboard shortcuts**

Safeguard provides these keyboard shortcuts.

**Table 263: Kiosk keyboard shortcuts**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl + D</td>
<td>Resets the kiosk to its original state. Clears challenges and options.</td>
</tr>
<tr>
<td>Ctrl + R</td>
<td>Re-draws the kiosk to fit a resized window. If you resize the window, type Ctrl + R to reorganize the kiosk elements to fit properly into the newly-sized window.</td>
</tr>
</tbody>
</table>

⚠️ **CAUTION:** When resetting the bootstrap admin password or performing a factory reset, if you reset the kiosk before you receive the response from One Identity Support, you must submit a new challenge.

ℹ️ **NOTE:** If you make the window too small to accommodate the kiosk elements, Safeguard notifies you of how to readjust the window size.

**Appliance information**

Use the **Appliance Information** option on the recovery kiosk to view basic appliance information and edit the IP addresses.

**To view or edit the appliance information**

1. From the recovery kiosk, select the **Appliance Information** option.
2. Right-arrow to see:
Appliance State: The appliance's current state.

Uptime: The amount of time (hours and minutes) the appliance has been running.

MGMT: The management host's network interface properties, including the MAC address and IPv4 (and optionally IPv6) properties.

X0: The network interface properties for the primary interface that connects your appliance to the network, including the MAC address and IPv4 (and optionally IPv6) properties.

X1: The network interface properties used for the sessions module, including the MAC address and IPv4 (and optionally IPv6) properties.

3. To change the network properties for the primary interface (x0) or session interface (X1), click **Edit** next to the appropriate heading. Clicking **Edit** displays the network interface properties which can be modified.

4. After editing the network interface properties, click **Submit**.
   Once the updates are completed, a "Network interface update request accepted" message is displayed.

**Power options**

Use the power options in the recovery kiosk to remotely restart or shut down the appliance.

- You can use the **Reboot** option in the recovery kiosk to restart the appliance if you cannot access the SafeguardWindows desktop client, web client, or API to restart the appliance using the normal procedures.
- You must use the **Shut Down** option in the recovery kiosk to shutdown the appliance.

**Rebooting the appliance**

If you cannot access the Safeguard Windows desktop client, web client, or API to restart the appliance using the normal procedures, you can restart the appliance from the recovery kiosk.

**To reboot the appliance**

1. From the recovery kiosk, select the **Power Options | Reboot** option.
2. Right arrow.
3. When prompted, select **Yes** to start the reboot or **No** to return to the main option screen.
Shutting down the appliance

You must use the recovery kiosk to manually shutdown the Safeguard 2000 appliance.

To shut down the appliance

1. From the recovery kiosk, select the Power Options | Shut Down option.
2. Right arrow.
3. When prompted, select Yes to shut down the appliance or No to return to the main option screen.

Admin password reset

If your bootstrap administrator's password is locked out, you can reset it to the initial password.

**IMPORTANT:** This is a challenge response operation, where Safeguard generates a challenge that is then sent to One Identity Support to get a response back. You must then copy and paste this challenge response into the kiosk screen in order to proceed. Please keep the following information in mind when performing a challenge response operation:

- A challenge response is only good for 24 hours.
- Do not navigate away from the kiosk or refresh the kiosk during a challenge response operation. Doing so will invalidate the challenge response.

**NOTE:** If a user has not logged onto Safeguard for a set number of days, Safeguard disables the user account. This is set using the Disable After setting in Administrative Tools | Settings | Safeguard Access | Login Control.

To reset the bootstrap admin password

1. From the recovery kiosk, select the Admin Password Reset option.
2. Right arrow.
3. At id, enter your identification and press the Tab key (or down arrow).
4. At Get Challenge, press the Enter key.
   Safeguard produces a challenge.
5. Copy and paste the challenge and send it to One Identity Support.
6. When you get the response from One Identity Support, copy and paste the response into the kiosk screen and select Reset Password.

One Identity Support resets the bootstrap administrator's password back to Admin123.

**NOTE:** Best practice: To keep your Safeguard appliance secure, change the default password for the bootstrap administrator's account.
Factory reset

The **Factory Reset** option in the recovery kiosk allows you to reset a Safeguard appliance to recover from major problems or to clear the data and configuration settings on the appliance.

⚠️ **CAUTION:** Care should be taken when performing a factory reset against an appliance, because this operation removes all data and audit history, returning it to its original state when it first came from the factory. The appliance must go through configuration again as if it had just come from the factory. For more information, see [Setting up One Identity Safeguard for the first time on page 37](#).

In addition, performing a factory reset may change the default SSL certificate and default SSH host key.

ℹ️ **IMPORTANT:** This is a challenge response operation, where Safeguard generates a challenge that is then sent to One Identity Support to get a response back. You must then copy and paste this challenge response into the kiosk screen in order to proceed. Please keep the following information in mind when performing a challenge response operation:

- A challenge response is only good for 24 hours.
- Do not navigate away from the kiosk or refresh the kiosk during a challenge response operation. Doing so will invalidate the challenge response.

ℹ️ **NOTE:** **Clustered environment:** Performing a factory reset on a clustered appliance will not automatically remove the appliance from a cluster. You will need to unjoin an appliance that has been factory reset from the cluster. The factory reset appliance must be configured again. For more information, see [Setting up One Identity Safeguard for the first time on page 37](#).

To perform a factory reset from the recovery kiosk

ℹ️ **NOTE:** You must contact One Identity Technical Support to perform a **Factory Reset** from the recovery kiosk.

1. From the recovery kiosk, select the **Factory Reset** option.
2. Right arrow.
3. At **id**, enter your identification and press the **Tab** key (or down arrow).
4. At **Get Challenge**, press the **Enter** key.
   
   Safeguard produces a challenge.
5. Copy and paste the challenge and send it to One Identity Support.
6. When you get the response from One Identity Support, copy and paste the response into the kiosk screen and select **Factory Reset**.
Support bundle

NOTE: Prior to using the **Support Bundle** option on the recovery kiosk, set up a Windows share where the support bundle is to be sent.

**To generate a support bundle:**

1. From the recovery kiosk, select the **Support Bundle** option.
2. Right arrow.
3. Select the type of support bundle to be generated:
   - Support Bundle
   - Quarantine Bundle
4. When prompted, enter the following information:
   - Address: Enter the address of the Windows share (\<IP Address>\<ShareName>) where the support bundle is to be saved.
   - User: Enter the user name to be used to access the Windows share.
   - Password: Enter the password associated with the specified user account.
     
     NOTE: If you set up the Windows share to allow anonymous access, you will not be prompted to enter a user name or password.
5. Select **Submit**.
   When completed, a message appears stating that a support bundle has been sent to the specified share.

Replica not adding

If you receive a persistent message that says, "An internal request has timed out..." when you attempt to add an appliance to a cluster, ensure that the appliance is at the same version of Safeguard as the primary. All members of a cluster must be the same.

System services did not update or restart after password change

If the system services do not update or restart after an automatic password change, first check your audit logs in the **Activity Center**.

NOTE: You can also check the **Support Bundle** logs.
If the audit logs do not adequately explain the problem, then check the options on the **Change password** tab of the profile that governs the service account. For more information, see [Creating a partition profile](#) on page 239.

For service accounts that run system services or scheduled system tasks, verify the options on the profile's **Change password** tab that enable or disable automatic service update, or restart. You must update the Change Password Setting to change these options. For more information, see [Change Password](#) on page 344.

## Test Connection failures

**NOTE:** The most common causes of failure in Safeguard are either connectivity issues between the appliance and the managed system, or problems with service accounts. For more information, see [Connectivity failures](#) on page 455.

The following topics explain some possible reasons that **Test Connection** could fail.

**Table 264: Causes for Test Connection failures**

<table>
<thead>
<tr>
<th>Cause</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Connection failures on archive server</td>
<td>Learn how to resolve <strong>Test Connection</strong> failures for archive servers.</td>
</tr>
<tr>
<td>Certificate issue</td>
<td>Learn how to resolve <strong>Test Connection</strong> failures for assets that require SSL.</td>
</tr>
<tr>
<td>Cipher support</td>
<td>Learn about Safeguard's cipher support.</td>
</tr>
<tr>
<td>Domain controller issue</td>
<td>Learn how Safeguard manages passwords for accounts on domain controllers.</td>
</tr>
<tr>
<td>Networking issue</td>
<td>Learn how to resolve system connectivity issues.</td>
</tr>
<tr>
<td>Windows WMI connection</td>
<td>Learn how to enable Safeguard to manage Windows assets.</td>
</tr>
</tbody>
</table>

**NOTE:** Disabling User Account Control (UAC) Admin Approval Mode on a remote host can also resolve **Test Connection** failures. For more information, see [Change password fails](#) on page 455.

## Test Connection failures on archive server

There could multiple reasons why you receive an *Unexpected copying error...* when attempting to run **Test Connection** on an existing archive server.
When you run **Test Connection**, Safeguard adds a file named `Safeguard_Test_Connection.txt` to the **Storage Path** location of the archive server owned by the **Account Name** you entered when you created the archive server. To run **Test Connection** on an existing archive server with a new account name, you must first delete the existing `Safeguard_Test_Connection.txt` file.

**Certificate issue**

If you are experiencing **Test Connection** failures for an asset that uses SSL, these are some possible causes:

- The asset's signing authority certificate has not been added to the **Trusted Certificates** store in Safeguard.
- The signing authority's certificate has expired.
- There is a name mismatch between the name given and the name on the certificate of the asset. For more information, see [Missing or incorrect SSH host key](#) on page 456.

**Cipher support**

Both the Safeguard client and the SSH server must support the same cipher. If you run **Test Connection** against an asset that uses SSH and there is no cipher supported by both the client and the server, Safeguard displays an error message that says, "Connecting to asset XXXXXXXXXXXXXXXXX failed (There is no cipher supported by both: client and server)". This means that during the setup of the asset connection, the Safeguard client and the SSH server did not have matching ciphers for message encryption. In this case, you must modify the SSH server's configuration by adding at least one cipher supported by Safeguard to the list of ciphers.

Safeguard supports these ciphers.

**Table 265: Supported ciphers**

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Equivalent Cipher</th>
</tr>
</thead>
<tbody>
<tr>
<td>3des</td>
<td>idea</td>
</tr>
<tr>
<td>3des-ctr</td>
<td>idea-ctr</td>
</tr>
<tr>
<td>aes128</td>
<td>none</td>
</tr>
<tr>
<td>aes128-ctr</td>
<td>serpent128</td>
</tr>
<tr>
<td>aes192</td>
<td>serpent128-ctr</td>
</tr>
<tr>
<td>aes192-ctr</td>
<td>serpent192</td>
</tr>
<tr>
<td>aes256</td>
<td>serpent192-ctr</td>
</tr>
<tr>
<td>Cipher</td>
<td>Cipher</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>aes256-ctr</td>
<td>serpent256</td>
</tr>
<tr>
<td>arcfour</td>
<td>serpent256-ctr</td>
</tr>
<tr>
<td>arcfour128</td>
<td>twofish128</td>
</tr>
<tr>
<td>arcfour256</td>
<td>twofish128-ctr</td>
</tr>
<tr>
<td>blowfish</td>
<td>twofish192</td>
</tr>
<tr>
<td>blowfish-ctr</td>
<td>twofish192-ctr</td>
</tr>
<tr>
<td>cast128</td>
<td>twofish256</td>
</tr>
<tr>
<td>cast128-ctr</td>
<td>twofish256-ctr</td>
</tr>
<tr>
<td>des</td>
<td></td>
</tr>
</tbody>
</table>

For example, if using an OpenSSH server with a default list of ciphers, you must add one or more of these ciphers in the OpenSSH's sshd_config file, and then restart the SSH server. For more information about OpenSSH ciphers, see: [http://www.openbsd.org/cgi-bin/man.cgi/OpenBSD-current/man5/sshd_config.5?query=sshd_config&sec=5](http://www.openbsd.org/cgi-bin/man.cgi/OpenBSD-current/man5/sshd_config.5?query=sshd_config&sec=5)

**Domain controller issue**

Safeguard does not manage passwords for accounts on domain controllers; Safeguard manages passwords for accounts on a domain controller through a directory that hosts the domain controller. For more information, see Adding directory accounts to a directory on page 193.

**Networking issue**

If you are having system connectivity issues, here are some things to consider:

- Are there security rules on the network (such as firewalls or routers) that might be preventing this traffic?
- Is traffic from Safeguard routable to the network address of the managed system?
- Are there any problems with cables, hubs, or switches, and so forth?

You could be experiencing network issues like these:

- a network outage
- a router misconfiguration
- an unplugged wire
- a switch not working
If Safeguard suspends event notifications, try logging out and logging back in to re-subscribe to SignalR.

**Windows WMI connection**

To enable Safeguard to manage Windows assets, you must configure your firewall to allow Windows Management Instrumentation (WMI).

**Timeout errors causing operations to fail**

If you experience any timeout errors, wait a few minutes and retry the operation.

If you are performing clustering operations in the background, for example adding replicas to a cluster, wait for the cluster operations to complete before performing other operations in Safeguard.

| TIP: A timeout error can appear as a "Request failed. A task was canceled." error message. |

**User locked out**

If a user has not logged onto Safeguard for a set number of days, Safeguard disables the user account.

| NOTE: This is set using the Disable After setting in Administrative Tools | Settings | Password Settings | Login Control. For more information, see Login Control on page 357. |

**Related Topics**

Unlocking a user's account

**User not notified**

If a user did not receive an email notification, first check to see if you have set everything up in Safeguard correctly for the email notifications to work properly. For more information, see Enabling email notifications on page 327.
Notification lists

Safeguard does not dynamically maintain the email addresses for an escalation notification contact list.

