One Identity Safeguard 2.1

Evaluation Guide

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.

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

Safeguard Evaluation Guide
Updated - December 2017
Version - 2.1

Contents

1

Introduction

The One Identity Safeguard Evaluation Guide steps you through a self-directed, hands-on demonstration of the core features of Safeguard and will enable you to perform a POC (proof of concept) of its capabilities in your own test lab

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

Feature	Description
Release control	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.
Workflow engine	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.
Discovery	Quickly discover any privileged account or system on your network with host, directory and network-discovery options.
Approval Anywhere	Leveraging One Identity Starling, you can approve or deny any access request anywhere without being on the VPN.
Favorites	Quickly access the passwords that you use the most right from the Home screen.
Always online	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.
RESTful API	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.
Activity Center	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 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.

Feature	Description
Two-factor authentication support	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.
Smartcard support	Authentication of your privileged users can be integrated with Microsoft's Active Directory support for Smartcards or manually uploaded to the Safeguard appliance itself.
Full session audit, recording and replay	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.
Proxy access	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.
Work the way you want	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.
Command detection	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). NOTE: For an RDP session, Safeguard can detect the title of any window that is opened on the desktop during a privileged session.
Indexing	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.
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

Feature	Description
	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: New features and enhancements

Feature/Enhancement	Description
Additional platform support	Safeguard now supports the management of assets on the following additional platforms: • ACF2 - Mainframe r14 and r15 • ACF2 - Mainframe LDAP r14 and r15 • Debian GNU/Linux 9 • ESXi 6.5 • Fedora 26 • Fortinet FortiOS 5.2 and 5.6 • F5 Big-IP 12.1.X and 13.0 • MAC OS X 10.13
Cluster patching	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.
Federated login	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.
Immediate recording archival	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.

Feature/Enhancement	Description
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.
Multi-request	Authorized Safeguard users can now request multiple password releases or sessions in a single request. In addition, these requests can be saved as a "favorite" access request, providing quick access to the request from the user's Home page.
Safeguard Desktop Player enhancements	The new version of the Safeguard Desktop Player includes the following new features: • Ability to display user activity as subtiltes 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. • 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. • Ability to export the sessions recording file, including the user event subtitles, as a video file.
Security Policy Administrator dashboard	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.
Restore/Suspend accounts	Safeguard allows you to suspend Safeguard managed accounts when they are not in use to reduce the vulnerability of password attacks on privileged accounts. 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

Feature/Enhancement	Description
	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.

Setting up Safeguard

By following these procedures you will set up a hierarchy of administrators that ensures your company follows entitlement-based access control, as you step through the process of writing some basic policies.

- Setting up the appliance
- Creating local administrator users
- Configuring external integration settings
- Creating local users
- Adding assets and accounts
- Writing entitlements

NOTE: To streamline your software evaluation, these instructions are not detailed. For a full explanation of the features, refer to the *One Identity Safeguard Administration Guide*.

Setting up the appliance

Follow these steps to set up and configure the One Identity Safeguard 2000 Appliance.

NOTE: Before you start, ensure that you install the Microsoft .NET Framework 4.6 (or greater) on your management host.

Step 1: Prepare for installation

Gather the following items before you start the appliance installation process:

1. Laptop
2. IP address
3. IP subnet mask
4. IP gateway
5. DNS server address

6. NTP server address

   NOTE: If a Safeguard appliance is going to be used for both Privileged Passwords and Privileged Sessions, you need this network interface information for both the appliance and the sessions module.

7. One Identity Safeguard license(s)

   NOTE: One Identity Safeguard ships with the following modules, each requiring a valid license to enable functionality:

   - One Identity Safeguard Privileged Passwords
   - One Identity Safeguard Privileged Sessions

NOTE: If you purchased One Identity Safeguard, the appropriate license file(s) should have been sent to you via email. If you have not received an email or need it to be resent, visit https://support.oneidentity.com/contact-us/licensing. If you need to request a trial key, please send a request to sales@oneidentity.com or call +1-800-306-9329.

Step 2: Rack the appliance

Prior to installing the racks for housing the appliance, refer to the Warnings and precautions appendix in the *One Identity Safeguard Appliance Setup Guide* provided in the box with the hardware equipment.

Step 3: Power on the appliance

Prior to powering up the appliance, see the Standardized warning statements for AC systems appendix in the *One Identity Safeguard Appliance Setup Guide*.

The One Identity Safeguard 2000 Appliance includes dual power supplies for redundant AC power and added reliability.

1. Plug the power cords to the power supply sockets on the appliance back and then connect the cords to AC outlets.

   TIP: As a best practice, connect the two power cords to outlets on different circuits. One Identity recommends using an UPS on all appliances.

2. 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.

   You can use the **Red X** button to shutdown the appliance. Once the Safeguard appliance is booted, press and hold the **Red X** button for four seconds until it displays POWER OFF.

NOTE: If the Safeguard appliance is not yet booted, it may be necessary to press the **Red X** button for up to 13 seconds.

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.

Step 4: Connect the management host to the appliance

IMPORTANT: The appliance can take up to five minutes to boot up. In addition, ping replies have been disabled on the appliance, so you will not be able to ping this secure appliance.

1. Connect an Ethernet cable from the laptop to the **MGMT** port on the back of the appliance.
2. Set the IP address of the laptop to 192.168.1.100, the subnet mask to 255.255.255.0, and no default gateway.

   NOTE: **MGMT**: The port used for a secure first-time configuration of the appliance.

   This IP address is a fixed address that cannot be changed. It will always be available in case the primary interface becomes unavailable.

   MGMT IP address: 192.168.1.105

   NOTE: **X0**: The "primary interface" that connects your appliance to the network.

   You must change the primary interface IP to match your network configuration.

   Default X0 IP: 192.168.0.105

Step 5: Log into Safeguard

1. Open a browser on the laptop and connect to the IP address of the **MGMT** port https://192.168.1.105

   NOTE: If you have problems accessing the configuration interface, check your browser Security Settings or try using an alternate browser.

2. Accept the certificate and continue.

   NOTE: This is only safe when using an Ethernet cable connected directly to the appliance.

3. Log into the Safeguard Web client using the bootstrap administrator account:
   - User name: ***admin***
   - Password: ***Admin123***

NOTE: **Best practice**: To keep your Safeguard appliance secure, change the default password for the bootstrap administrator's account.

