One Identity Safeguard 2.2

Release Notes

June 2018

These release notes provide information about the One Identity Safeguard 2.2 release.

About this release

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.

One Identity Safeguard Version 2.2 is a major release with new features and functionality in addition to numerous bug fixes. In this release you will find additional platform support for asset management, dynamic grouping and tagging, site awareness and network segmentation, Application to Application integration, Starling join, audit log archiving, an Asset administrator dashboard, and new attribute search. See New features and enhancements.

NOTE: For a full list of key features in One Identity Safeguard, see the *One Identity Safeguard Administration Guide*.

New features and enhancements

New features and enhancements in One Identity Safeguard version 2.2 include:

Table 1: Safeguard 2.2: Features and enhancements

Feature/Enhancement	Description
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 so that the authorized user can be notified of the available request and log in to Safeguard to retrieve a

Feature/Enhancement	Description
	password or start a session.
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

Feature/Enhancement	Description
	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.

See also:

- Resolved issues on page 7

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 2: Safeguard 2000 Appliance: Feature specifications

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

Table 3: Safeguard 2000 Appliance: Power requirements

Input Voltage	100-240 Vac
Frequency	50-60Hz
Power Consumption (Watts)	170.9
BTU	583

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 4: Appliance LCD and controls

Control	Description
Green check mark button	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. **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.**
Red X button	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. **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.**
Down, up, left and right arrow buttons	When the appliance is running, the LCD home screen displays: • Safeguard <version number> Use the arrow buttons to scroll through the following details: • Serial: <appliance serial number> • X0: <appliance IP address> • X1: <IP address of the session module interface> • MGMT: <management IP address> • MGMT MAC: <media access control address> • IPMI: <IP address for IPMI>

Resolved issues

The following is a list of issues addressed in this release.

Table 5: General resolved issues

Resolved Issue	Issue ID
Updated Network Interface information (**Administrative Tools** | **Settings** | **Appliance** | **Networking**) to include the appliance MAC address.	620757
Reduced the number of events logged to the Activity Center when initializing NTP.	702756
Canceling login now returns an "Authentication failed" message instead of a "Missing StsAccessToken parameter" message.	711544
Fixed the unhandled exception that was encountered if your machine did not include the time zone that was being selected from the Safeguard Desktop Client.	715946
Resolved the issue where an asset's connection credentials (Service Account) were being reset to **None** when an asset was assigned to a different partition or profile.	728859
Fixed error encountered when creating a favorite for Directory Account password request.	733202
Added certificate details to the error logs generated when a test connection failure is caused by an untrusted certificate.	734327
Resolved the issue where a newly added directory service provider was not available for selection when adding a new user or user group.	736926
Added the Lights Out Management (BMC) pane to the Appliance settings pane.	740797
Fixed unhandled exception that was encountered when updating a dependent asset during a password change operation.	741974
When changing SSH keys on an asset, the Service Account Name field is now read only because we are assuming the administrator is only changing the key and is therefore using the same service account.	745311
Resolved issue where adding an asset to a partition from the Partition view failed.	747754
Resolved the "Failed to resolve the selected object" issue where Safeguard was not allowing you to add an Active Directory group that contained a colon in its name.	749277

Resolved Issue	Issue ID
Resolved issue where a GUID was being displayed as the display name for Active Directory groups in the Users/User Groups dialog.	753428
Added note to the Lights Out Management (BMC) topic in the Safeguard Administration Guide to include the default user name for the BMC admin.	758258
Added a message to report when access request policies cannot be removed because the selected account is associated indirectly via a group.	758711
Included the zat file name for a session recording in the Activity Center.	759087
Users can now copy lines of text from the Activity Center.	759286
Fixed issue where TestDiscovery was failing when the user was not the only delegated partition owner.	763786
Fixed issue where only the first asset was being updated when multiple assets had dependencies on the same directory account.	764332
Resolved issue caused by Windows Update KB 4088875 that broke session request functionality.	764545
Added Access Request ID to All activity, Appliance activity, and Access Request activity in the Activity Center. NOTE: The Access Request ID is not shown by default. You can add it using the **Columns** button.	764696
Resolved issue where communication with Starling Two-Factor Authentication was failing when using it as a secondary authentication provider in Safeguard.	766248
Users can now set the client ID on the Connection page of the Asset dialog when adding an SAP asset.	767330
Resolved issue where Directory Sync intermittently failed to sync changes.	767870
Added version checking to resolve issues encountered during patching.	767893
Fixed the URL to access the LoginController to get identity provider ID for Token Retrieval.	770135
Users are now able to view all accounts without a password in the desktop client.	771520

Known issues

The following is a list of issues known to exist at the time of release.