If you change a Safeguard user’s email address or delete a Safeguard user after creating a policy, you must update the email addresses in escalation notification contact lists manually. For example, when you create a policy you can indicate who to contact when emergency access has been used. If a user has changed his or her email address, the notification will not be received by that individual. Furthermore, if a user has been deleted from Safeguard, he or she will still receive the notification.
Frequently asked questions

The following topics will help you find answers to some of your questions about managing Safeguard:

- How do I access the API
- How do I audit transaction activity
- How do I configure external federation authentication
- How do I manage accounts on unsupported platforms
- How do I modify the appliance configuration settings
- How do I prevent Safeguard messages when making RDP connections
- How do I see which assets and/or accounts are governed by a profile
- How do I set the appliance system time
- How do I setup discovery jobs
- How do Safeguard database servers use SSL
- What are the access request states
- What do I do when an appliance goes into quarantine
- What is required for One Identity Safeguard Privileged Sessions
- What is required to integrate with Starling Identity Analytics & Risk Intelligence
- What needs to be set up to use Application to Application
- What role-based email notifications are generated by default
- When does the rules engine run for dynamic grouping and tagging
- Why did the password change during an open request
- Why join Safeguard to One Identity Starling

Related Topics

Appliance settings
Troubleshooting
How do I access the API

You can use the API to automate Safeguard tasks and access functionality not currently available in the Windows desktop client. Safeguard has the following API categories:

- **Appliance**: Resources used to manage the appliance itself (like setting the time, network configuration, syslog, etc.)
  
  https://<Appliance IP>/service/appliance/swagger/

- **Core**: Resources used to govern policy and manage accounts, etc.
  
  https://<Appliance IP>/service/core/swagger/

- **Notification**: Resources used to query the Safeguard appliance status
  
  https://<Appliance IP>/service/notification/swagger/

You must use a bearer token to access most resources in the API. When using the Swagger web UI (as referenced in the URLs above), click the Authorize button at the top of each page and log in using the web UI. The Swagger web UI adds the bearer token to each API request automatically. However, if you are manually making the API request or writing your own application/script, perform the following two steps to obtain a bearer token:

1. You must first authenticate using the OAuth 2.0 **Resource Owner Password Credentials** or **Client Credentials** grant types. An example of the former is:

   ```
   POST https://<ApplianceIP>/RSTS/oauth2/token
   Host: <ApplianceIP>
   Content-Type: application/json
   Accept: application/json
   ```

   ```json
   {
     "grant_type": "password",
     "username": "<Username>",
     "password": "<Password>",
     "scope": "rsts:sts:primaryproviderid:local"
   }
   ```

   Where:

   - *grant_type* is required and must be set to *password*.
   - *username* is required and set to the user account you want to log in as.
   - *password* is required and set to the password associated with the username.
   - *scope* is required and set to one of the available identity provider's scope ID. The value shown in the example request, "rsts:sts:primaryproviderid:local",
is the default value available on all Safeguard appliances. User accounts that you create in Safeguard directly (that is, not an Active Directory or LDAP account) will most likely have this scope value.

**NOTE:** The list of identity providers is dynamic and their associated scope ID can only be obtained by making a request to:

```
https://<ApplianceIP>/RSTS/UserLogin/LoginController?response_type=token&redirect_uri=urn:InstalledApplication&loginRequestStep=1
```

and parsing the returned JSON for the Providers.Id property. That value should then be concatenated to the string "rsts:sts:primaryproviderid:" to produce the OAuth 2.0 scope parameter.

If you wish to authenticate using a client certificate, you must use the OAuth 2.0 **Client Credentials** grant type in which your certificate is included as part of the SSL connection handshake and the Authorization HTTP header is ignored. Set the scope to rsts:sts:primaryproviderid:certificate or any other identity provider that supports client certificate authentication.

```
POST https://<ApplianceIP>/RSTS/oauth2/token
Host: <ApplianceIP>
Content-Type: application/json
Accept: application/json

{
    "grant_type": "client_credentials",
    "scope": "rsts:sts:primaryproviderid:certificate"
}
```

2. After successfully authenticating, your response will contain an access_token that must be exchanged for a user token to access the API.

```
POST https://<ApplianceIP>/service/core/v2/Token/LoginResponse
Host: <ApplianceIP>
Content-Type: application/json
Accept: application/json

{
    "StsAccessToken": "<access_token from previous response>"
}
```

You should now have an authorization token to be used for all future API requests. The token is to be included in the HTTP Authorization header as a Bearer token like this:

```
Authorization: Bearer <UserToken value>
```

For example:

```
GET https://<ApplianceIP>/service/core/v2/Users/-2
```
Host: <ApplianceIP>
Accept: application/json
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1Ni...

<table>
<thead>
<tr>
<th>Table 266: API query filtering: Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Output</strong></td>
</tr>
<tr>
<td>fields</td>
</tr>
<tr>
<td>orderby</td>
</tr>
</tbody>
</table>

- implies descending order

The following paging parameters allow you to include an item count, the starting page, and the number of items per page.

<table>
<thead>
<tr>
<th>Table 267: API query filtering: Paging</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Paging</strong></td>
</tr>
<tr>
<td>count</td>
</tr>
<tr>
<td>page &amp; limit</td>
</tr>
</tbody>
</table>

The following operators can be used to filter the results.
Table 268: API query filtering: filter parameter

<table>
<thead>
<tr>
<th>Operator</th>
<th>Example</th>
<th>Description/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>eq</td>
<td>GET /AssetAccounts?filter=Name eq 'George'</td>
<td>equal to</td>
</tr>
<tr>
<td>ne</td>
<td>GET /Users?filter=LastName ne 'Bailey'</td>
<td>not equal to</td>
</tr>
<tr>
<td>gt</td>
<td>GET /Assets?filter=Id gt 10</td>
<td>greater than</td>
</tr>
<tr>
<td>ge</td>
<td>GET /Assets?filter=Id ge 10</td>
<td>greater than or equal to</td>
</tr>
<tr>
<td>lt</td>
<td>GET /Assets?filter=Id lt 10</td>
<td>less than</td>
</tr>
<tr>
<td>le</td>
<td>GET /Assets?filter=Id le 10</td>
<td>less than or equal to</td>
</tr>
<tr>
<td>and</td>
<td>GET /UserGroups?filter=(Id eq 1) and (Name eq 'Angels')</td>
<td>both operands return true</td>
</tr>
<tr>
<td>or</td>
<td>GET /UserGroups?filter=(Id eq 1) or (Name eq 'Bedford')</td>
<td>at least one operand returns true</td>
</tr>
<tr>
<td>not</td>
<td>GET /UserGroups?filter=(Id eq 1) and not (Name eq 'Potters')</td>
<td>narrows the search by excluding the &quot;not&quot; value from the results</td>
</tr>
<tr>
<td>contains</td>
<td>GET /Users?filter=Description contains 'greedy'</td>
<td>contains the word or phrase</td>
</tr>
<tr>
<td>q</td>
<td>GET /Users?q=bob</td>
<td>q can be used to search across text properties; means &quot;contains&quot; for all relevant properties.</td>
</tr>
<tr>
<td>in</td>
<td>GET /Users?filter=UserName in ['bob', 'sally', 'frank']</td>
<td>property values in a predefined set</td>
</tr>
</tbody>
</table>

**NOTE:** When using the filter parameter, you can use parenthesis () to group logical expressions.
For example, GET/Users?filter=(FirstName eq 'Jane' and LastName eq 'Smith') and not Disabled

**NOTE:** When using the filter parameter, use the backward slash character (\) to escape quotes in strings.
For example: Get/Users?filter=UserName contains ''

### How do I audit transaction activity

The appliance records all activities performed within One Identity Safeguard. Any administrator has access to the audit log information; however, your administrator
permission set determines what audit data you can access. For more information, see Administrator permissions on page 421.

Safeguard provides several ways to audit transaction activity.

Table 269: Safeguard’s auditing tools

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Archive</td>
<td>Where you access a previous password for an account for a specific date.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Viewing password archive on page 112.</td>
</tr>
<tr>
<td>Check and Change Log</td>
<td>Where you view an account’s password validation and reset history.</td>
</tr>
<tr>
<td></td>
<td>Access the Check and Change Log from Accounts. For more information, see Accounts on page 95.</td>
</tr>
<tr>
<td>History</td>
<td>Where you view the details of each operation that has affected the selected item.</td>
</tr>
<tr>
<td></td>
<td>Each of the Administrative Tools has a History tab. For more information, see History tab on page 100.</td>
</tr>
<tr>
<td>Activity Center</td>
<td>Where you can search for and review any activity for a specific time frame.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Activity Center on page 50.</td>
</tr>
<tr>
<td>Workflow</td>
<td>Where you can audit the transactions performed as part of the workflow process from request to approval to review for a specific access request.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Auditing request workflow on page 57.</td>
</tr>
<tr>
<td>Reports</td>
<td>Where you can view and export entitlement reports that show you which assets and accounts a selected user is authorized to access.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Reports on page 60.</td>
</tr>
</tbody>
</table>

How do I configure external federation authentication

One Identity Safeguard supports the SAML 2.0 Web Browser SSO Profile, allowing you to configure federated authentication with many different Identity Provider STS (IdP-STS) servers and services, such as Microsoft’s AD FS and Azure AD. Through the exchange of the federation metadata, you can create a trust relationship between the two systems. Then, you will create a Safeguard user account to be associated with the federated account. When an end user logs in, they will be redirected to the external IdP-STS to enter their credentials and perform any two-factor authentication that may be required by that IdP-
STS. After successful authentication, they will be redirected back to Safeguard and logged in.

**NOTE:** Additional two-factor authentication can be assigned to the associated Safeguard user account to force the user to authenticate again after being redirected back from the external IdP-STS.

To use external federation, you must first download the federation metadata XML for your IdP-STS and save it to a file. For example, for Microsoft's AD FS, you can download the federation metadata XML from:


### How do I add an external federation provider trust in Safeguard

It is the responsibility of the Appliance Administrator to configure the external federation service providers in Safeguard.

**To add an external federation service provider**

1. In Settings, select **External Integration | External Federation**.
2. Click (or tap) **Add External Federation** to add a new external federation service provider.
3. In the **External Federation** dialog, supply the following information:
   a. **Name**: Enter a unique display name for the external federation service provider. The name is used for administrative purposes only and will not be seen by end users.
      Limit: 100 characters
      Required
   b. **Realm**: Enter a unique realm value, typically a DNS suffix, like contoso.com, that matches the email addresses of users intended to use this IdP-STS for authentication. A case-insensitive comparison will be used on this value when performing Home Realm Discovery.
      Wildcards are not allowed.
      Limit: 255 characters
      Required
   c. **Federation Metadata File**: Choose or enter the file path to the IdP-STS federation metadata file that you previously downloaded.
   d. **Download Safeguard Federation Metadata**: If you have not done so before, click the link to download a copy of Safeguard's federation metadata XML. You will need this file when creating the corresponding trust relationship on your IdP-STS server.
NOTE: The federation metadata XML files typically contain a digital signature and cannot be modified in any way, including white space. If you receive an error regarding a problem with the metadata, ensure that it has not been edited.

How do I create a relying party trust for the IdP-STS

The process for creating the relying party trust in your IdP-STS will differ between applications and services. However, as stated earlier, you can download a copy of Safeguard’s federation metadata by clicking the link when you entered the IdP-STS information in Safeguard. You can also download the Safeguard federation metadata at any time from the Settings | External Integration | pane toolbar (Download) or from the following URL:

https://<Safeguard server>/RSTS/Saml2FedMetadata

If the IdP-STS does not support importing federation metadata, but instead requires you to manually input values, you will typically need an App ID and Login or Redirect URL. Both of these values can be copied from the Safeguard federation metadata XML file you downloaded.

- The App ID for Safeguard will come from the entityID attribute of the <EntityDescriptor> element in the XML file.
- The Login or Redirect URL will come from the Location attribute of the <AssertionConsumerService> element within the <SPSSODescriptor> element.

NOTE: Only the HTTP-POST binding is supported for this end point.

You must then configure or ensure that the IdP-STS returns the authenticated user’s email address as a SAML attribute claim. The email address must appear in either the standard SAML email address or name claim:

- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

NOTE: Any other attributes or claims will be ignored.

The SAML Response or Assertion must be signed, but not encrypted. When the signing certificate used by your IdP-STS expires, you must update the metadata in Safeguard by uploading a new copy of your IdP-STS’s metadata file. Safeguard will not automatically attempt to refresh the metadata.

NOTE: Your IdP-STS’s metadata can contain more than one signing certificate to allow for a grace period between an expiring certificate and a new one.

For further details regarding specific IdP-STS servers, see the following knowledge base articles on the One Identity support site:
How do I add an external federation user account

It is the responsibility of either the Authorizer Administrator or the User Administrator to add an associated external federation Safeguard user.

**NOTE:** You must add external federation service providers to Safeguard before you can add external federation user accounts.

**NOTE:** No user information, such as first name, last name, phone number, email address, is ever imported from the IdP-STS claims token. You must enter that information manually when creating the user in Safeguard if you need it.

**To add an external federation user account**

1. In Users, click (or tap) **Add User** from the toolbar.
2. In the User dialog, provide the following information on the **Authentication** tab:
   a. **Authentication Provider**: Select a previously configured external federation service provider.
   b. **Email Address or Name Claim**: Enter the email address or name claim that will be returned from the IdP-STS of an authenticated user.
      
      **NOTE:** A case-insensitive comparison will be performed on the value when the user is logging in.

      **NOTE:** You must configure or ensure that the IdP-STS includes either the email address claim or name claim. Safeguard will first look for the email address claim in the claims token. If that claim does not exist, it will use the name claim. You must create the user account in Safeguard according to what claim is returned by your IdP-STS, with precedence given to the email address claim.
   c. **Require Secondary Authentication**: If secondary authentication is required, select this check box.
      
      • Choose the secondary authentication provider for this user.
      
      • Once the secondary authentication provider is specified, choose or enter the information required for two-factor authentication based on the type.

      For more information, see **Authentication tab** on page 376.
How do I manage accounts on unsupported platforms

Safeguard makes it possible for you to manage passwords for accounts on unsupported platforms by using a profile with a manual change password setting. For example, you might have an asset that is not on the network. The manual change password setting allows you to comply with your company policies to change account passwords on a regular schedule without using the Safeguard automatic change password settings. Safeguard notifies you by email, toast notification, or both on a set schedule to change account passwords manually. You can then reset the password yourself, or allow Safeguard to generate a random password according to the password rule selected in the profile.