To change the password from the web client, click **Settings** in the upper right corner of the screen and select **Change Password**.

4. Configure the primary network interface (X0):
    a. On the **Appliance Configuration** page, configure the following:

NOTE: Click (or tap) the **Edit** icon to modify these settings.

- **Time**: Enable NTP and set the primary NTP server; if desired, set the secondary NTP server, as well. Click (or tap) **Save**.

NOTE: By default, the NTP server is set to pool.ntp.org.

- **Network (X0)**:
    - Enter the appliance's IPv4 and/or IPv6 address information (IP address, Subnet Mask, Gateway)
    - Enter the DNS server address.
    - Optional, enter the DNS suffixes.
    - Click (or tap) **Save**.

NOTE: The **Network Interface (X1)** information must be configured to use One Identity Safeguard for Privileged Sessions. You can configure the **Network Interface (X1)** for the Privileged Sessions module now or later using the Windows desktop client or web client.

Step 6: Connect the appliance to the network

- Connect an Ethernet cable from your primary interface (**X0**) on the appliance to your network.

Step 7: Configure Safeguard

1. Download and install the Safeguard Windows desktop client application from the web client's application settings.

NOTE: You must log into the web client using the bootstrap administrator account from Step 5.

2. Run the desktop client and log in with the configured IPv4 or IPv6 address for the primary interface (**X0**).

NOTE: To log in with an IPv6 address, enter it in square brackets.

3. License one or both of the Safeguard modules using the provided license file(s):
    a. One Identity Safeguard Privileged Passwords
    b. One Identity Safeguard Privileged Sessions

4. Designate an archive server for storing session recordings.

   NOTE: Defining archive server configurations and assigning an archive server to an appliance are done from the desktop's **Administrative Tools** view:

   - Go to **Settings** | **Backup and Retention** | **Archive Servers** to configure archive servers.
   - Go to **Settings** | **Sessions** | **Session Recordings Storage Management** to assign an archive server to an appliance for storing recording files.

Step 8: Backup Safeguard

Immediately after your initial installation of Safeguard, make a backup of your Safeguard appliance.

NOTE: The default backup schedule runs at 22:00 MST, which can be modified rather than manually running a backup.

1. From the Safeguard desktop **Home** page, select **Administrative Tools**.
2. In **Settings**, select **Backup and Retention | Backups**.
3. Click (or tap) **+ Run Now** from the action bar.

Step 9: Update Safeguard

Download the latest update from: https://support.oneidentity.com/one-identity-safeguard/.

1. From the Safeguard desktop **Home** page, select **Administrative Tools**.
2. In **Settings**, select **Appliance | Updates**.
3. 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.

4. Click (or tap) **Install Now** to install the update file immediately.
5. Once you have updated Safeguard, be sure to backup your Safeguard appliance.

Step 10: Add a user with Authorizer administrative permissions

The Authorizer administrator is responsible for granting administrative access to One Identity Safeguard.

1. From the Safeguard desktop **Home** page, select **Administrative Tools**.

   NOTE: This is where you add all the objects you need to write access request policies, such as users, accounts, and assets.

2. In **Administrative Tools**, select **Users**.

3. Click (or tap) **+ Add User** from the action bar and create a Safeguard user with a "local" authentication provider and Authorizer Administrator permissions.

Username	Password	Permissions	Description
AuthorizerAdmin	Test123	Authorizer	The administrator responsible for granting all administrative access to Safeguard.

NOTE: When you choose **Authorizer** permissions, Safeguard also selects **User** and **Help Desk** permissions. These additional settings cannot be cleared.

4. Log out:
   a. In the upper-right corner of the screen, click (or tap) the user avatar.
   b. Select **Log Out**.

Step 11: Change the local security policy

Before One Identity Safeguard can reset local account passwords on Windows systems, you must change the local security policy.

1. From the Windows Start menu, open **Local Security Policy**.
2. Navigate to **Local Policies** | **Security Options**.
3. Disable "User Account Control: Run all administrators in Admin Approval Mode" option.
4. Restart your computer.

Step 12: Enable password authentication (applies to Privileged Sessions module only)

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, enable the following parameter: PasswordAuthentication yes

Creating local administrator users

Once you have successfully installed the desktop client application, you must add the objects you need to write access request policies, such as users, accounts, and assets. If your company practices the principles of separation of duties (SoD), the Authorizer Administrator needs to create the following additional administrators.

NOTE: A user can be assigned more than one set of permissions.

To add local administrator users

1. Log into the Windows desktop client application as *AuthorizerAdmin*.
2. From the **Home** page, navigate to **Administrative Tools** and select **Users**.
3. Add the following additional local administrator users:

Username	Password	Permissions	Description
ApplianceAdmin	Test123	Appliance	The administrator responsible for configuring the appliance.
AssetAdmin	Test123	Asset	The administrator responsible for adding and managing partitions, assets and accounts.
Auditor	Test123	Auditor	The administrator responsible for reviewing all access request activity.
DirectoryAdmin	Test123	Directory	The administrator responsible for managing directory integration, including directory accounts.
PolicyAdmin	Test123	Security Policy	The administrator responsible for defining the entitlements and policies that control which assets and/or accounts a user can access.
UserAdmin	Test123	User	The administrator responsible for managing user accounts.

NOTE: When you choose certain permissions, Safeguard also selects additional permissions. Do not clear these additional settings.

Before you log out, let's see if Safeguard added these users.

To view the audit log

1. From the **Home** page, navigate to the **Activity Center**.
2. Leave the default search criteria (I would like to see all activity occurring within the last 24 hours).
3. Click (or tap) **Run**.

4. Explore the results.

   As the Authorizer Administrator, you can view User Authentication and Object History for Audit Events pertaining to users.

5. Log out.

Configuring external integration settings

First we will log into the desktop client with an Appliance Administrator account (*ApplianceAdmin*) to configure the following external integration settings:

- Secondary authentication
- Email notifications

Then we will log in with a Security Policy Administrator account (*PolicyAdmin*) to configure the Approval Anywhere feature.

Setting up a Starling account

We will be using Starling Two-Factor Authentication as our service provider for secondary authentication and Approval Anywhere. To get started, you must register a new account for the Starling Cloud platform and then you can begin a 30-day trial of Starling Two-Factor Authentication. 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 Two-Factor Authentication trial account

1. Go to https://www.cloud.oneidentity.com/ and register a new account for the Starling Identity as a Service Starling Two-Factor Authentication.
   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.
2. Once logged in, select the **Trial** button under the **Two-Factor Authentication** section.