Table 6: General known issues

Known Issue	Issue ID
A local account password reset can fail when you are using an asset that is configured with a service account with Administrative privileges other than the built-in Administrator. **Workaround**: Before Safeguard can reset local account passwords on Windows systems, using a service account that is not a built-in Administrator, you must change the local security policy to disable the "Run all administrators in Admin Approval Mode" option. ***To configure Windows assets to reset account passwords*** 1. From the Windows Start menu, open **Local Security Policy**. 2. Navigate to **Local Policies** | **Security Options**. 3. Disable the **User Account Control: Run all administrators in Admin Approval Mode** option. 4. Restart your computer.	478736
RDP Signing certificate fails with "A revocation check could not be performed for this certificate."	763103
Cannot change the default directory profile. **Workaround**: Use the Safeguard API to change the default directory profile.	774276
Backups cannot be created unless one already exists. More specifically, the **Run now** + button is not available on the **Administrative Tools** | **Settings** | **Backup and Retention** | **Safeguard Backup and Restore** pane to create a backup. **Workaround**: Schedule an automatic backup to occur in the next few minutes using the **Settings** ⚙ button on the **Safeguard Backup and Restore** pane. After the automatic backup has occurred and the + button is enabled, go back into settings to specify the automatic backup schedule that you want to use.	770122

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

Windows desktop client requirements

The desktop client is a native Windows application suitable for use on end-user machines. 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.

Table 7: Desktop client requirements

Component	Requirements
Technology	Microsoft .NET Framework 4.6
Windows platforms	32-bit or 64-bit editions of: • Windows 7 • Windows 8.1 • 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 requirements

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.

Table 8: Web client requirements

Component	Requirements
Web browsers	Desktop browsers: • Google Chrome 66 (or later) • Microsoft Internet Explorer 11 and Edge • Mozilla Firefox 52 (or later) Mobile device browsers: • Apple Safari iOS 10 (or later) • Google Chrome on Android The web client is implemented for modern web browser technology, using: • HTML5 • CSS • JavaScript NOTE: If your browser lacks these required technologies, then use the desktop client.

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.

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

Platform	Version	Architecture
ACF2 - Mainframe	r14, r15	zSeries
ACF2 - Mainframe LDAP	r14, r15	zSeries
AIX	6.1, 7.1, 7.2	PPC
Amazon Web Services	1	
CentOS Linux	6	x86, x86_64
	7	x86_64
Cisco IOS	12.X, 15.X	
Cisco PIX	7.X, 8.X	
Debian GNU/Linux	6, 7, 8, 9	MIPS, PPC, x86, x86_64, zSeries
Dell iDRAC	7, 8	
F5 Big-IP	12.1.X, 13.0	
Facebook		
Fedora	21, 22, 23, 24, 25, 26	x86, x86_64
Fortinet FortiOS	5.2, 5.6	
FreeBSD	10.4, 11.1	x86, x86_64
HP iLO	iLO 2, 3, 4	x86
HP iLO MP	2, 3, 4	IA-64
HP-UX	11iv2 (B.11.23), 11iv3 (B.11.31)	IA-64, PA-RISC
IBM i	7.1, 7.2	PPC
Junos - Juniper Networks	12, 13, 14, 15	
MAC OS X	10.9, 10.10, 10.11, 10.12, 10.13	x86_64
MongoDB	3.4, 3.6	
MySQL	5.6, 5.7	
Oracle Database	11g Release 2, 12c Release 1	
Oracle Linux (OEL)	6	x86, x86_64
	7	x86_64

Platform	Version	Architecture
PAN-OS	6.0, 7.0	
PostgreSQL	9.6.7, 10.2	
RACF - Mainframe	z/OS V2.1 Security Server, z/OS V2.2 Security Server	zSeries
RACF - Mainframe LDAP	z/OS V2.1 Security Server, z/OS V2.2 Security Server	zSeries
Red Hat Enterprise Linux (RHEL)	6 7	PPC, x86, x86_64, zSeries PPC, x86_64, zSeries
SAP HANA	2.0	Other
SAP Netweaver Application Server	7.3, 7.4	
Solaris	10 11	SPARC, x86, x86_64 SPARC, x86_64
SonicOS	5.9, 6.2	
SonicWALL SMA or CMS	11.3.0	
SQL Server	2012, 2014, 2016	
SUSE Linux Enterprise Server (SLES)	11 12	IA-64, PPC, x86, x86_64, zSeries PPC, x86_64, zSeries
Sybase (Adaptive Server Enterprise)	15.7, 16	
Top Secret - Mainframe	r14, r15	zSeries
Top Secret - Mainframe LDAP	r14, r15	zSeries
Twitter		
Ubuntu	14.04 LTS, 15.04, 15.10, 16.04 LTS, 16.10, 17.04	x86, x86_64
VMware ESXi	5.5, 6.0, 6.5	
Windows	Vista, 7, 8, 8.1, 10	
Windows Server	2008, 2008 R2, 2012, 2012 R2, 2016	