IMPORTANT: After you change the password in Safeguard you must remember to change the password on the account; Safeguard does not do that automatically for you.

The following summarizes the general workflow for managing accounts on unsupported platforms.

To manage account passwords manually

1. Configure a profile with a manual change password setting and assign asset accounts to it. For more information, see Adding change password settings on page 344.
2. Ensure toast notifications or email notifications are properly configured. For more information, see Settings or Enabling email notifications.
3. When notified to change an account password, choose the Set Password option you prefer:
   a. Generate Password - to have Safeguard generate a new random password, that complies with the password rule that is set in the account's profile.
      i. Click (or tap) Generate Password to display the Password Change dialog.
      ii. Click (or tap) Show Password to reveal the new password.
      iii. Click (or tap) Copy to place the value into your copy buffer.
      iv. Click (or tap) Success to change the password in the Safeguard database.
      i. Click (or tap) Manual Password to display the Set Password dialog.
      ii. Enter and save a new password.
      OK updates the Safeguard database.
iii. Set the account password on the physical device to synchronize it with Safeguard.

How do I modify the appliance configuration settings

You can modify the appliance configuration settings using the Web client or Windows desktop client (Administrative Tools | Settings | Appliance).

**NOTE:** This topic assumes you have already performed the initial appliance installation and configuration steps in the One Identity Safeguard Appliance Setup Guide provided in the box with your hardware equipment.

**To modify the appliance configuration settings (web client)**

1. Log into the Safeguard Web client using the Appliance Administrator account.
2. Select ; then, click (or tap) a to open the Appliance Settings pane.
3. In the Application Settings pane, select Appliance Configuration.
4. On the Appliance Configuration page, configure the following:

   **NOTE:** Click (or tap) the Edit icon to modify these settings. After editing a setting, you must save that individual setting before editing an additional setting.

   - **Time:** Enable Network Time Protocol (NTP) and set the primary and secondary NTP servers, if desired.
   - **Network (X0):** Enter the DNS Server address information for your primary interface.
   - **Sessions (X1):** Configure the sessions interface.

**To modify the appliance configuration settings (Windows desktop client)**

1. Log in using the Appliance Administrator account.
2. Navigate to Administrative Tools | Settings | Appliance.
3. Expand the Time pane to enable NTP and set the primary and secondary NTP servers. Click (or tap) OK.
4. Expand the Appliance Information pane to change the appliance name.
   a. To change the appliance's name, click (or tap) Edit next to the Appliance Name.
5. Expand the Networking pane to add or modify DSN suffixes and to configure the network interface for the Privileged Sessions module.
a. To change the DNS suffixes for your primary interface, click (or tap) Edit next to the **Network Interface X0** heading.
   - Enter the DSN suffixes to be used.
   - Click (or tap) OK.

b. To configure the sessions interface, click (or tap) Edit next to the **Network Interface X1** heading.
   - Enter the IP Address, netmask, and gateway information, and the DNS servers and suffixes.
   - Click (or tap) OK.

**How do I prevent Safeguard messages when making RDP connections**

When making an RDP connection, you may encounter two different certificate messages.

- **Unsigned RDP file message**

  ![Remote Desktop Connection](image)

  This message occurs when Remote Desktop Connection opens the RDP file that is downloaded when you click (or tap) **Play** in the Safeguard user interface.

  We are currently working on a solution that will allow Safeguard to sign this RDP file to avoid this message.

- **Untrusted server certification message**
This message occurs when the workstation has not trusted the Safeguard RDP Connection Signing Certificate.

NOTE: The IP address of the connecting server is that of the Safeguard appliance.

To avoid this message, you must trust the RDP Connection Signing Certificate and certificates in its chain of trust or replace the current certificate with an enterprise certificate and chain of trust that is trusted. For more information on certificate chain of trust, see Certificate chain of trust on page 487. For more information on replacing the RDP Connection Signing Certificate, see Sessions Certificates on page 302.

One Identity recommends that you replace the entire configuration with your own trusted enterprise PKI. This would result in a structure such as:

- Your Root CA
  - Your Issuing CA
    - Your RDP Signing Certificate (from Safeguard CSR)
      - <Sessions module generated certificate>

The Root CA, Issuing CA, and RDP Signing Certificates can be distributed via Group Policy, Active Directory, or other distribution means.

Related Topics

Sessions Certificates
Certificate chain of trust

The default certificate chain of trust configuration that ships with Safeguard is generated from the SafeguardCluster root certificate.

Figure 1: Default certificate chain of trust

When setting up RDP Connection Signing, the certificate chain of trust also includes the certificate issued to Safeguard for RDP, as illustrated below.
Figure 2: Default certificate chain of trust when setting up RDP Connection Signing

NOTES:

- The Safeguard Cluster certificate must be added to the trusted root CA certificate store and the DefaultSessionRdpSigning certificate must be added to the intermediate CA certificate store of the workstations from which a session request is submitted.
- Once configured, RDP sessions from any cluster member will be trusted (thus avoiding the Untrusted server certification message) because the certificate for each Safeguard cluster member is issued the DefaultSessionRdpSigning certificate.
- This also prevents receiving new messages should the IP address of the Safeguard appliance change.
How do I see which assets and/or accounts are governed by a profile

To see which assets and/or accounts are assigned to a profile, you must open the profile details window.

To view which assets or accounts are assigned to a partition profile

1. In Partitions or Directories, switch to the Profiles tab.
2. Select a profile and click (or tap) the Details icon.
3. In the profile dialog, select the Scope tab which provides a list of the assets and accounts currently being governed by the selected profile.

How do I set the appliance system time

NOTE: Changing appliance time can result in unintended consequences with processes running on the appliance. For example, there could be a disruption of password check and change profiles and audit log timestamps could be misleading.

TIP: As a best practice, set an NTP server to eliminate possible time-related issues. For more information, see Time on page 264.

To set the time on your appliance

- Use the appliance API to change the appliance time (SystemTime). For information about using the API, see How do I access the API.

How do I setup discovery jobs

Safeguard allows you to configure these types of discovery jobs to automatically add assets and accounts.

Table 270: Safeguard Discovery types

<table>
<thead>
<tr>
<th>Discovery job</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset discovery</td>
<td>Asset discovery jobs run automatically against the directories you have added to Safeguard. For more information, see Asset discovery job workflow on page 490.</td>
</tr>
<tr>
<td>Account discovery</td>
<td>Account discovery jobs run automatically against the assets that</td>
</tr>
</tbody>
</table>
### Discovery job

<table>
<thead>
<tr>
<th>Discovery job</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>are in the scope of a partition profile. For more information, see <a href="#">Account discovery job workflow</a> on page 491.</td>
<td></td>
</tr>
<tr>
<td>Directory account discovery</td>
<td>Directory account discovery jobs run automatically each time Safeguard synchronizes the directory. For more information, see <a href="#">Directory account discovery job workflow</a> on page 492.</td>
</tr>
</tbody>
</table>

### Asset discovery job workflow

Safeguard's asset discovery jobs run automatically against the directories you have added to Safeguard. For more information, see [Discovery](#) on page 156.

*To configure and schedule rules that perform asset discovery jobs*

1. Create an asset discovery job. For more information, see [Creating an asset discovery job](#) on page 157.
2. After you save the discovery job, you can test it by selecting **Run Now**. For more information, see [Managing asset discovery jobs](#) on page 165.
3. After the asset discovery job runs, navigate to **Assets**, right-click (or press and hold) an asset and choose one of these context menu options:

   - **Manage**: Select to manage an "ignored" asset.
     - This option is only available for assets that have been ignored.

   - **Ignore**: Select to prevent Safeguard from managing the selected asset.
     - **NOTE**: When you ignore an asset, Safeguard disables it and removes all associated accounts. If you choose to **Manage** the asset later, Safeguard re-enables all the associated accounts.

4. To show or hide assets marked as "Ignore", use these buttons:

   - **Show Ignored**: Display the hidden assets.
   - **Hide Ignored**: Hide assets marked as "Ignore".

5. Search the **Activity Center** for information about discovery jobs that have run. Safeguard lists the asset discovery events in the **Asset Discovery Activity** category.
Account discovery job workflow

Safeguard's account discovery jobs run automatically against the assets that are in the scope of a partition profile. For more information, see About profiles on page 233.

**NOTE:**

Safeguard supports account discovery on the following platforms:

- AIX
- HP-UX
- Linux
- MAC OS X
- Solaris
- Windows

**To configure and schedule rules that perform discovery jobs**

1. Create a partition. For more information, see Adding a partition or Adding a directory.
2. Create an account discovery job. For more information, see Account Discovery on page 267.
3. Create a profile. (For more information, see Creating a partition profile or Creating a directory profile.

**NOTE:** All profiles run the configured account discovery jobs on the assets that are assigned to the scope of the profile, according to the account discovery setting’s schedule.

4. After the account discovery job runs, open the partition's Discovered Accounts tab to mark the accounts:
   a. Click (or tap) **Ignore** to prevent Safeguard from managing the selected account.
   b. Click (or tap) **Manage** to add the selected account to the selected partition and assign it to the scope of the default profile.

**NOTE:** The discovery job finds all accounts that match the discovery rule's criteria regardless of whether it has been marked Ignore or Manage in the past.

5. Search the Activity Center for information about discovery jobs that have run. Safeguard lists the account discovery events in the Account Discovery Activity category.
Directory account discovery job workflow

Safeguard's directory account discovery jobs run automatically each time it synchronizes the directory. You can view or modify the Synchronization Interval on the directory’s General tab.

To configure directory account discovery jobs

1. Create a directory account discovery job. For more information, see Managing directory account discovery jobs on page 195.
2. After the directory account discovery job runs, open the directory's Discovered Accounts tab to mark the accounts:
   a. Click (or tap) Ignore to prevent Safeguard from managing the selected directory account.
   b. Click (or tap) Manage to add the selected account to the selected directory and assign it to the scope of the default profile.

   **NOTE:** The discovery job finds all accounts that match the discovery rule’s criteria regardless of whether it has been marked Ignore or Manage in the past.
3. Search the Activity Center for information about discovery jobs that have run. Safeguard lists the directory account discovery events in the Account Discovery Activity category.

How do Safeguard database servers use SSL

Some database servers use Secure Socket Layer (SSL) when communicating with Safeguard. Depending on the platform type, version, and configuration, the database server can either use SSL for only encrypting the session or it can use SSL for encrypting and verifying the authenticity of the database server.

ODBC Transport

The following platforms use the ODBC transport. Safeguard installs the appropriate software driver on the appliance to communicate with the platform. The configuration data that Safeguard uses to initialize a connection with the server is in the form of a connection string consisting of a colon-separated list of driver-specific options.

By default, the database servers encrypt the login data, but not the subsequent data passed on the connection. You must configure SSL and enable it on the database server to enable encryption for the session data.
Microsoft SQL Server

Microsoft SQL Server is always capable of encrypting the connection with SSL. It listens on a single port for both SSL and non-SSL connections.

If you have set the Force Encryption option to yes on the SQL server, then it uses SSL to encrypt the data, regardless of whether the Safeguard client requests it or not.

You can set the Force Encryption option to yes on the SQL server without configuring a server certificate. In this case, the SQL server transparently generates a self-signed certificate to use when a Safeguard client requests encryption. This makes it possible for the SQL server to use SSL only to provide encryption for the session without verifying the server certificate.

**NOTE:** It is not possible from within a running session to detect whether the SQL server is using SSL for encryption.

### Table 271: SQL Server SSL Support

<table>
<thead>
<tr>
<th>Safeguard Client Options</th>
<th>Microsoft SQL Server Configuration</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use SSL Encryption</td>
<td>Verify SSL Cert</td>
<td>Force Encryption</td>
</tr>
<tr>
<td>No</td>
<td>n/a</td>
<td>No</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>n/a</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>n/a</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>n/a</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>n/a</td>
</tr>
</tbody>
</table>

### MySQL Server

To support SSL you must compile the MySQL server software with SSL support and correctly configure it with a CA certificate and server certificate. If there is any problem
with the certificate, the MySQL server may log an error and start up without SSL support. In this case the MySQL server rejects the request to enable SSL for a session as there is no certificate to verify against and does not encrypt the session. The MySQL server listens on a single port for both types of connections.

The behavior of the MySQL server depends on the server version and configuration. In some versions of MySQL, the server enables SSL by default on all Safeguard client sessions once it is configured.

If the MySQL server defaults to using SSL, or requires SSL for a user, the MySQL server encrypts the session even if the Safeguard client does not request it. However, the Safeguard client cannot request to use SSL just for encryption; it can only request SSL if you have imported the correct CA certificate to Safeguard.

NOTE: It is possible to detect that SSL is in use from within a session by examining the session variables. That is, the Safeguard client can detect if a request to use SSL has not been honored and displays an error.

<table>
<thead>
<tr>
<th>Safeguard Use SSL Encryption Option</th>
<th>SSL Supported on MySQL Server</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Unencrypted session.</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Determined by the MySQL server. The server encrypts the session if it defaults to using SSL or requires it for this user.</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Safeguard client detects this and reports a failure.</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Safeguard requests that the MySQL server encrypt the session and verify the server certificate against the trusted CA certificate in Safeguard</td>
</tr>
</tbody>
</table>

**Sybase ASE Server**

To support SSL you must correctly configure the Sybase server with a CA certificate and server certificate. The Sybase server listens on different ports for SSL and non-SSL connections, and rejects a mismatched request from a Safeguard client to a particular port.

The Safeguard client cannot request to use SSL just for encryption; it can only request SSL if you have imported the correct CA certificate to Safeguard.
Table 273: MySQL Server SSL Support

<table>
<thead>
<tr>
<th>Safeguard Use SSL Encryption Option</th>
<th>Sybase Server Listening Port uses SSL</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Unencrypted session.</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>The Sybase server rejects the connection attempt.</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>The Sybase server rejects the session with an SSL error.</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Safeguard requests that the Sybase server encrypt the session and verify the server certificate against the trusted CA certificates in Safeguard.</td>
</tr>
</tbody>
</table>

**NOTE:** The ODBC driver cannot detect that this is an SSL error and displays a 'client cannot connect' error.

### What are the access request states

Safeguard uses the following access request states, which change as a request steps through the workflow process.