3. Click **Two-Factor Authentication** to open the Dashboard.
4. Expand the **Subscription key** pane to reveal your subscription key. Copy the key to your clipboard.

Configuring Starling Two-Factor Authentication as a secondary authentication service provider

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 into the Safeguard desktop client.

Now that you have the subscription key for a Starling Two-Factor Authentication instance, the following procedure guides you through the process of adding Starling Two-Factor Authentication as a secondary authentication service provider. Later in the guide, we will step through the process of configuring a user to require two-factor authentication as well as logging in with two-factor authentication.

To configure a secondary authentication service provider

1. Log into the Windows desktop client as *ApplianceAdmin*.
2. From the **Home** page, navigate to **Administrative Tools** and select **Settings**.
3. In **Settings**, select **External Integration | Secondary Authentication**.
4. Click **Add** to add **Starling Two-Factor Authentication** as a secondary authentication service provider and provide the Starling subscription key.

Stay logged in as the *ApplianceAdmin* for setting up email notifications.

Setting up email notifications

To demonstrate how Safeguard sends out event notifications, you must configure Safeguard to automatically send email notifications when certain events occur. For the purposes of this software evaluation, we have you set up a template for Access Request Auto-Approval.

To setup email notifications

1. Navigate to **Administrative Tools** and select **Settings**.
2. In **Settings**, select **External Integration | Email**.

3. To configure the **Email** notifications, enter these settings for all Safeguard emails:

SMTP Server Address	Enter the IP address or FQDN of the mail server. NOTE: If you are using a mail exchanger record (MX record), you must specify the domain name for the mail server.
SMTP Port	Enter the TCP port number for the email service.
Sender Email	Enter your email address.
Require Transport Layer Security	Select this option to require that Safeguard uses TLS to provide communication security over the internet.

To validate your setup

1. Select the **Test Email Settings** link.
2. Enter your email address as the **Send To** email address and click (or tap) **Send**.

   Safeguard sends an email using the configuration settings.

Configuring 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.

To configure Approval Anywhere

1. Log into the desktop client as *PolicyAdmin*.
2. Navigate to **Administrative Tools** and select **Settings**.
3. In **Settings**, select **External Integration | Approval Anywhere**.
4. Click **Configure Now**.
5. Enter the **Starling subscription key**.

NOTE: After we have added local users, we will return to this page to add the Safeguard users authorized to use the Approval Anywhere feature.

Creating local users

Local users do not have any Safeguard administrative permissions. These users can be granted rights to request access, approve access requests, or review completed access requests.

NOTE: You can perform the exercises in this guide with directory users as well as local users. To do that, you must add a directory, the associated directory accounts, and directory users.

To streamline your software evaluation, we recommend that you simply use local users. The access request workflow is the same no matter what users perform them. To make your user experience more realistic, you can set up other local users from your test lab to be a "Requester", "Approver", and "Reviewer" or use the test users we suggest creating below.

To create local users

1. Log into the Windows desktop client as *UserAdmin*.
2. From the **Home** page, navigate to **Administrative Tools** and select **Users**.
3. In **Users**, click (or tap) **+ Add User** from the action bar and add the following Safeguard non-administrator users:

Username	Password	Permissions	Description
Joe	Test123	None	The "Requester user", authorized to request access.
Abe	Test123	None	The "Approver user", authorized to approve access requests. See the following procedure for more information on how to configure Abe for two-factor authentication.
Ralph	Test123	None	The "Reviewer user", authorized to review past (or completed) access requests.
Pete	Test123	None	The delegated partition owner.

To configure a user for two-factor authentication

NOTE: Abe will be authorized to approve access requests.

1. As the *UserAdmin* add a new local user named "Abe".
2. On the Authentication page,
    a. **Authentication Provider**: Select **Local**.
    b. **User Name**: Enter **Abe**.
    c. **Password | Confirm Password**: Enter **Test123**.
    d. **Require Secondary Authentication**: Select this check box.
    e. **Authentication Provider**: Select the **Starling Two-Factor Authentication** service provider you previously defined.
    f. **Use alternate mobile phone number**: Optionally, select this check box and enter an alternate mobile number to be used for two-factor authentication notifications.
3. On the Contact page,
    a. **Mobile Phone**: Enter your mobile phone number.
    b. **Email Address**: Enter a valid email address.
4. Finish adding the local user to Safeguard.
5. Log out of Safeguard.
6. Log in as the *PolicyAdmin* and navigate to **Administrative Tools | Settings | External Integration | Approval Anywhere**.
7. Click **+ Add** to add *Abe* as a user authorized to use the Approval Anywhere feature.
8. Log out of Safeguard.

Adding assets and accounts

Now let's add some systems so that you can see how Safeguard manages them.

To add partitions, assets, and accounts to Safeguard

1. Log in as *AssetAdmin* and navigate to **Administrative Tools**.
2. In **Partitions**, click (or tap) **+ Add Partition** from the action bar to add these partitions:

Partition	Description	Delegated Owner
Linux Servers	The Linux Administrator's workspace.	Pete
Windows Servers	The Windows Administrator's workspace.	none

NOTE: 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.

3. Configure the **Profile** check and change schedules to run daily:
   a. Navigate to **Settings** | **Profile** | **Check Password** (and **Change Password**).
   b. Double-click (or double-tap) each schedule to modify the schedule.
   c. Select **Schedule** and choose the **Day** interval, set the time of day, and leave the daily repeat interval set to 1 day.
4. In **Assets**, add some Linux and Windows servers. Be sure to put them into the appropriate partition.

   NOTE: To observe how Safeguard automatically changes passwords, setup assets from your test lab, with actual network addresses, service accounts, and passwords.

   Run **Test Connection** on the **Connection** tab to ensure that Safeguard can communicate with the asset.

   a. Once you add an asset, go to the **Accounts** tab and add one or more unique accounts for each asset.

      NOTE: These are the accounts Safeguard will use to give people access to the asset.

   b. After you add the account, right-click (or press and hold) the new account to set the password (**Account Security | Set Password**).
5. Log out.

Writing entitlements

Now that we have demonstrated that Safeguard is actually managing your account passwords, let's define some rules for requesting password release and session access requests, such as the maximum duration, how many approvals are required, and so forth.