Table 10: Supported platforms: Directories that can be searched

Platform	Version
Microsoft Active Directory	Windows 2008+ DFL/FFL
OpenLDAP	2.4

Product licensing

The One Identity Safeguard 2000 Appliance ships with the following modules, each requiring a valid license to enable functionality:

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

To add a Safeguard module license

The first time you log into the Safeguard desktop client as the Appliance Administrator, it prompts you to add a license. In addition, you can add additional Safeguard module licenses by navigating to **Administrative Tools** | **Settings** | **Appliance** | **Licensing** in the desktop client.

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.
4. To add another module license, click (or tap) **Add Another License** from 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.

Update and installation instructions

The One Identity Safeguard appliance is built specifically for use only with the Safeguard software that is already installed and ready for immediate use.

To setup a new One Identity Safeguard 2000 appliance

If this is a new One Identity Safeguard 2000 appliance, see the *One Identity Safeguard Appliance Setup Guide* that was included in the package with your appliance. You can also find this guide on the One Identity Support Portal: https://support.oneidentity.com/one-identity-safeguard/2.1/technical-documents.

To update an existing Safeguard 2000 appliance with this patch

It is the responsibility of the Appliance Administrator to upgrade One Identity Safeguard by installing an update file (patch).

NOTE: **Minimum patch version**: 2.0.1.5037. If you are running an earlier version of the Safeguard appliance, you must upgrade to this version before applying the 2.2.0 patch.

NOTE: **Clustered environment**: Please see the *Patching cluster members* section in the *One Identity Safeguard Administration Guide* for instructions on how to deploy a patch so all appliances in the cluster are on the same version.

IMPORTANT: Always back up your appliance before you install an update file. Once you install an update file, you cannot uninstall it. For more information, see the *One Identity Safeguard Administration Guide*.

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

To install the software patch

1. As an Appliance Administrator, log into the Safeguard desktop client.
2. From the **Home** page, select **Administrative Tools**.
3. Select **Settings** | **Appliance** | **Updates**.

   The current appliance and client versions are displayed.
4. Click **Upload a File** and browse to select the update file you downloaded from the One Identity support web site.

   NOTE: When you select a file, Safeguard uploads it to the server, but does not install it.
5. Once the file has successfully uploaded, click **Install Now**.

To install the Safeguard desktop client

To define and enforce security policy for your enterprise, install the Windows desktop client application which gives you access to the Administrative Tools. You install the Windows desktop client by means of an MSI package which can be downloaded from the appliance web client portal. You do not need administrator privileges to install the One Identity Safeguard 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.

Verify successful installation

You can verify that the correct version has been successfully installed from the Safeguard desktop client or the LCD on the Safeguard 2000 appliance.

To verify the uploaded patch was installed

1. Log into the Safeguard desktop client as an Operations Administrator or an Appliance Administrator.
2. Select **Administrative Tools**.
3. Select **Settings** | **Appliance** | **Appliance Information**.
4. Verify the correct appliance version is displayed in the appliance properties pane.

In addition, when the appliance is running, the LCD home screen on the front panel of the appliance displays **Safeguard** <version number>. Therefore, you can verify the correct appliance version is running from there as well.

More resources

Additional information is available from the following:

- Online product documentation: https://support.oneidentity.com/one-identity-safeguard/technical-documents
- One Identity Community: https://www.quest.com/community/products/one-identity/

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. It supports simultaneous operation with multilingual data. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan. It supports bidirectional writing (Arabic and Hebrew). The release supports Complex Script (Central Asia – India, Thailand).

The release is localized to the following languages: Arabic (Saudi Arabia), Chinese (Simplified), Chinese (Traditional), Dutch, French, German, Italian, Japanese, Korean, Russian, Spanish.

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

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.