Table 274: Access request states

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>Approved requests that are ready for the requester. That is, for password release requests, the requester can view or copy the password. For session access requests, the requester can launch the session.</td>
</tr>
<tr>
<td>Approved</td>
<td>Requests that have been approved, but the checkout time has not arrived.</td>
</tr>
<tr>
<td>Denied</td>
<td>Requests denied by the approver.</td>
</tr>
<tr>
<td>Expired</td>
<td>Requests for which the checkout duration has elapsed.</td>
</tr>
<tr>
<td>Pending</td>
<td>Requests that are waiting for approval.</td>
</tr>
<tr>
<td>Revoked</td>
<td>Approved requests retracted by the approver.</td>
</tr>
</tbody>
</table>

**NOTE:** The approver can revoke a request between the time the requester views it and checks it back in.
What do I do when an appliance goes into quarantine

Safeguard appliances can end up in a quarantine state if something goes wrong while doing certain activities with the Safeguard appliance. The best defense against losing data or compounding problems associated with quarantined appliances is a good and recent backup (Backup and Retention settings). The appliance (at least one appliance in a clustered environment), should be set up to take a scheduled backup regularly, which should be saved to an archive server so that if something happens, you can recover with minimum downtime and loss.

To recover an appliance in a quarantine state

If a Safeguard appliance goes into a quarantine state, use one of the following options to recover:

Option 1: Restart the appliance

Unless you have a good reason not to restart the appliance, this should be your first step. Often times, a quarantine happens because the system was waiting for a response that did not return in time. Restarting the Safeguard appliance allows it to retry and frequently fixes itself.

1. To restart a quarantined appliance, connect to the recovery kiosk (Recovery kiosk) for that machine and restart it from there. Once the appliance has restarted, it will take several minutes for Safeguard to start.
2. If you log into the appliance using the desktop client while Safeguard is starting, you will see a maintenance mode screen. At the end of the maintenance mode, you will see a Restart Desktop Client button or the Quarantine warning.
   a. If you see the Restart Desktop Client button, the restart successfully recovered the appliance and brought the appliance back in a healthy state.
   b. If the Quarantine warning appears, proceed to Option 2.

   NOTE: Clustered environment: If the quarantined appliance was the primary appliance, use the Failover option to reassign the primary appliance role to a healthy member of the cluster (Failing over to a replica by promoting it to be the new primary).

Option 2: Factory reset the appliance

If restarting the appliance did not fix the problem, it will be necessary to do a factory reset on the appliance in order to fix it.

CAUTION: Factory reset returns the appliance to its original state when it first came from the factory. All data and configuration settings will be lost and any patches applied will be removed.
1. To perform a factory reset, connect to the recovery kiosk and select the **Factory Reset** option (Factory reset).

   NOTE: You must contact One Identity Technical Support to complete the operation.

   Once the factory reset is started, you must wait until it finishes (it could take up to 30 minutes to complete). When the factory reset is complete, the kiosk will return an Online indicator.

2. Once the factory reset is complete:
   a. Re-configure the network interface settings.
   b. Re-apply any patches you had installed.
   c. If this is an unclustered appliance, upload and restore the most recent backup to retrieve your data (Restore).
   d. If the appliance was a member of a cluster, skip the restore step and join the appliance to the cluster as if it were a brand new appliance (Enrolling replicas into a cluster). Safeguard will take care of replicating all the data back to the appliance.

**To remove a quarantined appliance from a cluster**

1. First try to unjoin the replica appliance from the cluster (Unjoining replicas from a cluster).
2. If unjoining the appliance fails, reset the cluster to remove the appliance from the cluster (Resetting a cluster that has lost consensus).

### What is required for One Identity Safeguard Privileged Sessions

One Identity Safeguard for Privileged Sessions enables you to issue privileged access to users for a specific period or session and gives you the ability to record, archive, and replay user sessions so that your company can meet its auditing and compliance requirements.

Before using Privileged Sessions, make sure the following settings and configuration are in place:

- **Appliance Administrator**: Ensure the Privileged Sessions module is licensed (`Settings` | `Appliance` | `Licensing`). For more information, see Licensing on page 259.
- **Appliance Administrator**: Ensure the Network Interface X1 is configured (`Settings` | `Appliance` | `Networking`). For more information, see Networking on page 261.
- **Appliance Administrator**: Ensure the session request service is enabled (`Settings` | `Access Request` | `Enable or Disable Services`). For more information, see
Enable or Disable Services (Access request and password management services) on page 247.

- Appliance Administrator: Safeguard ships with default session certificates; however, it is recommended that you replace the default certificate with your own (Settings | Certificates | Session Certificates). For more information, see Sessions Certificates on page 302.
- Security Policy Administrator: Ensure there is an entitlement with an access request policy for both SSH and RDP sessions defined. For more information, see Entitlements on page 204.
- Ensure Remote Desktop is enabled for Windows machines that are going to be using RDP.
- Ensure the necessary SSH algorithms are configured for any Unix or Linux machines that are going to be using SSH.

**NOTE:** Safeguard ships with default SSH algorithms configured for Unix and Linux machines. To add new algorithms, use the API endpoint:

https://<Appliance IP>/service/core/swagger/SessionsSSHAlgorithm

**Related Topics**

About sessions and recordings

**What is required to integrate with Starling Identity Analytics & Risk Intelligence**

The Starling Identity Analytics & Risk Intelligence service collects and evaluates information from data sources, such as Safeguard, to provide you with valuable insights into your users and entitlements. When integrated with Safeguard, Starling Identity Analytics & Risk Intelligence allows you to identify Safeguard users and entitlements that are classified as high risk and view the rules and details attributing to that classification.

In order to use Safeguard as a data source module in Starling Identity Analytics & Risk Intelligence, you must first add a user to Safeguard, with the following properties:

- Authentication Type: Local or Certificate
- Permissions: Auditor

Once this Safeguard user is defined, you will enter this user's credentials and Safeguard connection information when adding a new data source module in the Starling Identity Analytics & Risk Intelligence service. For more information on configuring a new data source module and the classification rules used to identify high risk users and entitlements, see the One Identity Starling Identity Analytics & Risk Intelligence User Guide.
What needs to be set up to use Application to Application

In order to use Application to Application integration with Safeguard, you must perform the following tasks:

**Step 1:** Prepare third-party application for integration with Safeguard.

**Step 2:** Appliance administrator enables Application to Application service in Safeguard.

Using the desktop client, navigate to Administrative Tools | Settings | Appliance | Enable or Disable Service and click the Application to Application Enabled toggle.

-OR-

Use the following URL: https://appliance/service/appliance/v2/A2AService/Enable

**Step 3:** Asset Administrator adds assets and accounts to Safeguard.

For more information, see Adding an asset and Adding an account

**Step 4:** User Administrator adds certificate users to Safeguard.

For more information, see Adding a user on page 375.

**Step 5:** Security Policy Administrator adds application registration to Safeguard.

For more information, see Adding an application registration on page 321.

**Step 6:** Get the API key and copy/paste it into the third-party application in order to make requests from the third-party application.

For more information, see How do I make a request using the Application to Application service on page 499.

How do I make a request using the Application to Application service

Using the Application to Application service, third-party applications can interact with Safeguard in the following ways:

- Credential retrieval: A third-party application can retrieve a credential from the Safeguard vault in order to perform automated functions on the target asset. In addition, you can replace hard coded passwords in procedures, scripts, and other programs with programmatic calls.

- Access request broker: A third-party application can initiate an access request on behalf of an authorized user so that the authorized user can be notified of the available request and log in to Safeguard to retrieve a password or start a session.
A third-party application authenticates with Safeguard using an API key and a client certificate, rather than the bearer token normally used to authenticate Safeguard API requests. To make a request, you must first retrieve the API key for the application from Safeguard using an authorized user account (that is, using bearer token authentication), and install the correct certificate on the host that will be making the request. The certificate must be installed in the certificate store of the authorized certificate user that will make the request.

**Prerequisites**

- Register the third-party application with Safeguard. For more information, see Adding an application registration on page 321.
- Associate the third-party application with an existing Safeguard certificate user.

**To make a "credential retrieval" request from the third-party application**

1. Retrieve the relevant API key for the application from Safeguard. You can retrieve the API key using the desktop client or API.
   
   Using the desktop client:
   
   - Log into the Safeguard client as a Security Policy Administrator.
   - Navigate to **Administration Tools | Settings | External Integration | Application to Application**.
   - Click ‹ to display the API keys.
   - On the API Keys dialog, select the API key and click ‼.

   Using the Safeguard API:
   
   - Use the following URL to retrieve the details of the registered application from the Safeguard API. The Id property in the response can then be used to retrieve the relevant API key. The Certificate Thumbprint property in the response identifies the certificate that the application must use to authentication the request.
     
     ```
     https://<Appliance IP>/service/core/V2/A2ARegistrations?filter=AppName%20eq%20%22<Application Name>%22
     ```

   - Use the Id property in the response retrieved for the application registration to retrieve the API key for the selected account from the Safeguard API:
     
     ```
     https://<Appliance IP>/service/core/V2/A2ARegistrations/<Id>/RetrievableAccounts?filter=AccountName%20eq%20%22<account name>%22%20and%20SystemName%20eq%20%22<system name>%22&fields=ApiKey
     ```

2. Ensure that the certificate matching the application’s registered CertificateUserThumbprint is installed on the host that will be making the request.

3. Ensure that the selected certificate is trusted by Safeguard. That is, install the trusted root certificate in Safeguard.
4. Create the application request, authenticating with the retrieved API key and the certificate thumbprint.
   - Set the Authorization header in the request to A2A <API key>.
   - The type can be Password or PrivateKey. Note that private keys can only be retrieved for service accounts.
   - Present the certificate with the request as appropriate for the invoking method. For example, when using the Invoke-WebRequest cmdlet, use the option: -CertificateThumbprint <thumbprint>

To retrieve a credential, use the following request:
GET https://<ApplianceIP>/service/A2A/V2/Credentials?type=Password
Host: <ApplianceIP>
Content-Type: application/json
Accept: text/plain
Authorization A2A <API Key>
This URL returns a string response.

To make an "access request broker" request from the third-party application

1. Retrieve the relevant API key for the application from Safeguard. You can retrieve the API key using the desktop client or API.

   Using the desktop client:
   - Log into the Safeguard client as a Security Policy Administrator.
   - Navigate to Administration Tools | Settings | External Integration | Application to Application.
   - Click to display the API keys.
   - On the API Keys dialog, select the API key and click .

   Using the Safeguard API:
   - Use the following URL is retrieve the details of the registered application from the Safeguard API. The Id property in the response can then be used to retrieve the relevant API key. The Certificate Thumbprint property in the response identifies the certificate that the application must use to authentication the request.
     https://<ApplianceIP>/service/core/V2/A2ARegistrations?filter=AppName%20eq%20"<Application Name>"%22
   - Use the Id retrieved for the application registration to retrieve the API key from the Safeguard API:
     https://<ApplianceIP>/service/core/V2/A2ARegistrations/<Id>/AccessRequestBroker/ApiKey

2. Ensure that the certificate matching the application's registered CertificateUserThumbprint is installed on the host that will be making the request.
3. Ensure that the selected certificate is trusted by Safeguard. That is, install the trusted root certificate in Safeguard.

4. Create the application request, authenticating with the retrieved API key and the certificate thumbprint.

   - Set the Authorization header in the request to `A2A <API key>`.
   - Present the certificate with the request as appropriate for the invoking method. For example, when using the `Invoke-WebRequest` cmdlet, use the option: `-CertificateThumbprint <thumbprint>`
   - To create an access request, use the following request:

```
POST
Host: <Appliance IP>
Accept: application/json
Content-type: application/json
Authorization: A2A <API key>
{
  "ForUser": "<user name>",
  "ForUserId": <user id>,
  "ForProvider": "<providername>",
  "SystemId": <system id>,
  "SystemName": "<system name>",
  "AccountID": <account id>,
  "AccountName": "<account name>",
  "AccessRequestType": "<request type>",
  "RequestedDurationDays": <days>,
  "RequestedDurationHours": <hours>,
  "RequestedDurationMinutes": <minutes>,
  "RequestedFor": "<date>",
  "ReasonCodeId": <reason code id>,
  "ReasonCode": "<reason name>",
  "Comment": "<comment>",
  "IsEmergency": <bool>,
  "TicketNumber": "<ticket>"
}
```

This URL returns the new request if successful.
NOTE: Most of the fields in this access request match those in a normal access request, with the following exceptions:

The following fields are used to identify the target Safeguard user that will be used to create the request. The result must uniquely identify a valid Safeguard user for which the application has been granted permission to create an access request. If the search results in multiple matches or no matches, an error is returned.

- ForUserId: The database ID of a Safeguard user. This takes priority if it contains a value.
- ForUser: The name of a Safeguard user. This value is ignored if ForUserId contains a value.
- ForProvider: An optional provider name, that can be used to limit the search for ForUser.

The following fields are used to uniquely identify the target system. If the search results in multiple matches or no matches, an error is returned.

- SystemId: The database ID of a Safeguard asset. This field is used to search for a matching asset in the following order:
  - System Name: Exact match on the system name.
  - Network Address: Exact match on the network address.
  - String search: A string search on all string properties for the asset.

The following fields are used to uniquely identify the target account. If the search results in multiple matches or no matches, an error is returned.

- AccountId: The database ID of a Safeguard account. This takes priority if it contains a value.
- AccountName: This is ignored if AccountId contains a value. This field is used to search for a matching account in the following order:
  - Account Name: Exact match on the account name.
  - String search: A string search on all string properties for the account.

The following fields can be used to identify the reason code. If the search results in multiple matches or no matches, the reason code is set to null.