To write the entitlements that govern access requests

1. Log in as *PolicyAdmin* and navigate to **Administrative Tools**.
2. In **Settings**, select **Access Request | Reasons** and add these access request reason codes:

Reason	Description
SU	Software Updates
Sys Maint	System Maintenance
SSH Session	SSH Session Request
RDP Session	RDP Session Request

3. In **User Groups** add these user groups:

User Groups	Description	User
Approvers	Users authorized to approve password release requests.	Abe
Requesters	Users authorized to request passwords.	Joe
Reviewers	Users authorized to review password release requests.	Ralph

   a. On the **Users** tab, add each user to the specified user group.

4. In **Account Groups**, add the following account groups:

Account Group	Description
Linux Server Accounts	Accounts for the Linux machines
Windows Server Accounts	Accounts for the Windows machines.

   a. On the **Accounts** tab, add the appropriate accounts to each account group.

5. In **Entitlements**, add the following entitlements:

   NOTE: At this time, do not set entitlement time restrictions.

Entitlement	Description
Linux Password Requests	The rules that govern password release requests for the Linux Servers.
Windows Password Requests	The rules that govern password release requests for the Windows Servers.
Sessions Requests	The rules that govern session access requests.

6. Stay logged in as the Security Policy Administrator (*PolicyAdmin*) and proceed to the next exercise.

Now let's add access request policies to each of these entitlements that restrict system access to authorized users.

Adding password release request policies

We now need to define the users who are authorized to make password release requests and add access request policies to define the scope (accounts that can be accessed) and rules for checking out passwords.

To add a policy to the Linux Password Requests Entitlement

1. As *PolicyAdmin* navigate to **Administrative Tools | Entitlements** .
2. Select the **Linux Password Requests Entitlement**.
3. On the **Users** tab, add the *Requesters* user group as the "user" for this entitlement.

   An entitlement "User" is a person who is authorized to request passwords to accounts governed by the polices in the entitlement.
4. On the **Access Request Policies** tab, create the following access request policy:
   a. **General** tab:
      - Policy Name: *Linux Servers Password Release Request Policy*
      - Description: *The rules that define the request, approval, and review of password release requests for the Linux Server Accounts.*
      - Access Type: **Password Release**

   b. **Scope** tab:
      - *Linux Server Accounts* group

   c. **Requester** tab:
      - Select the following reasons: **SU** and **Sys Maint**
      - Require a Reason.
      - Require a Comment.
      - Select the **Allow Requester to Change Duration** option.

   d. **Approver** tab:
      - Require one person from the *Approvers* user group to approve a password release request.

   e. **Reviewer** tab:
      - Require one person from the *Reviewers* user group to review a completed password release.

   f. **Access Config** tab
      - Select the **Change password after check-in** option.

g. **Time Restrictions** tab:
   - Do not set policy Time Restrictions.

h. **Emergency** tab:
   - Enable Emergency Access.

To add a policy to the Windows Password Requests Entitlement

1. As *PolicyAdmin* navigate to **Administrative Tools | Entitlements** .
2. Select the **Windows Password Requests Entitlement**.
3. On the **Users** tab, add the *Requesters* user group as the "user" for this entitlement.

   An entitlement "User" is a person who is authorized to request passwords to accounts governed by the polices in the entitlement.
4. On the **Access Request Policies** tab, create the following access request policy:
   a. **General** tab:
      - Policy Name: *Weekday Maintenance Policy*
      - Description: *The rules that define the request, approval, and review of password release requests for the Windows Server Accounts on weekdays.*
      - Access Type: **Password Release**

   b. **Scope** tab:
      - *Windows Server Accounts* group

   c. **Requester** tab:
      - Do not require a Reason.
      - Do not require a Comment.
      - Select the **Allow Requester to Change Duration** option.

   d. **Approver** tab:
      - Require one person from the *Approvers* user group to approve a password release request.

   e. **Reviewer** tab:
      - Require one person from the *Reviewers* user group to review a completed password release.

   f. **Access Config** tab
      - Select the **Change password after check-in** option.

   g. **Time Restrictions** tab:
      - Allow users to access passwords in the scope of this policy anytime Monday through Friday.

   h. **Emergency** tab:
      - Do not Enable Emergency Access.

Adding session request policies

Prior to requesting a session, you must create a session request policy that defines the users who are authorized to access an asset or account. As part of this request policy you will also define the protocol (SSH or RDP) to be used as well as the type of account credentials to be specified to access the asset or account.

To write the policies that govern session requests

1. As *PolicyAdmin* navigate to **Administrative Tools | Entitlements**.
2. Select the **Sessions Requests** entitlement.
3. On the **Users** tab, add the *Requesters* user group as the "user".
4. On the **Access Request Policies** tab, create the following access request policies for the sessions request entitlement:
    a. Create a policy for SSH sessions:

    General tab:

    - Policy Name: *SSH Session Request Policy*
    - Description: *The rules that define the request, approval, and review of session requests using SSH protocol.*
    - Access Type: **SSH**

    Scope tab:

    - *Linux Server Accounts* group

    Requester tab:

    - Select the following reason: **SSH Session**.
    - Require a Reason.
    - Require a Comment.
    - Select the **Allow Requester to Change Duration** option.

    Approver tab:

    - Require one person from the *Approvers* user group to approve a session request.

    Reviewer tab:

    - Require one person from the *Reviewers* user group to review a session release.

    Access Config tab

    - Use the default settings (**None** is selected by default).

    Session Settings tab

    - Select **Record Sessions**.
    - Select **Enable Command Detection**.

- Leave the **SSH Controls** selected:
  - **Allow SFTP**
  - **Allow SCP**
  - **Allow X11 Forwarding**

Time Restrictions tab:

- Do not set policy time restrictions.

Emergency tab:

- Do not enable emergency access.

b. Create a policy for RDP sessions:

General tab:

- Policy Name: *RDP Session Request Policy*
- Description: *The rules that define the request, approval, and review of session requests using RDP protocol.*
- Access Type: **RDP**

Scope tab:

- *Windows Server Accounts* group.

Requester tab:

- Do not select or require a reason.
- Do not require a comment.
- Select the **Allow Requester to Change Duration** option.

Approver tab:

- Select **Auto-approved**.
- Select the **To** button to **Notify when Account is Auto-Approved** and select the Safeguard user to receive the email notification.

Reviewer tab:

- Require one person from the *Reviewers* user group to review a past session release.

Access Config tab:

- Select **User Supplied**.

