One Identity Safeguard 2.1

Release Notes

December 2017

These release notes provide information about the One Identity Safeguard 2.1 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 2.1 is a minor release with new features and functionality in addition to numerous bug fixes. In this release you will find enhancements to the access request, cluster patching, and session recording archival experiences. In addition, this version supports additional platforms for asset management, federated authentication, Lights Out Management (BMC), and X11 forwarding of session recordings. It also includes the ability to restrict in-bound communications to TLS 1.2, a new Security Policy Administrator dashboard for reviewing and managing access requests, and a new Safeguard Desktop Player for playing back recorded sessions. 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 2.1 include:

Table 1: 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.

Feature/Enhancement	Description
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.
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.

Feature/Enhancement	Description
	NOTE: This new feature applies to Windows platforms (Windows server and Active Directory accounts) and Unix platforms (AIX, HP-UX, Linux, Solaris, and Mac OS X accounts).
TLS 1.2 Only	To remediate security vulnerabilities identified in early versions of the TLS encryption protocol, Appliance Administrators can configure Safeguard to respond only to TLS 1.2 requests. This allows organizations to comply with the security and strong cryptography requirements in PCI-DSS.
X11 Forwarding	When configuring the settings for SSH session access requests, Security Policy Administrators can now enable **Allow X11 Forwarding**, which forwards a graphical X-server session from the server to the client.

See also:

- Resolved issues on page 6

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

Safeguard 2000	Feature / Specification
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
Max Wall Current (Amps)	1.42
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	Use the **Green check mark** button to start the appliance. Press the

Control	Description
mark button	**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
If a second user logs into the web client, using Microsoft Internet Explorer or Edge, this user will no longer see the page of the first user.	714410
Fixed the issue where two-factor authentication was prompting you twice for primary credentials.	715676

Resolved Issue	Issue ID
Fixed the issue where logins were intermittently failing after restoring a back up to an appliance.	720876
Fixed the issue where **Test Connection** was failing on Mac OS X devices, when the device to be managed was configured to use an Active Directory Service Account.	731051
Users are now able to use a linked account to submit access requests on several different assets simultaneously.	733092

Table 6: Privileged Sessions resolved issues

Resolved Issue	Issue ID
With the updated player, if you do not have the proper permissions to terminate a "live" session, the **Terminate** button is no longer displayed.	712475
The Safeguard Desktop Player can now connect to multiple instances of a "live" session.	716235
You can now use the SCP protocol to download an archived sessions file (.zat file) from the archive server.	724889

Table 7: Clustered environment resolved issues

Known Issue	Issue ID
Fixed the issue where the networking settings (Network Interface X1) are not being reset properly on the replica appliances in a clustered environment when the sessions module was redeployed.	724053

Known issues

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

Table 8: 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.	478736

Known Issue	Issue ID
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.	
Windows must be updated to include the time zone that is being selected from the Safeguard Desktop Client, otherwise you will get an unhandled exception.	715946
When an asset is assigned to a different partition or profile, the asset's connection credentials (Service Account) are reset to **None**. **Workaround**: After changing the partition or profile assignment for an asset, check the connection settings for the asset and re-enter the service account credentials if necessary.	728859
After adding a new directory, that directory service provider is not available for selection when adding a new user or user group. **Workaround**: Log out of the Safeguard Desktop client and log back in. The newly added directory is now available for selection when you add a new user or user group.	736926

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 9: 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 10: Web client requirements

Component	Requirements
Web browsers	Desktop browsers: • Google Chrome 58 (or later) • Microsoft Internet Explorer 11 and Edge • Mozilla Firefox 52 (or later)

Component	Requirements
	Mobile device browsers: • Apple Safari iOS 8 (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.

Table 11: 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 7	x86, x86_64 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

Platform	Version	Architecture
Fortinet FortiOS	5.2, 5.6	
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
MySQL	5.6, 5.7	
Oracle Database	11g Release 2, 12c Release 1	
Oracle Linux (OEL)	6 7	x86, x86_64 x86_64
PAN-OS	6.0, 7.0	
RACF-Mainframe	z/OS V1.13 Security Server, 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 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

Platform	Version	Architecture
Sybase (Adaptive Server Enterprise)	15.7, 16	
Top Secret - Mainframe	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 12: 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 from the **Administrative Tools | Settings** view.

1. In **Settings**, select **Licensing | Licensing Modules**.
2. Click (or tap) **+ Add License**.
3. **Browse** to select the license file.

   Once you add a license, Safeguard displays the current license information and additional links that allow you to update the license or view the license history for a module.

4. To add another module license, click (or tap) **Add Another License** 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 2.1.0 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/2.1/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

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

Patents

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

Trademarks

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

Legend

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

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

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

Safeguard Release Notes
Updated - December 2017
Version - 2.1