- ReasonCodeId: The database ID of a predefined reason code. This takes priority if it contains a value.
- ReasonCode: The name of a predefined reason code. This is ignored if ReasonCodeId contains a value.

Once the target user and account have been determined, the Application to Application service attempts to create the access request. Normal policy rules determine whether the attempt is successful.
What role-based email notifications are generated by default

One Identity Safeguard can be configured to send email notifications warning you of operations that may require investigation or action. Your administrative permissions determine which email notifications you will receive by default.

**Table 275: Email notifications based on administrative permissions**

<table>
<thead>
<tr>
<th>Administrative permission</th>
<th>Event/Warning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Administrator</td>
<td>Appliance Healthy</td>
</tr>
<tr>
<td>Operations Administrator</td>
<td>Appliance Restated</td>
</tr>
<tr>
<td></td>
<td>Appliance Sick</td>
</tr>
<tr>
<td></td>
<td>Appliance Task Failed</td>
</tr>
<tr>
<td></td>
<td>Archive Task Failed</td>
</tr>
<tr>
<td></td>
<td>Cluster Failover Started</td>
</tr>
<tr>
<td></td>
<td>Cluster Replica Enrollment Completed</td>
</tr>
<tr>
<td></td>
<td>Cluster Replica Removal Started</td>
</tr>
<tr>
<td></td>
<td>Cluster Reset Started</td>
</tr>
<tr>
<td></td>
<td>Disk Usage Warning</td>
</tr>
<tr>
<td></td>
<td>Factory Reset Appliance</td>
</tr>
<tr>
<td></td>
<td>License Expired</td>
</tr>
<tr>
<td></td>
<td>NTP Error Detected</td>
</tr>
<tr>
<td></td>
<td>Operational Mode Appliance</td>
</tr>
<tr>
<td></td>
<td>Raid Error Detected</td>
</tr>
<tr>
<td></td>
<td>Reboot Appliance</td>
</tr>
<tr>
<td></td>
<td>Shutdown Appliance</td>
</tr>
<tr>
<td>Directory Administrator or delegated partition owner</td>
<td>Account Discovery Failed</td>
</tr>
<tr>
<td></td>
<td>Dependent Asset Update Failed</td>
</tr>
<tr>
<td></td>
<td>Password Change Failed</td>
</tr>
<tr>
<td></td>
<td>Password Check Failed</td>
</tr>
<tr>
<td></td>
<td>Password Check Mismatch</td>
</tr>
<tr>
<td></td>
<td>Password Reset Needed</td>
</tr>
<tr>
<td></td>
<td>Restore Account Failed</td>
</tr>
<tr>
<td></td>
<td>Ssh Host Key Mismatch</td>
</tr>
</tbody>
</table>

Safeguard 2.3 Administration Guide
Frequently asked questions
<table>
<thead>
<tr>
<th>Administrative permission</th>
<th>Event/Warning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ssh Key Change Failed</td>
</tr>
<tr>
<td></td>
<td>Ssh Key Install Failed</td>
</tr>
<tr>
<td></td>
<td>Suspend Account Failed</td>
</tr>
<tr>
<td></td>
<td>Test Connection Failed</td>
</tr>
<tr>
<td>Security Policy Administrator</td>
<td>Policy Expiration Warning</td>
</tr>
<tr>
<td></td>
<td>Policy Expired</td>
</tr>
<tr>
<td></td>
<td>Entitlement Expiration Warning</td>
</tr>
<tr>
<td></td>
<td>Entitlement Expired</td>
</tr>
</tbody>
</table>

**NOTE:** Safeguard administrators can use the following API to turn off these built-in email notifications:

POST /service/core/v2/Me/Subscribers/{id}/Disable

In addition, Safeguard administrators can subscribe to additional events based on their administrative permissions using the following API:

POST /service/core/v2/Events

---

**When does the rules engine run for dynamic grouping and tagging**

The running of the rules engine used for dynamic grouping and tagging is triggered by the creation or change of pertinent objects. For example:

- Whenever you add or change an asset account, all applicable rules are reevaluated against that asset account.
- Whenever you change an asset account rule, the rule is reevaluated against all asset accounts within the scope of that rule. That is, against all asset accounts for grouping and the asset accounts within the designated partitions for tagging.

**NOTE:** In large environments, there is a possibility that the user interface may return before all of the rules have been reevaluated and you may not see the results you were expecting. If this happens, wait a few minutes and **Refresh** the screen to view the results.
Why did the password change during an open request

There are three ways a password can change while a user has it checked out.

1. An Asset Administrator manually changes the password. For more information, see Checking, changing, or setting an account password on page 110.
2. A profile was scheduled to automatically change the password. For more information, see Change Password on page 344.
3. A policy allows both simultaneous access and requires that the password change when a user checks it in.

If the password changes while a user has it checked out, and the current request is still valid, the user can select either Copy or Show Password again to obtain the new password.

Why join Safeguard to One Identity Starling

One Identity Starling Two-Factor Authentication is a SaaS solution that provides two-factor authentication on a product enabling organizations to quickly and easily verify a user's identity. This service is provided as part of the One Identity Starling cloud platform. In addition Starling offers a hybrid service, One Identity Hybrid, that allows you to take advantage of companion features from multiple Starling services, such as Starling Two-Factor Authentication and Starling Identity Analytics & Risk Intelligence.

Joining Safeguard to Starling adds Safeguard to the One Identity Hybrid service allowing you to use features from both the Starling Two-Factor Authentication and Starling Identity Analytics & Risk Intelligence services.

Once Safeguard is joined to Starling, the following Safeguard features are enabled and can be implemented using Starling Two-Factor Authentication:

- **Secondary authentication**
  Safeguard supports two-factor authentication by configuring identity providers, such as Starling Two-Factor Authentication, which are used to configure Safeguard's authentication process such that it prompts for two sources of identity when users log in to Safeguard.

  A Starling 2FA service provider is automatically added to Safeguard when you join Safeguard to Starling. As an Authorizer or User Administrator, you must configure users to use Starling 2FA as their secondary authentication provider when logging into Safeguard. For more information, see Configuring user to use Starling Two-Factor Authentication when logging into Safeguard on page 381.

- **Approval Anywhere**
The Safeguard Approval Anywhere feature integrates its access request workflow with Starling Two-Factor Authentication, allowing approvers to receive a notification through an app on their mobile device when an access request is submitted. The approver can then approve (or deny) access requests through their mobile device without needing access to the desktop or web application.

Approval Anywhere is enabled when you join Safeguard to One Identity Starling. As a Security Policy Administrator, you must define the Safeguard users authorized to use Approval Anywhere. For more information, see Adding authorized user for Approval Anywhere on page 325.

How do I set up a Starling account

To use Starling Two-Factor Authentication as a service provider for secondary authentication and Approval Anywhere, you must first register a Starling Organization Admin account or a Collaborator account associated with the One Identity Hybrid subscription. Also, you must download the Starling 2FA app on your mobile phone to use the Approval Anywhere feature.

NOTE: For additional information and documentation regarding the Starling Cloud platform and Starling Two-Factor Authentication, see https://support.oneidentity.com/starling-two-factor-authentication/hosted/technical-documents.

To sign up for a Starling One Identity Hybrid service trial account

1. Go to https://www.cloud.oneidentity.com/ and log in or register a new account for the Starling cloud platform.
   a. From the Starling home page, click Sign in to Starling.
   b. Enter a valid email address and click Next.
   c. Enter your password and click Sign In.
   d. On the Create your Account page, enter your organization and your mobile phone number.

   NOTE: If the email address you entered does not exist, you will be taken directly to the Create your Account page to register your organization and enter your name, password, and mobile phone number.

   When registering for the first time, you will be sent a verification email in which you must click the supplied link in order to complete the registration process.

2. Once logged in, click the Trial button under the One Identity Hybrid tile. Follow the prompts on the screen.

   The service will be added to the My Services section and be available for use until the trial period has ended. The number of days left in your trial is indicated by a countdown at the top right of the service access button on the home page of Starling.
At any point in the trial you can use the More Information button associated with the service to find out how to purchase the product.
The Safeguard Desktop Player is installed with the Windows desktop client. When the player is launched from the desktop client, the recording is being streamed from the Safeguard appliance. It only exists on the disk for the lifetime of the player session. That is, when you shut down the player, the recording file is removed from the cache.

When you launch the Safeguard Desktop Player, the main view displays, which consists of the following tabbed pages:

- **Information**: Displays detailed information about the recorded session and allows you to play back the recording.
- **Warnings**: Displays warnings associated with the recording.

**Information tab**

The information tab displays the following details for the session recording.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session recording location</td>
<td>Displays the path of where the recording is currently stored.</td>
</tr>
<tr>
<td>Thumbnail</td>
<td>Click the thumbnail in the right corner of the screen to play back the recording.</td>
</tr>
</tbody>
</table>

**NOTE**: The thumbnail is only available for RDP Drawing and SSH Session Shell channels.

**NOTE**: A blinking red recording button in the upper right corner of the thumbnail indicates that the session is "live" allowing you watch the session in follow mode. Follow mode is only available to users with Security Policy Administrator permissions.

| Validation indicators | The Safeguard Desktop Player checks the upstream and downstream traffic from the recording and validates the digital signature and timestamp. The |
**Control** | **Description**
--- | ---
indicators across the top of the screen show the results of this validation process, where all indicators should display a green check mark. If the Signature or Timestamp indicators are red Xs, this indicates that the corresponding certificate has not been validated. For more information, see **Sessions Certificates** on page 302.

<table>
<thead>
<tr>
<th>Recording details</th>
<th>Displays details about the recording, such as:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Duration</td>
</tr>
<tr>
<td>File size</td>
<td>Session ID</td>
</tr>
</tbody>
</table>

| User | Displays the name of the user that authenticated to the remote machine. |
| Connections | Displays connection information, including the address and port of client computer and the remote machine. |

<table>
<thead>
<tr>
<th>Channels</th>
<th>The Channels pane displays the different types of data streams available for a recorded session. An SSH session recording will contain a single channel. Valid channels for an SSH session recording are:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Session Shell</strong>: This is the only SSH channel that can be played back using the desktop player and it contains the actions performed during the session.</td>
<td></td>
</tr>
<tr>
<td><strong>Session SFTP</strong>: Contains data that was transferred using the Secure File Transfer protocol (SFTP). Since this is a file transfer protocol, there is no recording file available for play back.</td>
<td></td>
</tr>
<tr>
<td><strong>NOTE</strong>: This channel is only available when <strong>Allow SFTP</strong> is selected on the Sessions Settings tab in an access request policy.</td>
<td></td>
</tr>
<tr>
<td><strong>Session SCP</strong>: Contains data that was transferred using the Secure Copy protocol (SCP). Since this is a file transfer protocol, there is no recording file available for play back.</td>
<td></td>
</tr>
<tr>
<td><strong>NOTE</strong>: This channel is only available when <strong>Allow SCP</strong> is selected on the Sessions Settings tab in an access request policy.</td>
<td></td>
</tr>
<tr>
<td><strong>X11</strong>: Use this channel to play back the graphical X-server session that was forwarded from the server to the client.</td>
<td></td>
</tr>
</tbody>
</table>
Control | Description
--- | ---
NOTE: This channel is only available when **Allow X11 Following** is selected on the Sessions Settings tab in an access request policy.

An RDP session may contain multiple channels. Valid channels for an RDP session recording are:

- **Clipboard**: Contains any data that was transferred through the clipboard; there is no recording file available for play back.

  NOTE: This channel is only available when **Allow Clipboard** is selected on the Session Settings tab in an access request policy.

- **Drawing**: All RDP sessions will have a Drawing channel, which contains the actions taken during the session. This type of channel is most likely to be replayed.

- **Sound**: Contains any audio associated with the recording.

  Click (or tap) the **Play** button next to the channel to play back the session recording.

  Clicking the expansion button next to a channel displays a list of key details. For a description of these keys and values, see **Key descriptions**.

**Warning tab**

The warning tab displays any warnings encountered when opening and processing the recording.

**Toolbar**

Use the toolbar buttons located at the top of the main view as described below.

**Table 277: Safeguard Desktop Player toolbar**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Back</strong></td>
<td>Displays the previous view. For example, if you clicked play and are in the video view, clicking this button returns you to the recording information view.</td>
</tr>
</tbody>
</table>

  NOTE: When no recording is loaded, there is an additional view that prompts you to drag and drop a recording file onto the player. Once you add the recording file, the recording information view displays.

| **Play Channel** | Plays back the selected sessions recording. |
### Recording navigation

Once the playback window opens you can use the controls at the bottom of the screen or keyboard shortcuts to navigate through the recording.

#### Recording navigation controls

Use the controls at the bottom of the screen to navigate through the sessions recording.

<table>
<thead>
<tr>
<th>Table 278: Navigation controls: Playback mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control</strong></td>
</tr>
<tr>
<td><strong>Timeline</strong></td>
</tr>
<tr>
<td><strong>Play speed</strong></td>
</tr>
<tr>
<td><strong>Skip back</strong></td>
</tr>
<tr>
<td><strong>Play</strong></td>
</tr>
<tr>
<td><strong>Pause</strong></td>
</tr>
</tbody>
</table>
### Control

<table>
<thead>
<tr>
<th>Control</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>✡️ Skip forward</td>
<td>Allows you to jump forward to the next user event in the recording.</td>
</tr>
<tr>
<td>✡️ Closed Captioning</td>
<td>Allows you to display subtitles for the video that list user events as they occurred within the recorded session.</td>
</tr>
<tr>
<td></td>
<td>User events that may appear as subtitles include windows titles, executed commands, mouse activity, and keystrokes.</td>
</tr>
<tr>
<td>✈️ Configure seeker indicators</td>
<td>Allows you to configure the visibility of user event indicators on the timeline. To show a user event indicator move the toggle to the right; to hide a user event indicator move the toggle to the left.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The type of user events that can be included in the timeline depends on the type of session:</td>
</tr>
<tr>
<td></td>
<td>- RDP: Windows titles, keystrokes, mouse activity, and on-screen changes</td>
</tr>
<tr>
<td></td>
<td>- SSH: Commands, keystrokes, and on-screen changes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Control</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scaled video</td>
<td>Allows you to view the recording in a smaller or larger window. Clear this check box to play the video using the original resolution.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The video is rendered at the same resolution as the original session. This setting adjusts the video size based on the size of the viewing screen.</td>
</tr>
</tbody>
</table>

When you are watching a "live" session, the playback navigation controls are replaced with different follow mode navigation controls.

| NOTE: Follow mode is only available to users with Security Policy administrator permissions. |

### Table 279: Navigation controls: Follow mode

<table>
<thead>
<tr>
<th>Control</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminate</td>
<td>Allows you to end the current session you are following.</td>
</tr>
<tr>
<td>Live</td>
<td>Indicates you are following a &quot;live&quot; session.</td>
</tr>
</tbody>
</table>
Keyboard shortcuts

You can also use the following shortcut keys to navigate through the recording.