Session Settings tab:

- Select **Record Sessions**.
- Leave the **RDP In-Session Controls** selected:
  - Allow **Clipboard**

Time Restrictions tab:

- Do not set policy time restrictions.

Emergency tab:

- Do not enable emergency access.

5. Log out.

3

Password release workflow exercises

Now that you have setup One Identity Safeguard, it's time to validate the access request policies you created for password release requests.

Exercise 1: Testing the password release workflow

This exercise demonstrates the password release workflow from request to approval to review.

NOTE: If you setup users from your test lab as a "Requester", "Approver", and "Reviewer" user, have each of them log into a web client using a mobile device. If mobile devices are not available, have your users log into the Safeguard desktop client at their own workstations.

You can also perform these exercises with directory users. To do that, you must add a Directory Administrator to add a directory and the associated directory accounts. The password release workflow is the same no matter what users perform them.

To start the Web application

1. Open a browser and navigate to: **HTTPS://<*Appliance IP Address*>**
2. Start three instances of the web client, logging in as *Joe*, *Abe*, and *Ralph*, respectively.

   NOTE: Alternatively, you can open three browser windows on a single desktop and display them side-by-side to simulate mobile devices. Log into each instance as your "Requester", "Approver", and "Reviewer" users.

To test the password release process

Request password

1. As *Joe*, the "Requester" user.
2. On your **Home** page, select **New Request**.
    - If you have set up a Linux account and a Windows account, request a password from each.
3. Use the default access options.
    - Notice how the policy configuration changes the user experience.
4. Open **Requests** and review your pending request(s).

Approve password requests

NOTE: Did you receive a notification on your mobile phone? You can approve the request from your mobile device without being logged into Safeguard.

If you'd rather approve it using the desktop client proceed to the steps below.

1. As *Abe*, the "Approver" user.

    NOTE: Notice Abe has an additional authentication step to take in order to log into Safeguard. In addition, since we have set up Approval Anywhere you can use the Starling 2FA app on your mobile phone to complete the login process.

2. Open **Approvals** and review the requests waiting for your approval.
3. Select **Approve/Deny** to approve *Joe*'s password requests.

Test the password and check it in

1. As *Joe*.
2. Once the password becomes **Available**, open the requests and select **Show Password** to see the password on your screen.
    - Make note of the password so that you can verify that Safeguard changes it after you use it.
3. Select **Copy**.
4. Using the password in your copy buffer, log into the test server.
5. Log out of the test server and return to the Safeguard desktop.
6. Select **Check-In** to complete the password checkout process for the password requests.

Review a password release

1. As *Ralph*, the "Reviewer" user.
2. Open **Reviews** and review the requests that are waiting for your review.
    a. Select **Workflow** to view the transactions that took place as part of the request.
    b. Select **Review** to enter a comment and complete the review process.

Request emergency access

1. As *Joe*.
2. Request the password for the Linux asset again, this time use the **Emergency Access** option.
    - Notice that the password becomes immediately available. That is because **Emergency access** bypasses the approval.
3. Once the password becomes **Available**, open the password request and select **Show Password**.
    - Is the password different this time? When the **Change Password After Release** option is selected in the policy, Safeguard automatically changes the password after each use.
4. **Copy** the password so you can use it to manually log into the remote asset\account.
5. After you have successfully logged into the remote asset\account, log out of the test server and return to the Safeguard desktop.
6. Select **Check-In**.

Review a password release

1. As *Ralph*.
2. Open **Reviews** and review the requests that are waiting for your review.
3. a. Select **Workflow** to view the transactions that took place as part of the request.
    b. Select **Review** to enter a comment and complete the review process.

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 (*PolicyAdmin*) 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.

Exercise 2: Testing time restrictions

Now that you have seen the end-to-end password release process from request to approval to review, let's demonstrate how the entitlement and policy time restrictions affect a password request.

NOTE:

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.

To test time restrictions

Entitlement time restrictions

1. As *PolicyAdmin*, navigate to **Entitlements**.
2. Navigate to the **General** tab of the *Linux Password Requests* entitlement.
3. Set the entitlement **Time Restrictions** to allow users to access passwords only during their lunch hour Monday through Friday.
4. As *Joe*, assuming that it is currently *not* during your lunch hour, request a password for a Linux account, for a duration of 5 minutes.
    - Did Safeguard allow you to check out this password? The request dialog disables the **Request Immediately** option. The request time will automatically be set for the next unrestricted time frame that allows the account password to be requested.
5. **Cancel** the request (or return to your *Home* page).

Entitlement expiration

1. As *PolicyAdmin*, set the **Time Restrictions** for the *Linux Password Requests* role to 8:00 a.m. - 5:00 p.m. Monday through Friday.
2. While you are in **Time Restrictions**, set this entitlement to expire today in 1 minute from now.

3. Wait for the entitlement to expire.
    - Did you see Safeguard's notification?

      NOTE: If you do not see the notification refresh your screen.
4. As *Joe*, request a password for a Linux account.
    - Notice that the account is not available to check out. Safeguard does not allow you to checkout accounts associated with expired entitlements.
5. As *PolicyAdmin*, remove the expiration time from the **Time Restrictions**, but leave the entitlement Time Restrictions enforced.
6. As *Joe*, request a password for the same Linux account.
    - Observe that you are now allowed to request passwords for the *Linux Password Requests* accounts.
7. **Cancel** the request (or return to your Home page).

Policy time restrictions

1. As *PolicyAdmin*, set the policy **Time Restrictions** for the *Weekday Maintenance Policy* to allow users to access passwords 8:00 a.m. - 5:00 p.m. Monday through Friday.
2. As *Joe*, request a password for the Windows account for Sunday at 2:00 p.m.
    - This request was denied because the *Weekday Maintenance Policy* does not allow you to check out accounts on Sunday.
3. **Cancel** the request (or return to your Home page).

Exercise 3: Testing priorities

To determine which policy to use for a password release, Safeguard considers both entitlement and policy priorities. Safeguard first considers the entitlement priority, then the priorities of policies within that entitlement.

To test priorities

Entitlement priorities

To test entitlement priorities, an account must be governed by two different entitlements.

1. As *PolicyAdmin*, navigate to **Entitlements**.
2. Verify that the *Linux Password Requests* entitlement is priority #1.

   NOTE: Safeguard displays the priority number under the entitlement name.
3. In **Account Groups**, add the Windows account to the *Linux Servers Accounts* group.