Table 280: Keyboard shortcuts: Playback mode

<table>
<thead>
<tr>
<th>Shortcut keys</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPACE</td>
<td>Play/pause recording</td>
</tr>
<tr>
<td>Ctrl+Z</td>
<td>Enable video scaling</td>
</tr>
<tr>
<td>f</td>
<td>Toggle full screen replay</td>
</tr>
<tr>
<td>[</td>
<td>Decrease replay speed</td>
</tr>
<tr>
<td>]</td>
<td>Increase replay speed</td>
</tr>
<tr>
<td>=</td>
<td>Reset replay speed</td>
</tr>
<tr>
<td>Shift + Left Arrow</td>
<td>Jump backwards - short</td>
</tr>
<tr>
<td>Alt + Left Arrow</td>
<td>Jump backwards - medium</td>
</tr>
<tr>
<td>Ctrl + Left Arrow</td>
<td>Jump backwards - long</td>
</tr>
<tr>
<td>Shift + Right Arrow</td>
<td>Jump forward - short</td>
</tr>
<tr>
<td>Alt + Right Arrow</td>
<td>Jump forward - medium</td>
</tr>
<tr>
<td>Ctrl + Right Arrow</td>
<td>Jump forward - long</td>
</tr>
</tbody>
</table>

Exporting video

Use the Export Video button at the top of the Safeguard Desktop Player to export the sessions recording file as a video file (WEBM format). This WEBM file can then be played back using any standard video player, such as the one available with Firefox or Google Chrome.

To export a video

1. In the Safeguard Desktop Player, click (or tap) Export Video.
   The Export screen appears, displaying the name of the video file and the size of the file.

2. If you want to include user event subtitles with the exported file, select the Subtitle check box in the upper left corner of the screen.

3. Click (or tap) the browse button (…) in the lower right corner of the screen to specify the location where the file is to be stored.
   The specified location appears in the Export to field.
4. Click the **Export** button.
   An Export Successful message appears.

**Key descriptions**

Expanding a channel in the **Channels** pane of the Safeguard Desktop Player displays additional details about the recording. The keys displayed depends on the type of channel selected. The keys marked with an asterisk (*) may provide you some additional insight into the recording; most of the other keys are internal values.

**Table 281: Safeguard Desktop Player: Key descriptions**

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth_method</td>
<td>Authentication method used.</td>
</tr>
<tr>
<td>bpp</td>
<td>Color depth (bits-per-pixel) of the remote machine.</td>
</tr>
<tr>
<td>channel_id</td>
<td>Internal identifier assigned to the channel being recorded.</td>
</tr>
<tr>
<td>channel_name</td>
<td>Internal name assigned to the channel being recorded.</td>
</tr>
<tr>
<td>channel_policy</td>
<td>Internal name assigned to the channel policy being used.</td>
</tr>
<tr>
<td>channel_type</td>
<td>Type of channel: SSH or RDP</td>
</tr>
<tr>
<td>client_address*</td>
<td>Address of the client computer.</td>
</tr>
<tr>
<td>client_address.ip</td>
<td>IP address of the client computer.</td>
</tr>
<tr>
<td>client_address.port</td>
<td>Port used by the client computer.</td>
</tr>
<tr>
<td>client_id</td>
<td>Internal identifier assigned to the client computer.</td>
</tr>
<tr>
<td>client_x509_subject</td>
<td>Client certificate subject.</td>
</tr>
<tr>
<td>connection</td>
<td>Internal connection policy being used.</td>
</tr>
<tr>
<td>connection_id</td>
<td>Internal connection identifier assigned to the recording.</td>
</tr>
<tr>
<td>data_received</td>
<td>Data received flag: True</td>
</tr>
<tr>
<td>data_sent</td>
<td>Data sent flag: True</td>
</tr>
<tr>
<td>dst_ip</td>
<td>IP address of the session recording module.</td>
</tr>
<tr>
<td>duration*</td>
<td>Duration of the recording.</td>
</tr>
<tr>
<td>duration_raw</td>
<td>Raw duration of the recording (should be the same as the duration).</td>
</tr>
<tr>
<td>exit_status</td>
<td>Exit status of the program run on the remote server.</td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>height_rows*</td>
<td>Number of rows shown in the SSH terminal.</td>
</tr>
<tr>
<td>initiator</td>
<td>Who initiated the connection: Client</td>
</tr>
<tr>
<td>is_processable</td>
<td>Indicates if the session can be processed: True</td>
</tr>
<tr>
<td>local_ip</td>
<td>IP address of the session module.</td>
</tr>
<tr>
<td>protocol*</td>
<td>Protocol used: SSH or RDP</td>
</tr>
<tr>
<td>remote_username*</td>
<td>Name of the user name that log into the remote machine.</td>
</tr>
<tr>
<td>server_address*</td>
<td>Address and port of the remote machine.</td>
</tr>
<tr>
<td>server_address.ip</td>
<td>IP address of the remote machine.</td>
</tr>
<tr>
<td>server_address.port</td>
<td>Port used to connect to the remote machine.</td>
</tr>
<tr>
<td>server_id</td>
<td>Internal identifier assigned to the remote machine.</td>
</tr>
<tr>
<td>server_ip</td>
<td>IP address of the remote machine.</td>
</tr>
<tr>
<td>session_end</td>
<td>Time (in milliseconds) when the session ended.</td>
</tr>
<tr>
<td>session_id</td>
<td>Internal session ID assigned to the session.</td>
</tr>
<tr>
<td>session_start</td>
<td>Time (in milliseconds) when the session started.</td>
</tr>
<tr>
<td>Signature</td>
<td>Validity of the Session Recording Signing certificate.</td>
</tr>
<tr>
<td>source</td>
<td>Source protocol: SSH or RDP</td>
</tr>
<tr>
<td>stream_type</td>
<td>Internal type assigned to the recording stream.</td>
</tr>
<tr>
<td>term</td>
<td>Type of SSH terminal.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Validity of the Timestamping Authority certificate.</td>
</tr>
<tr>
<td>username</td>
<td>Name of the user that authenticated to the remote machine.</td>
</tr>
<tr>
<td>width_cols</td>
<td>Width (in columns) of the original SSH session screen.</td>
</tr>
<tr>
<td>width_pix*</td>
<td>Width (in pixels) of the original SSH session screen.</td>
</tr>
<tr>
<td>width*</td>
<td>Screen width of the RDP session.</td>
</tr>
</tbody>
</table>
About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product
A
access API 475
Access Config tab 221
access historical information 479
Access Key, about 150
access request broker 319
Access Request Policies tab
   account 98
   account group 115
   asset 133
   asset group 169
   entitlement 207
access request policy
   access settings 221
   add account 124
   approver settings 218
   assign accounts and assets 216
   emergency access 224
   requester settings 217
   reviewer settings 220
   session access settings 222
   time restrictions 224
Access Request Policy dialog
   Access Config tab 221
   Approver tab 218
   Emergency tab 224
   General tab 215
   Requester tab 217
   Reviewer tab 220
   Scope tab 216
   Session Settings tab 222
   Time Restrictions tab 224
Access Request settings 246
   Enable or Disable Services 247
   Reasons 249
access request states 495
access request workflow 69
access requests
   enable for service account 140, 182
   enable or disable services 247
   view details 49
Access Requests dashboard
   about 48
   view details 49
account
   about 95
   Access Request Policies tab 98
   Account Groups tab 99
   add 103, 123
   add cloud platform account 104
   add dependent account to a Windows server 154
   add to access request policy 98
   add to account group 99, 106, 114, 123, 134
   add to directory 182, 194
   add to profile 241
   associate with asset 131, 153
   associated asset 97
   change password 107
   Check and Change Log tab 99
   check and set password 110
create 242
directory 193
General tab 96
History tab 100
manually add tag 106
modify 107
remove 108
unlock 389
account dependencies
about 153
add to Windows servers 154
Account Dependencies tab
asset 132
account discovery
add setting 267-268
copy setting 267
delete setting 267
how to setup 491
modify setting 267
account discovery rule
add 269
account discovery setting
about 267
add to profile 240
account group
about 113
Access Request Policies tab 115
Accounts tab 114
add 107, 118
add a dynamic group 118
add account 106, 123
add to policy 124
General tab 114
History tab 116
History tab membership
operation 101, 117, 209, 236,
374, 395
modify 124
remove 125
Account Groups tab
account 99
account password
change 111
check 111
set 111
account password rules
about 341
add 341-342
add to profile 240
copy 341
delete 341
modify 341
Accounts tab
account group 114
asset 131
directory 181
ACF - Mainframe systems
prepare for Safeguard 435
activate read-only appliance 407
Activity Center
about 50
apply search criteria 51
audit request workflow 57
delete saved search 56
delete scheduled report 56
edit saved search 56
edit scheduled report 56
generate report 54
query builder 51
save search criteria 53
schedule report  55
activity events
  filtering report results  59
  view details  57
activity log data
  export  101
add
  account  96, 103
  account dependency to Windows severs  154
  account discovery rule  269
  account discovery setting  267-268
  account group  107, 113
  account groups  118
  account password rules  342
  account to access request policy  124
  account to account group  106
  account to asset  153
  account to directory profile  202
  accounts to account groups  123
  application registration  321
asset  127, 136
  asset group  167, 171
  asset or account to partition profile  242
  asset to asset group  154
  asset to partition  238
audit log signing certificate  300
cloud platform account  104
directory  178, 188
directory account  182
directory account password rule  349
directory accounts to a directory  193
directory group  397
directory user  382
dynamic account group  118
dynamic asset group  172
dynamic asset or asset account tag  279
entitlement  205, 210
external federation provider trust  480
external federation user account  482
license  259
managed network  315
partition  230, 237
password reset schedule  345
password reset schedule, directory accounts  351
password sync group  355
password validation schedule
  accounts  347
  directory accounts  353
secondary authentication service provider  330-331
sessions certificate  304
tag for dynamically tagging directory accounts  272
trusted certificate  309
user  368, 375
  user group  391, 396
  user group to entitlement  213
  user group to role  398
  user to entitlement  213
  user to role  385
  user to user group  398
Administrative Tools  61
administrator
  permissions  421
administrator permissions
  Appliance administrator  421
  Asset administrator  423
Auditor administrator 425
Authorizer administrator 426
Directory administrator 427
Help Desk administrator 429
Operations administrator 429
Security Policy administrator 430
User administrator 432
Administrator widget about 461
Amazon Web Services platforms prepare for Safeguard 436
API
access 475
customize response 477
EventSubscribers 327
query filtering 477
API key
regenerate for Application to Application service 323
appliance activate 407
add license 259
add to cluster 403
appliance name, set 253
Appliance settings 250
assign SSL certificate 309
backup and restore cluster 411
diagnose cluster 408
enroll replica into cluster 403
factory reset 258, 413
LCD controls 459
LDD status messages 458
Lights Out Management (BMC) 260
modify network suffixes 262
monitor cluster health 312
networking settings 261
patch cluster members 409
remove from cluster 404
reset cluster 412
restart 254, 458, 465
shut down 253, 466
specifications 27
states 416
time 264
unjoin from cluster 404
update license 260
view information about 251
Appliance administrator permissions 421
appliance configuration
about 317
DNS 484
IP address 484
NTP server 264, 484
Appliance Information
restart appliance 254
settings 251
shut down appliance 253
Appliance settings 250
application registration
add 321
delete 322
Application to Application
about 319
add registration 321
delete registration 322
regenerate API key 323
setting up 499
settings 318
Application to Application service
check status 319
disable service 258
enable 319
enable service 258
make request to 499
apply search criteria to a activity audit log 51
Approval Anywhere
configure 323
approve password release request 78
approve session access request 86
Approver tab 218
archive backup file 296
archive servers 289
configure 290
configure for session recordings 363
delete configuration 290
modify configuration 290
asset
about 126
Access Request Policies tab 133
Account Dependencies tab 132
Accounts tab 131
add 136
add dynamic tag 279
add to asset group 168, 174
add to directory 202
add to directory profile 201
add to partition 243
add to partition profile 241
add to partitions 238
associate account with 131, 153, 155
authentication types 139
copy tag to another partition 287
create 238, 242
delete tag 283
General tab 128
hide asset marked "ignore" 127
History tab 134
ignore 157
import 127
link to profile 152
manage 128, 152
modify 154
modify connection timeout 155
modify tag 284
product (operating system)
not modifiable 138
remove 155
show hidden 127
view tag assignments 288
asset account
add dynamic tag 279
copy tag to another partition 287
delete tag 283
modify tag 284
view tag assignments 288
Asset administrator permissions 423
asset authentication type
access key 142, 150
none 147, 151
password 147
Asset dialog
Connection tab 139
General tab 137
Management tab 138
session access properties 139
asset discovery
about 156
add new job 157
General tab 158
Information tab 159
Rules tab 159
Condition 160
Connection 163
Profile 164
Schedule tab 164
Summary tab 164
directory scan 158
how to setup 490
manage jobs 165
network scan 158
asset group
about 167
Access Request Policies tab 169
add 171
add account to 174
add asset to 154
add dynamic group 172
Assets tab 168
General tab 168
History tab 169
History tab membership operation 135, 170
modify 175
remove 176
view 167
Asset Management settings 266
Assets tab
asset group 168
assign accounts and assets to access request policy 216
assign user to partition 384
Attributes tab 191
Audit Log Management settings 292
Audit Log Signing certificate 299
audit log signing certificates
add 300
create CSR 300
audit request workflow 57
Auditor administrator permissions 425
Authentication tab 376
directory user 382
Authorizer administrator permissions 426
backup
about 289
archive 293
archive backup file 296
clustered appliance 411
configure archive server 290
create 293-294
delete 293
download 293, 295
information 292
restore 141, 293, 296
run now 293
schedule 294
upload 293, 295
Backup and Retention settings 288
Archive Servers 289
Audit Log Management 292
Safeguard Backup and Restore 292
Safeguard Backup Retention 297
backup retention setting
enable 297
baseboard management console (BMC) 261
Best Practice

Add service accounts to profiles set to never change passwords 140

Add User Groups as approvers or reviewers rather than individuals 219-220

After changing a user's administrative permissions, close the user's connections to the appliance 387

Disable directory users instead of deleting 387

Keep a minimum number of backups on the appliance 293

Perform backups more frequently than the Maximum Password Age setting 294

Setup an NTP server to eliminate system time issues 489

bootstrap admin password reset 466

C

cancel pending session access request 85

Cannot 454

certificate settings 297

Certificate Signing Request 301

create for audit logs 300

create for sessions 305

SSL certificate 308

certificate support for TELNET 436, 440, 443, 448

certificates

about 298

Audit Log Signing 299

chain of trust 487

CSRs 301

how to prevent messages when making RDP connections 485

install audit log signing certificates 300

install sessions certificates 304

RDP Connection Signing Certificate 299, 302

Session Recording Signing Certificate 299, 302

Timestamping Authority Certificate 299, 302

change password 107

change password management

disable 248

enable 248

change password setting

about 344

add to profile 239

copy 344

delete 344

modify 344

Check and Change Log tab

account 99

check asset connectivity

about 151

check directory connectivity

about 193

check password management

disable 248

enable 248

check password setting

about 346

add to profile 239

copy 347

delete 347

modify 347
Cisco devices
  prepare for Safeguard 436
Clipboard channel 510
cloud platform account
  add to Safeguard 104
cluster
  about 401
  add appliance 403
  appliance details 312
  backup and restore 411
  diagnose 408
  enroll replica appliance 403
  failover to replica 406
  monitor health 312
  patch 409
  promote replica to primary 406
  remove quarantined appliance 497
  remove replica appliance 404
  reset 412
  settings 310
  troubleshooting tips 415
  unjoin replica appliance 404
  unlock 415
Cluster Management settings 310
cluster member
  about cluster patching 410
  Activate 405
  Check Health 405
  Diagnose 405
  Failover 405
  patch 409
  Unjoin 405
Cluster monitoring page 310
cluster patching
  failure scenarios 410
  service guarantees 410
Cluster settings
  Cluster Management 310
  Managed Networks 314
Cluster view pane 311
configure alerts 72
configure assets for Safeguard 434
configure Privileged Sessions 497
Connection tab 139
contact information
  change personal information 44
Contact Information tab 378
copy
  account discovery setting 267
  account password rule 341
  asset or asset account tag to another partition 287
  change password setting 344
  check password setting 347
  directory account password rule 348
  directory account tag to another directory 277
  directory change password setting 351
  directory check password setting 353
  SNMP subscription 333
  syslog server configuration 336
create relying party trust in IdP-STS 481
credential retrieval 319

D
default email notifications 504
delete
  account 96
  account discovery setting 267
account group 113
account password rule 341
application registration 322
archive server configuration 290
asset 127
asset group 167, 176
asset or asset account tag 283
change password setting 344
check password setting 347
directory 178
directory account 182
directory account password rule 348
directory account tag 274
directory change password setting 351
directory check password setting 353
entitlement 205, 228
external federation service provider configuration 329
managed network 316
partition 230
password sync group 355
saved search 56
scheduled activity audit log report 56
secondary authentication service provider configuration 331
SNMP subscription 333
Syslog server configuration 336
ticketing system 338
user 368
user group 391
dependent accounts
  about 153
dependent system updates 153
desktop client
  application settings 43
install 35
start 36
system requirements 29
uninstall 36
diagnostic tests
  about 254
  clustered appliance 408
  nslookup 256
  ping 255
  show routes 257
  Telnet 257
  trace route 256
directories that can be searched 31
directory
  about 177
  Accounts tab 181
  add 188
  add assets 202
  add directory group 397
  change description 202
  default profile 201
  Discovered Accounts tab 185
  General tab 179
  History tab 186
  History tab membership operation 187
  modify 202
  Profiles tab 183
  remove 203
  Sync Now 178
directory account
  about 193
  add dynamic tag 272
  add to directory 182, 194
  copy tag to another directory 277
delete tag 274
delete 182
modify tag 275
view tag assignments 278
directory account discovery
  how to setup 492
Directory Account Discovery dialog
  General tab 195
  Rules tab 196
directory account discovery job
  add 195
  edit 182
directory account discovery rule 196
directory account password reset
  schedule 351
directory account password rules
  about 348
  add 349
  apply to directory accounts 200
  copy 348
  delete 348
  modify 348
Directory administrator permissions 427
directory attributes, mapping 191
directory change password setting
  about 350
  add to profile 200
  copy 351
  delete 351
  modify 351
directory check password setting
  about 352
  add to profile 200
  copy 353
  delete 353
modify 353
Directory dialog
  Attributes tab 191
  General tab 189
directory profile
  add account 202
directory scan for assets 158
Directory Tags setting 271
directory user
  add 382
directory user authentication 382
disable
  change password management 248
  check password management 248
  password requests 248
  session requests 247
  toast notifications 72
disaster recovery
  about 401
  diagnose cluster members 405
  enroll cluster members 401
  maintain cluster members 405
  troubleshooting tips 415
  unjoin cluster members 401
discovered accounts 185, 235
Discovered Accounts tab
  directory 185
  partition 235
discovery
  about 489
  account 267, 491
  asset 156-157, 165, 490
  run now 165
directory account 195, 492
Domain Name System (DNS)  484

download Safeguard federation metadata  329

Drawing channel  510
dynamic account group  add  118

Dynamic Account Group dialog
  Asset Account Rules tab  119
  Directory Account Rules tab  121
  General tab  119
  Summary tab  122

dynamic asset group  add  172

Dynamic Asset Group dialog
  Asset Rules tab  173
  General tab  172
  Summary tab  174
dynamic tag  add to assets or asset accounts  279

emergency access
  about  224
  Emergency tab  224

enable
  change password management  248
  check password management  248
  Lights Out Management  261
  password requests  248
  session requests  247
  toast notifications  43, 72

Enable or Disable Services settings  247, 258

enroll cluster member  401

entitlement
  about  204
  Access Request Policies tab  207
  add  210
  add from Entitlements dialog  385, 399
  add policy  227
  add user  206, 213, 227
  add user group  213, 393, 398
  change priority  212
  delete  228
  expired  204

General tab  205

History tab  208

membership  213, 385

modify  227

modify priority  227

modify time restrictions  227

Policies tab  207

priority  211

time restrictions  212

Users tab  206

edit saved search  56

edit scheduled activity audit log report  56

email
  administrative permissions
determine what emails are sent  504

configure notifications  327

configure Safeguard to receive notifications  73

configure SMTP server  325
default events sent  504

modify templates  328

template macros  328

E

Emergency tab  224

Enable or Disable Services settings  247, 258

enroll cluster member  401

entitlement
  about  204
  Access Request Policies tab  207
  add  210
  add from Entitlements dialog  385, 399
  add policy  227
  add user  206, 213, 227
  add user group  213, 393, 398
  change priority  212
  delete  228
  expired  204

General tab  205

History tab  208

membership  213, 385

modify  227

modify priority  227

modify time restrictions  227

Policies tab  207

priority  211

time restrictions  212

Users tab  206

edit saved search  56

edit scheduled activity audit log report  56

email
  administrative permissions
determine what emails are sent  504

configure notifications  327

configure Safeguard to receive notifications  73

configure SMTP server  325
default events sent  504

modify templates  328

template macros  328

E
Entitlement dialog
   General tab 210
   Time Restrictions tab 212
entitlement report
   filtering report results 59
Entitlements tab
   user 371
   user group 393
export 101
   action bar option 55, 60
   video 514
External federation
   add external federation provider trust 480
   add external federation user account 482
   configure 479
   create relying party trust in IdP-STS 481
external federation service provider
   delete configuration 329
   modify configuration 329
External Integration settings 317
   Application to Application 318
   Approval Anywhere 323
   Email 325
   External Federation 479
   SNMP 333
   Starling 334
   Syslog 336-337
   Ticketing 338
Facebook Hosts
   prepare for Safeguard 437
factory reset 258, 413, 467
FAQ
   How do I access the API 475
   How do I audit transaction activity 478
   How do I configure external federation authentication 479
   How do I customize the response using API query parameters 477
   How do I manage account passwords manually 483
   How do I modify the appliance configuration settings 484
   How do I prevent Safeguard prompt when making RDP connections 485
   How do I require users to log in using secondary authentication 380
   How do I require users to log in using two-factor authentication 377, 383
   How do I see which assets and/or accounts are governed by a profile 489
   How do I set the appliance system time 489
   How do I setup a Starling account 507
   How do I setup account discovery 491
   How do I setup asset discovery 490
   How do I setup directory account discovery 492
   How do I setup discovery jobs 489
   How do Safeguard database servers use SSL 492
   How to I make a request using the
Application to Application service 499
What administrators receive warning email notifications 504
What are the access request states 495
What do I do when an appliance goes into quarantine 496
What is required for One Identity Safeguard for Privileged Sessions 497
What needs to be set up to use Application to Application 499
What role-based email notifications are generated by default 504
When does rules engine run for dynamic grouping and tagging 505
Why did the password change during an open request 506
Why integrate with Starling Two-Factor Authentication 506
favorites
create 70
remove 71
set color 71
federation metadata 479
download 329
download Safeguard federation metadata 480
manually input values 481
filtering report results 59
follow mode, session play back 92
Fortinet FortiOS devices
prepare for Safeguard 438
G
General tab
account 96
account group 114
asset 128
asset group 168
directory 179
entitlement 205
partition 230
user 369
user groups 392
generate
activity audit log report 54
support bundle 468
global access request settings 246
H
Help Desk administrator permissions 429
hide ignored assets 127
historical data
export 101
History tab
account 100
account group 116
asset 134
asset group 169
directory 186
entitlement 208
partition 235
user 373
user group 394
Home page
  about 46
  navigation pane 45
  widgets 46
HP iLO Management Processors
  prepare for Safeguard 439
HP iLO servers
  prepare for Safeguard 439

I
IBM i (AS/400) systems
  prepare for Safeguard 439
IdP-STS 479
  create relying party trust 481
iDRAC devices
  prepare for Safeguard 437
ignore asset 157
import
  about 108, 156, 388
  accounts 96
  assets 127
  create import file 109
  CSV Template Assistant 109
  file format 109
  how to import objects 108, 156, 388
  users 368
install
  audit log signing certificate 300
  desktop client 35
  patch 266
  sessions certificate 304
  SSL certificate 307
  update file 266
integrate with Safeguard
  external ticket system 338

Starling Two-Factor Authentication 506

J
join to Starling 334
JunOS servers
  prepare for Safeguard 440

L
launch
  RDP session 88
  Safeguard Desktop Player 91
  SSH client 87
LCD
  controls 459
  status messages 458
license
  add 259
  settings 259
  update 260
licensing 33
Lights Out Management (BMC)
  enable 261
  settings 260
Linked Accounts tab
  users 372
live session
  follow 92
  terminate 92
Location tab 379
login control
  configure 357
Login Notification setting 339
M
make a request to the Application to Application service 499
manage accounts passwords manually 483
manage asset 128, 157
managed network
  add 315
  delete 316
  modify configuration settings 315
  resolve IP address 316
Managed Networks
  settings 314
Management tab 138
member
  add to entitlement 213, 385
  add to user group 370, 383, 398
Message of the Day setting 340
Messaging settings 339
MIIBSNMP
  configure subscriptions 333
Microsoft SQL Servers
  prepare for Safeguard 446
  SSL support 493
minimum required permissions for Windows assets 450
modify
  account discovery setting 267
  account group membership 124
  account information 107
  account password rule 341
  archive server configuration 290
  asset group information 175
  asset or asset account tag 284
  change password setting 344
  check password setting 347
  directory account discovery job 182
  directory account password rule 348
  directory account tag 275
  directory change password setting 351
  directory check password setting 353
  email template 328
  external federation service provider configuration 329
  managed network 315
  network suffixes 262
  password sync group 355
  secondary authentication service provider configuration 331
  SNMP subscription 333
  syslog server configuration 336
  ticketing system 338
  user password rules 360
MongoDB
  prepare for Safeguard 440
MySQL servers
  prepare for Safeguard 441
  SSL support 493
N
navigation
  recording 512
  network diagnostic tools 250
  Network Interface X0 properties 261
  Network Interface X1 properties 263
  network scan for assets 158
  Network Time Protocol (NTP)
    enable 264, 484
  Networking settings 261
nslookup 256

O
ODBC Transport 492
Operations administrator permissions 429
Oracle databases
  prepare for Safeguard 441
Other (or Other Linux) operating system
  about 138, 155, 157