4. As *Joe*, request a password for the Windows account, for Sunday at 9:00 a.m.
    - Are **Reasons** and a **Comment** required? If so, then you know that Safeguard used the *Linux Password Requests* entitlement; the *Windows Password Requests* entitlement does not require **Reasons** or **Comments**.
    - Did the **Time Restriction** prevent you from checking out this password? The *Linux Password Requests* entitlement only allows you to checkout passwords Monday through Friday, from 8:00 a.m. to 5:00 p.m.
5. **Cancel** the request.
6. As *PolicyAdmin*, change the priority of these entitlements, making the *Windows Password Requests* priority #1, and run through this test again to see if you get different results.
    - Are **Reasons** and a **Comment** required? If not, then you know that Safeguard used the *Windows Password Requests* entitlement as it does not require **Reasons** or **Comments**.
    - Did the **Time Restriction** prevent you from checking out this password? The *Weekday Maintenance Policy* only allows you to checkout passwords Monday through Friday, from 8:00 a.m. to 5:00 p.m.
7. Before you leave this test, change the priority back and remove the Windows account from the *Linux Servers Accounts* group.

Policy priorities

To test policy priorities, an account must be in the scope of two policies within the same entitlement.

1. Log in as *PolicyAdmin* and navigate to **Administrative Tools**.
2. In **Entitlements**, add this new policy to the *Windows Password Requests* entitlement:

    General tab:
    - Policy Name: *Sunday Maintenance Policy*.
    - Description: *The rules that define the request, approval, and review of password requests for the Windows Server Accounts on Sundays.*
    - Access Type: **Password Release**

    Scope tab:
    - *Windows Server Accounts* group

    Requester tab:
    - Select all Reasons.
    - Require a Reason.
    - Require a Comment.
    - Select the **Allow Requester to Change Duration** option.

Approver tab:

- Require one person to approve a password request, then select the *Abe* account.

Reviewer tab:

- Require one person to review a past password release, then select the *Ralph* account.

Access Config tab:

- Ensure access type is **Password Release**
- Select the **Change password after Check-in** check box.

Time Restrictions tab:

- Allow users to checkout passwords only on Sunday.

Emergency tab:

- Enable Emergency Access.

3. Verify that the *Weekday Maintenance Policy* is priority #1.
4. As *Joe*, request a password for the Windows account, for Sunday at 9:00 a.m.
   - Are you required to add a **Reason** for your password request?

     If not, then you know Safeguard used the *Weekday Maintenance Policy* which does not have **Reasons** or **Comments** enabled.
   - Did the **Time Restrictions** prevent you from checking out this password?

     The *Weekday Maintenance Policy* does not permit you to request a password on Sunday.
5. **Cancel** the request.
6. As *PolicyAdmin*, change the priority of these policies, making the *Sunday Maintenance Policy* priority #1, and run through this test again to see if you get different results.
   - Are you required to add a **Reason** for your password request?

     If so, then you know Safeguard used the *Sunday Maintenance Policy*; the *Weekday Maintenance Policy* does not have **Reasons** or **Comments** enabled.
   - Did the **Time Restrictions** prevent you from checking out this password?

     The *Sunday Maintenance Policy* permits you to request a password on Sunday.
7. Before you leave this test, change the policy priority back.
8. Cancel the request and log out.

Sessions access request exercises

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.

Before you begin:

- Appliance Administrator: Ensure the Privileged Sessions module is licensed (**Settings** | **Licensing** | **Licensing Modules**).
- Appliance Administrator: Ensure the Network Interface X1 is configured (**Settings** | **Appliance** | **Networking**).
- Appliance Administrator: Ensure the session request service is enabled (**Settings** | **Access Request** | **Enable or Disable Services**).
- 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**).
- Security Policy Administrator: Ensure there is an entitlement with an access request policy for both SSH and RDP sessions defined. For more information, see Writing entitlements on page 23.
- 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

These exercises will guide you through a step-by-step evaluation of the Safeguard session request workflow process:

Exercise 1: Testing the SSH session request workflow

This exercise demonstrates the SSH session request workflow from request to approval to review.

To test the SSH session request process

Request session

1. As *Joe*, the "Requester" user.
2. On your **Home** page, select **New Request**.
   - Request an SSH session for a Linux account.
   - Notice how the policy configuration dictates the user experience. For example, you are required to enter a reason and a comment.
3. Open **Requests** and review your pending request.

Approve sessions request

NOTE: Did you receive a notification on your mobile phone? You can approve the request from your mobile device without being logged into Safeguard.

If you'd rather approve it using the desktop client proceed to the steps below.

1. As *Abe*, the "Approver" user.

   NOTE: Notice Abe has an additional authentication step to take in order to log into Safeguard. In addition, since we have set up Approval Anywhere you can use the Starling 2FA app on your mobile phone to complete the login process.

2. Open **Approvals** and review the request waiting for your approval.
3. Select **Approve/Deny** to approve *Joe*'s session request.

Launch the SSH session

1. As *Joe*.
2. Once the session becomes **Available**, open the session request and select ▶ **Launch SSH client**.

   The PuTTy Configuration dialog appears pre-populated with the required information, click (or tap) **Open**.
3. Accept the security certificate to continue.
4. Perform various commands on the test server.

5. Log out of the test server and return to the Safeguard desktop.
6. Select ✓ **Check-In** to complete the checkout process for the sessions request.

Review a completed sessions request

1. As *Ralph*, the "Reviewer" user.
2. Open **Reviews** and review the request that is waiting for your review.
3. Select **Workflow** to view the transactions that took place as part of the request.
    a. Since **Record Sessions** is enabled in the policy, on the Initialize Session event, click ▶ **Play** to replay the session.
    b. Since **Enable Command Detection** is enabled in the policy, on the Initialize Session event, click the **events** link to view a list of the commands and programs run during the session.
4. Select **Review** to complete the review process.

Exercise 2: Testing the RDP session request workflow

This exercise demonstrates the RDP session request workflow from request to approval to review. Since the entitlement's policy specified that you will provide your own credentials, you will need to enter those before you launch the RDP session.

To test the RDP session request process

Request session

1. As *Joe*, the "Requester" user.
2. On your **Home** page, select **New Request**.
    - Request an RDP session for a Windows account.
    - Notice how the policy configuration dictates the user experience. For example, you are not required to enter a reason and a comment for this policy.
3. Open **Requests** and review your pending request.