P
Palo Alto Networks
  prepare for Safeguard 441
partition
  about 229
  add 237, 384
  add asset 238
  add assets 243
  assign asset 152
  change description 243
  default profile 241
  delegate management of 237, 243, 371
  delete assets from 151, 238-239
  Discovered Accounts tab 235
  General tab 230
  History tab 235
  modify 243
  Profile tab 232
  remove 243
  Scope tab 230-231
  set default 243-244
partition profiles
  add assets or accounts 242
Partitions tab
  user 371
password
  change 44
  change password manually 345
  check and set 110
  partition profile 137
  policy, add to role 214
  policy, modify 226
  request, how to prevent 103
  reset 389
  viewing Password Archive 112
Password Archive
  viewing 112
  password check and change did not run 462
password Check and Change Log
  view 100
password management services 247
password release
  check-in 76
  checkout 76
password release request 73
  approval 78
  cancel pending request 77
  check-in 76
  checkout 76
  disable 248
  enable 248
  remove request 77
  resubmit request 77
  review 79
  workflow 73
password sync group
  add 355
change sync group password 355
delete 355
modify 355-356
priority 354, 356
password validation schedule
   add 347
patch cluster members 409
permissions
   about 421
   Appliance administrator 421
   Asset administrator 423
   Auditor administrator 425
   Authorizer administrator 426
deleated partition owner 384
Directory administrator 427
Help Desk administrator 429
Operations administrator 429
Security Policy administrator 430
User administrator 432
Permissions tab 379
photo
   change 44
ping 255
platforms that can be managed 31
play back recorded session 91
player 509
Policies tab
   account 98
   account group 115
   asset 133
   entitlement 207
policy
   about 214
   add accounts to scope 115, 169
   add to role 207, 214
change priority 212
copy 226
edit 226
expired 204
priority 215
reason codes 249
remove 225
time restrictions 212
view details 226
PostgreSQL
   prepare for Safeguard 442
prepare asset for management 434
   ACF - Mainframe systems 435
Amazon Web Services platforms 436
Cisco devices 436
Dell iDRAC devices 437
ESXi Hosts 437
F5 Big-IP devices 438
Facebook Hosts 437
Fortient FortiOS devices 438
HP iLO Management Processors 439
HP iLO servers 439
IBM i (AS/400) systems 439
JunOS - Juniper Networks
   servers 440
MongoDB 440
MySQL servers 441
Oracle databases 441
PAN-OS Networks 441
PostgreSQL 442
RACF - Mainframe systems 442
SAP HANA 443
SAP Netweaver Application
   Servers 444
SonicOS devices 445
SonicWALL SMA or CMS appliances 445
SQL Server 446
Sybase (Adaptive Server Enterprise) servers 445
Topic Secret - Mainframe systems 447
Unix-based systems 448
Windows systems 449
prevent Safeguard prompts when making RDP connections 485
priority
about 211
change entitlement priority 212
change policy priority 212
entitlement 211
policy 215
Privilege Elevation Command 143, 146, 148
Privileged Sessions
required configuration 497
product licensing 33
profile
about 184, 233
add account to directory profile 202
add asset or account to partition profile 242
add to directory 183
add to partition 232
assign to asset 152
explicit association 184, 234
implicit association 184, 234
reset default profile 184, 234
Profile settings 340
Account Password Rules 341
Change Password 344
Check Password 346
Directory Account Password Rules 348
Directory Change Password 350
Directory Check Password 352
profile, directory
about 183, 199
add 199
add assets 201
modify 201-202
set as default 201
profile, partition
about 232
add 239
add accounts 241
add assets 241
modify 241, 243
set as default 241
Profiles tab
directory 183
partition 232
property constraint search option 196
Proxy Server X0 properties 262
Q
quarantined appliance 496
R
RACF - Mainframe systems
prepare for Safeguard 442
RDP connection prompts 485
RDP Connection Signing certificate 299, 302
RDP session
launch 88
read-only appliance
  activate 407
reason codes 249
recording navigation 512
recover a quarantined appliance 496
recovery kiosk 462
  appliance information 464
  factory reset 467
  generate support bundle 468
  reboot appliance 465
  reset bootstrap admin password 466
  shutdown appliance 466
regenerate API key 323
remove
  asset group 176
  quarantined appliance from a cluster 497
  session access request 85
  trusted certificate 310
replay recorded session 91
replica
  add 403
  enroll into cluster 403
  failover to replica 406
  promote to primary 406
  remove 404
  unjoin 404
Reports
  about 60
  run entitlement report 60
request password release 73
request workflow
  audit 57
  dialog 91
  password release requests 73
Requester tab 217
reset bootstrap admin password 466
reset cluster 412
reset to default certificate 306
resolve IP address in managed networks 316
restart appliance 254, 465
restore
  backup file 141, 296
  clustered appliance 411
review
  password release request 79
  session access request 90
Reviewer tab 220
role-based access control 421
role-based email notifications 504
Rules tab 196
run asset discovery job 165
run entitlement report 60
run in the system tray 43

S
Safeguard
  features 20
  new features in 2.1.0 22, 24, 26
  set up 37
Safeguard Access settings 357
  Login Control 357
  User Password Rules 360
Safeguard Desktop Player 509
  channels 510
  export video 514
  key descriptions 515
  navigation 512
SAP HANA
prepare for Safeguard 443
SAP Netweaver Application Servers
prepare for Safeguard 444
save search criteria 53
schedule
activity audit log report 55
asset discovery 164
auto account password reset 345
auto account password validation 347
auto directory account password reset 351
auto directory account password validation 353
backup, how to 294
scope
add assets or accounts to partition 238
Scope tab
partition 230-231
search box
using 66
secondary authentication
about 380
enable 377, 383
login 36
settings 330-331
secondary authentication service provider
delete configuration 331
modify configuration 331
Secret Key, about 150
Security Policy administrator permissions 430
separation of duties 37
server
archive, configure 290
service account 95
about 140
set as managed account 140
session access properties 139
session access request 81
approve 86
cancel pending request 85
check-in session 84
launch RDP session 88
launch session 84
launch SSH client 87
remove 85
resubmit request 86
review 90
revoke 87
session recording
about 80
follow mode 92
navigation controls 512
play back 91
Session Recording Signing Certificate 299, 302
session request workflow 79
session requests
disable 247
enable 247
Session SCP channel 510
Session Settings tab 222
Session SFTP channel 510
Session shell channel 510
sessions
about 80
about certificates 299, 302
sessions certificates
about 299, 302
add 304
create CSR 305
reset to default certificate 306
Sessions Module settings 364
Sessions settings 362
Session Recording Storage Management 363
Sessions Module 364
SSH Banner 365
SSH Host Key 366
set account password reset schedule 345
set account password validation schedule 347
set appliance name 253
set appliance system time 489
set directory account password validation schedule 353
set password
generate 111, 199, 483
manual 111, 199
settings
Access Request 246
Account Discovery 267
Account Password Rules 341
Appliance 250
Appliance Information 250-251
Application to Application 318
Approval Anywhere 323
Archive Servers 289
Asset Management 266
Audit Log Signing Certificate 299
Audit Log Management 292
Backup and Retention 288
backup settings 294
Certificate Signing Request 301
Certificates 297
Change Password 344
Change Password Management Enabled 248
Check Password 346
Check Password Management Enabled 248
Cluster 310
Cluster Management 310
desktop client application settings 43
Diagnostics 254
Directory Account Password Rules 348
Directory Change Password 350
Directory Check Password 352
Directory Tags 271
Email 325
Enable Backup Retention 297
Enable or Disable Services 247, 258
External Federation 479
External Integration 317
Factory Reset 258
Licensing 259
Lights Out Management (BMC) 260
Login Control 357
Login Notification 339
Managed Networks 314
Message of the Day 340
Messaging 339
Networking 261
Password Requests Enabled 248
Profile 340
Reasons 249
run in the system tray 43
Safeguard Access 357
Safeguard Backup and Restore 292
Safeguard Retention 297
Secondary Authentication 330-331
Session Recording Storage Management 363
Sessions 362
Sessions Certificates 299, 302
Sessions Module 364
SNMP 333
SSH Banner 365
SSH Host Key 366
SSL Certificates 306
Starling 334
Support Bundle 263
Syslog 336-337
Tags 278
Ticketing 338
Time 264
Trusted Certificates 309
User Password Rules 360
setup Safeguard 37
setup Starling account 507
show ignored assets 127
show routes 257
shut down appliance 253
shutdown appliance 466
sign up for Starling One Identity Hybrid service trial account 507
SNMP
    copy subscription 333
delete subscription 333
modify subscription 333
SonicOS devices
    prepare for Safeguard 445
SonicWALL SMA or CMS appliances
    prepare for Safeguard 445
sort entity lists 66
sorting report results 59
Sound channel 510
SSL certificates
    about 306
    assign to appliance 309
    create certificate signing request 308
    install 307
SSL support
    about 492
    Microsoft SQL servers 493
    MySQL servers 493
    Sybase ASE servers 494
Starling join 334
Starling One Identity Hybrid service
    setup account 507
start desktop client 36
support bundle 263, 468
supported platforms 31
Sybase ASE servers
    prepare for Safeguard 445
    SSL support 494
Sync Now 178
syslog 336
    configure 337
copy server configuration 336
delete server configuration 336
modify server configuration 336
system requirements 29
desktop client 29
web client 30

tags
  add dynamic tag for directory accounts 272
copy asset or asset account tag to another partition 287
copy directory account tag to another directory 277
delete asset or asset account tag 283
delete directory account tag 274
manage asset and asset account tags 278
manually adding a tag to an account 106
modify asset or asset account tag 284
modify directory account tag 275
view asset and asset account tag assignments 288
view directory account tag assignments 278
when does rules engine run 505
tasks
  stop 94
  viewing 93
Telnet 257
terminate session play back 92
Test Connection
  about 142
disable UAC to resolve connectivity failures 455
resolve failures 469
ticket system
  integrate with Safeguard 338
ticketing system
  delete 338
  integrate with Safeguard 338
  modify settings 338
time
  current appliance time 264
time restrictions 212
Time Restrictions tab
  Access Request Policy dialog 224
  Entitlement dialog 212
timeout errors causing operations to fail 472
Timestamping Authority Certificate 299, 302
TLS 1.2 setting 251
toast notifications 72
  about 43
toolbar
  Administrative Tools views 63
  main screen 42
Toolbox
  about 93
Topic Secret - Mainframe systems
  prepare for Safeguard 447
trace route 256
troubleshooting
  account is stuck in a pending password change state 462
  account is stuck in a pending password review state 461
  appliance information 464
appliance status 458
cannot add replica to cluster 468
cannot connect to remote machine through SSH or RDP 454
Check Password fails on Unix host 342, 461
Check, Change, or Set failures 455
cluster 415
diagnostic tests 254
domain controller issues 471
error message
  An internal request has timed out 468
  Anti Cross Site Request Forgery token error 454
  cannot play session 455
  no cipher supported 455
  No SSH host key was provided 455
  system was unable to unlock your login keychain 460
  There is no cipher supported by both client and server 470
factory reset 467
How do I access the recovery kiosk 462
How do I close a password request without review 461
How do I download MIB Definitions 333
How do I enable Network Time Protocol (NTP) 264
How do I generate a support bundle 468
How do I make a Safeguard SSL Webserver Certificate 307
How do I move assets from one partition to another 151, 238-239
How do I obtain a new password during an open request 506
How do I reboot the appliance 465
How do I reset the bootstrap admin password 466
How do I set a directory account’s time zone 397
How do I shut down the appliance 466
How do I test a directory’s connectivity 193
How do I test an asset’s connectivity 151
incorrect or insufficient service account privileges 457
incorrect service account credentials 456
incorrect SSH host keys 456
login credentials fail on Unix host 342, 461
networking issues 471
password fails for Unix host 461
Safeguard is not working on Windows-based systems 472
Test Connection fails for admin account on Windows machine not in domain 455
Test Connection failures 455, 469
Test Connection failures on archive servers 469
Test Connection failures on assets that require SSL 470
timeout errors causing operations to fail 472
What do I do if the system services do not restart 468
Why are directory users in wrong time zone 379
Why are my email template macros blank 328
Why can't I checkout an account 462
Why can't I delete an account 461
Why can't my AD user log in 458
Why did Test Connection fail 455, 470-472
Why did the password change fail 108, 140, 455, 458
Why didn't a user receive email notifications 327
Why didn't the automatic password check and change run on schedule 462
Why doesn’t Safeguard automatically Check and Change SSH Keys 144
Why don’t others see the changes I made 63
Why is the bootstrap account locked out of Safeguard 472
Why is the user account locked out of Safeguard 472
Why isn't the password available for checkout 140, 461-462
Why wasn't the Approver (or reviewer) notified 472

troubleshooting tools 250
trusted certificates

   about 309
   add 309
   remove 310

U
uninstall desktop client 36
Unix-based systems
   prepare for Safeguard 448
unjoin
   cluster member 402
unlock account 389
unlock locked cluster 415
update license file 260
update Safeguard appliance 266
updates
   install 266
user
   about 367
   add 368, 375, 398
   add directory users 382
   add from Users selection dialog 213
   add to entitlement 213, 371, 387
   add to group 399
   add to user group 370, 383, 398
   administrator permissions 379
   authentication settings 376
   change authentication provider 386
   change password 44
   change personal contact information 44
   change photo 44
   change time zone 387
delete 368
enable or disable 390
Entitlements tab 371
General tab 369
grant partition ownership 387
History tab 373
import 368
Linked Accounts tab 372
modify 386
modify admin permissions 387
Partitions tab 371
remove 387
reset password 389
User Groups tab 370
view history 387
User administrator permissions 432
User dialog
   Authentication tab 376, 382
   Permissions tab 379
user group
   about 391
   add 384, 396
   add from User Groups selection dialog 213
   add member 370, 383, 392, 398
   add to entitlement 213, 398
   add to role 399
   add user 370, 383, 392, 398-399
   change description 399
   delete 391
   Entitlements tab 393
   General tab 392
   History tab 394
   modify 399
   remove 400
   Users tab 392
User Groups tab
   user 370
user password rule
   about 360
   configure 360
Users tab
   entitlement 206
   user group 392

V
view
   access request details 49
   activity event details 57
asset and asset account tag assignments 288
Check and Change Log 100
directory account tag assignments 278
VMware ESXi Hosts
   prepare for Safeguard 437

W
web client
   about 42
   system requirements 30
widgets
   administrator widget 461
   approvals widget, controls 78, 86
   requests widget, controls 76, 84
   reviews widget, controls 79, 90
Windows systems
   minimum required permissions 450
   prepare for Safeguard 449