Approve sessions request

Since the access request policy was set to **Auto-approved**, there is no approval required.

Did you get an email notification of the auto-approved access request?

Launch the RDP session

1. As *Joe*.
2. Once the session becomes **Available**, open the session request.
3. Enter the credentials to be used (user name and password) and click (or tap) **Apply**.

   Clicking **Apply** retrieves the information required to log in: Computer ID and Username Connection String.
4. Select ▶ **Launch RDP**.
5. Accept the security certificate to continue.
6. Run programs (for example, launch a browser and browse the internet) on the test server.
7. Log out of the test server and return to the Safeguard desktop.
8. Select ✓ **Check-In** to complete the checkout process for the sessions request.

Review a completed sessions request

1. As *Ralph*, the "Reviewer" user.
2. Open **Reviews** and review the request that is waiting for your review.
3. Select ☰ **Workflow** to view the transactions that took place as part of the request.
   a. Since **Record Sessions** is enabled in the policy, on the Initialize Session event, click ▶ **Play** to replay the session.
   b. Notice that since **Enable Window Title Detection** is not enabled in the policy, a list of the windows opened on the desktop during the session are not available for review.
4. Select **Review** to complete the review process.

5

Auditing exercises

Now that you have performed some password request activities, you can audit the transaction data.

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.

Safeguard provides several ways to audit transaction activity:

Table 3: Safeguard's auditing tools

Option	Description
Password Archive	Where you access a previous password for an account for a specific date.
Check and Change Log	Where you view an account's password validation and reset history.
History	Where you view the details of each operation that has affected the selected item.
Activity Center	Where you can search for and review any activity for a specific time frame.
Workflow	Where you can audit the transactions performed as part of the workflow process from request to approval to review for a specific access request.
Reports	Where you can view and export entitlement reports that show you which assets and accounts a selected user is authorized to access.

The exercises in this section demonstrate Safeguard's auditing capabilities. But before we start, let's create some password check and change activity.

These exercises will guide you through a step-by-step evaluation of the Safeguard auditing features.

Exercise 1: Creating audit data

By following these steps, you will add some password check and change history to Safeguard's audit log and you will learn how to manually verify and reset account passwords.

To perform password check and change activity

1. Log in as *AssetAdmin* and navigate to **Administrative Tools**.
2. In **Accounts**, select an account.
3. Open the **Account Security** menu from the action bar, and notice the three options: **Check Password**, **Change Password**, and **Set Password** using the **Manual Password** option.

   NOTE: These same options are available from an account's context menu.
4. **Check** the password for the account.

   NOTE: The **Tasks** pane opens when you start a task. You can re-size your desktop client console so that the **Tasks** pane is not covering the **Administrative Tools**.

   The "Check" option verifies the account password is synchronized with the Safeguard database; this action should succeed.

   TIP: If **Check Password** fails, run **Check Asset** from the context menu of the asset to ensure that Safeguard can communicate with it. Then retry the **Check Password** option on the account.
5. Set the password for the account to "*Mypass01*" using the **Manual Password** option.

   The "Manual Password" option manually sets the account password in the Safeguard database; not on the appliance; so now they are not in synch.
6. **Check** the password for the account.

   The "Check" option should fail because the account password is not in synch with the Safeguard database.
7. **Change** the password for the account.

   The "Change" option creates a new account password and synchronizes it on the Safeguard database.

8. **Check** the password for the account again.

   This task should now be successful.

Stay logged in as the *AssetAdmin* for the next exercise.

Exercise 2: Accessing the Password Archive

Password Archive allows you to access a previous password for an account for a specific date.

NOTE: The Password Archive dialog only displays previously assigned password(s) 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. In **Accounts**, select the account you have been working with.
2. Click (or tap) **Password Archive** from the action bar.
3. In the Password Archive dialog, select today's (or a previous) date.

   TIP: If 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 for the specified date.
5. Either **Copy** the password, or click (or tap) **OK** to close the dialog.
6. **Close** Password Archive to return to **Accounts**.

Stay logged in as the *AssetAdmin* for the next exercise.

Exercise 3: Viewing the Check and Change log

Each account has a **Check and Change Log** tab that allows you to view an account's password validation and reset history.

To view an account's change history

1. In **Accounts**, select the account you have been working with.
2. Select the **Check and Change Log** tab to view the password change history.
3. Explore the results. Sort the items by **Status** or **Time**.

Stay logged in as the *AssetAdmin* for the next exercise.

Exercise 4: Viewing the History tab

Each of the **Administrative Tools** has a **History** tab that allows you to view or export the details of each operation that has affected a selected item.

To view the transaction history of an account

1. In **Assets**, select a managed system.
2. Select the **History** tab to view the transaction history.
3. Poke around and notice that each of the **Administrative Tools** (Account, Assets, Partitions, Users, etc.) has a **History** tab.
4. Log out.

Exercise 5: Using the Activity Center

The **Activity Center** is the place to go for troubleshooting issues. 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.

To run an activity report

1. Log in as the Auditor.

   NOTE: The Auditor has read-only access to all features.

2. From the **Home** page, navigate to the **Activity Center**.
3. Use the default query settings: I would like to see *all activity* occurring within the *last 24 hours*.
4. Click (or tap) **Run**.
5. Explore the results.
6. Double-click an event to see more details; Double-click to close the details.

To filter the content

1. Open the **User** filter list and select *AssetAdmin*.
2. Sort the records so the latest time is listed first.
3. Double-click a password event to view the details of the event.

Stay logged in as the Auditor for the next exercise.

Exercise 6: Auditing access requests

The Request Workflow dialog allows you to audit the transactions that took place within a password release or session request. This dialog can be accessed using the **Workflow** action button in the Activity Center view when an access request event is selected in an activity audit log report.

NOTE: The **Workflow** action button also appears to reviewers for completed access requests.

To view the request workflow for a password release or session request

1. Log in as the Auditor.
2. From the **Home** page, navigate to the **Activity Center**.
3. Run an activity audit log report.
4. On the results page, select an access request event and click (or tap) **Workflow** from the action bar.

   The Request Workflow dialog displays the workflow transactions from request to approval to review.
5. Select **Show Details** to view more information about the request, approval, and review transactions of that request.

Stay logged in as the Auditor for the next exercise.

Exercise 7: Running entitlement 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.

One Identity Safeguard provides these entitlement reports:

Table 4: Entitlement reports

Entitlements By...	Description
User	Lists information about the accounts a selected user is authorized to request.
Asset	Lists information about the accounts associated with a selected asset and the users who have authorization to request those accounts.
Account	Lists information about the users who have authorization to request a selected account, including asset and directory accounts.

To run an entitlement report

1. As Auditor, select **Reports** from the Safeguard desktop **Home** page.
2. Choose to view entitlements by **Asset**.
3. **Browse** to select all assets and click (or tap) **OK**.
4. In the top pane of the results screen select an asset to see the details.
5. View both the **Total Accounts** tab and the **People** tab.
6. Select an item from the results to drill down into the details about the users and the accounts.
7. Click (or tap) **Export** to create a file of the search results in a location of your choice.
8. Log out.

6

Discovery exercises

These exercises will guide you through a step-by-step evaluation of the Safeguard discovery features:

Exercise 1: Discovering assets

Safeguard allows you to set up asset discovery jobs to run automatically against the directories you have added to Safeguard. Therefore you must first add a directory to Safeguard before you can create an asset discovery job.

To add a directory

1. Log in as the Directory Administrator and navigate to **Administrative Tools**.
2. In **Directories**, click (or tap) **+ Add Directory** from the action bar.
3. In the **General** tab, choose a directory type and provide the service account information.
4. In the **Attributes** tab, accept the defaults and click (or tap) **Add Directory**.
5. Log out.

Now that you have a directory, you are ready to create an asset discovery job.

To create an asset discovery job

1. Log in as the Asset Administrator and navigate to **Administrative Tools**.
2. In **Assets**, click (or tap) **Discovery** and select **Manage** to open the **Asset Discovery Jobs** dialog.
3. Click (or tap) **+ Add** to create an asset discovery job.

4. Provide information for the discovery job on the following tabs:

Tab	Description
General tab	a. Enter a name for the asset discovery job. b. Use the default partition. c. Choose the **Directory** scan.
Information tab	**Browse** to select search location.
Rules tab	Click (or tap) **+ Add** to create an asset discovery rule: a. Enter a name for the rule. b. In **Conditions**, define search criteria. c. In **Connection**, configure the authentication credentials or choose the **None** authentication type. d. In **Profile**, choose the default password profile to govern the discovered assets.
Schedule tab	Optionally, schedule the discovery job. NOTE: You can run the discovery job manually, rather than wait for it to run automatically. So, for this POC, you can skip this step.
Summary tab	Review the discovery job and save it.

5. In the Asset Discovery Jobs dialog, select the job and click (or tap) ▶ **Run Now**.
6. When the **Progress** column indicates that the job is successful, close the **Asset Discovery Jobs** dialog.
7. Click (or tap) **Refresh** from the action bar to display the discovered assets.
8. Open the context menu and choose **Ignore** on one or more discovered assets.

   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.

9. Click (or tap) **Hide Ignore** from the action bar to hide the ignored assets; click (or tap) **Show Ignored** to redisplay them.
10. Search the **Activity Center** for information about discovery jobs that have run. Safeguard lists the "Asset Discovery" events in the **Asset Discovery** category.

If you selected **None** as the authentication type, the discovered assets will not have a service account, which is necessary for the next exercise.

To set asset authentication credentials

1. In **Assets**, select one of the newly discovered assets.
2. On the **General** tab, double-click (or double-tap) the **Connection** information box or click (or tap) the **Edit** icon next to it.
3. Choose an **Authentication Type** and provide the service account credentials.

   NOTE: Safeguard uses a *service account* to connect to an asset to securely manage passwords for the accounts on that asset.

Exercise 2: Discovering accounts

Safeguard allows you to set up account discovery jobs to run automatically against the assets it manages in the scope of a partition.

To create an account discovery job

1. As the Asset Administrator, navigate to **Partitions**.
2. Select a partition and switch to the **Profiles** tab.
3. Double-click (or double-tap) a profile, and switch to the **Account Discovery** tab.
4. Click (or tap) **+ Add** to create a new **Account Discovery Setting**.
   a. Enter a **Name** for the setting, such as "Daily".
   b. **Schedule** the discovery job to run daily starting in about 5 minutes.
   c. Allow it to **Find All accounts** and click (or tap) **OK** to save the schedule.

      NOTE: If you opt to experiment with finding accounts based on rules, note that all search terms return exact matches and are case sensitive.
5. Save the profile and wait for it to run.
6. After the account discovery job runs, switch to the partition's **Discovered Accounts** tab.
7. Click (or tap) **Refresh** from the details action bar to display the discovered accounts.
8. Select an account and click (or tap) **Manage** to have Safeguard manage that account password.
9. In **Accounts**, set the password for the new account, if you know it.

   Now you can check and change the account password successfully.

   NOTE: If you do not know the password, you can run **Check Password** and observe that the check fails.
10. Search the **Activity Center** for information about discovery jobs that have run. Safeguard lists the "Account Discovery" events in the **Password Management** category.

Exercise 3: Discovering directory accounts

Directory account discovery jobs run automatically each time Safeguard synchronizes with the directory, which is every 15 minutes by default. (You set the synchronization interval in the directory's **General** tab, under **Advanced**.)

To create a directory account discovery job

1. From **Directories** select a directory and switch to the **Accounts** tab.
2. Click (or tap) **Manage Discovery** from the details action bar.
3. On the **Manage Discovery** dialog, click (or tap) **+ Add** to open the **Directory Account Discovery** dialog.
4. In the **General** tab,
    a. Enter a name for the directory account discovery job.
    b. Select a profile to govern the account(s) Safeguard discovers.
5. In the **Rules** tab, click (or tap) **+ Add** to add a new discovery rule:
    a. Enter a rule name.
    b. Select to **Find All**.
    c. **Browse** to select the **Filter Search Location**.
6. Save the directory account discovery job and click (or tap) **Sync Now**.
7. After the job runs, switch to the directory's **Discovered Accounts** tab.
8. Click (or tap) **Refresh** from the details action bar to display the discovered accounts.
9. Select an account and click (or tap) **Manage** to have Safeguard manage that account password.
10. Switch to the **Accounts** tab to set the password for the new account, if you know it.

    Now you can check and change the account password successfully. If you do not know the password, you can still run **Check Password** to watch it fail.
11. Search the **Activity Center** for information about discovery jobs that have run (Account Discovery Activity).

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
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Index

L

P

R

S

T

W