One Identity Safeguard 2.0.1.5037 Release Notes

September 2017

These release notes provide information about the One Identity Safeguard 2.0.1 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 2.0.1 is a language release providing localized strings for the following languages: Arabic (Saudi Arabia), Chinese (Simplified), Chinese (Traditional), Dutch, French, German, Italian, Japanese, Korean, Russian, and Spanish (Mexico). In addition, this release addresses issues related to clustering, sessions module stability, LCD navigation, network scan discovery using operating system rules, and web client RDP launch functionality. See Resolved issues.

New features

The key features available in One Identity Safeguard include:

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

Feature	Description
	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 save or export the data.
Two-factor authentication support	Protecting access to passwords with another password isn't enough. Enhance 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. NOTE: This feature requires a Privileged Sessions license.
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. NOTE: This feature requires a Privileged Sessions license.
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. NOTE: This feature requires a Privileged Sessions license.
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).

Feature	Description
	NOTE: This feature requires a Privileged Sessions license.
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. NOTE: This feature requires a Privileged Sessions license.
Auto-login	Sessions access request launch and auto-login enhances security and compliance by never exposing the account credentials to the user. NOTE: This feature requires a Privileged Sessions license.
Protocol support	Safeguard for Privileged Sessions provides full support for the SSH and RDP protocols. In addition, administrators can decide what options within the protocols they want to enable/disable. NOTE: This feature requires a Privileged Sessions license.
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.

See also:

- Resolved issues

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
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 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: Resolved issues

Resolved issue	Issue ID
Added a download RDP file option that allows you to initiate an RDP session from the web client.	712884
Updated cluster reset to prevent the primary appliance from going into a quarantine state due to a time out error while processing the join operation. IMPORTANT: Care should be taken when performing a cluster reset. In particular, do NOT perform a cluster reset on a newly created cluster. We recommend that your cluster be up and running for at least one day before performing a cluster reset.	713441
Fixed LCD display on appliance. Use the up, down, left or right arrow buttons to scroll through the following appliance information: Serial number, X0 IP address, X1 IP address, MGMT IP address, MGMT MAC address, and IPMI IP address. For more information about the LCD and controls on the front panel of the appliance, see Appliance LCD and controls.	713824
Updated sessions module to return module container state.	715524
Fixed error that occurred when attempting to configure the Network Interface (X1) after performing a factory reset.	715945
Fixed issue where a session would no longer connect after the sessions module was redeployed.	715948
Fixed the unjoin operation to prevent an appliance from going into quarantine state when unjoining from a cluster.	716729
Fixed memory issue that was causing the sessions module to become unresponsive.	708906
Fixed "500 Internal server" error that was causing the sessions module to become unresponsive after several reboots.	719177
Fixed issues that prevented Safeguard from performing a successful restore from a backup after performing a factory reset.	719183 719184
Fixed "You are not authorized to create a request for account" error that occurred when attempting to create a favorite request for a directory account or a linked account.	720155

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
VMWare ESXi 6.5 is not supported in this release.	712862
Two-factor authentication prompts you twice for primary credentials. When attempting to log into the Safeguard Desktop Client using an Active Directory or LDAP account that is also configured for two-factor authentication, you will be prompted to enter your primary credentials twice, before being prompted to enter your two-factor authentication credentials. NOTE: This does not occur when using a web browser to access Safeguard. **Workaround**: After entering your primary credentials and clicking **Log in**, the screen will refresh and you will again be presented with the username and password text boxes. However, there will not be a message or directory list drop-down. At this time, enter your Active Directory or LDAP credentials again and click **Log in**. You will then be presented with the two-factor authentication screen allowing you to complete the log in.	715676
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
Intermittently, after restoring a back up to an appliance, logins fail. **Workaround**: Reboot the appliance to restore login capabilities.	720876

Table 7: Privileged Sessions known issues

Known Issue	Issue ID
If you do not have the proper permissions to terminate a "live" session, clicking the **Terminate** button in the Safeguard Desktop Player makes it appear that the session has been terminated, but the session remains active.	712475
The Safeguard Desktop Player cannot connect to multiple instances of a "live" session. **Workaround**: Do not follow more than one active session at a time.	716235
You cannot use SCP protocol to download an archived sessions file (.zat file) from the archive server. **Workaround**: Use SFTP or SMB to download the session's zat file from the archive server.	724889

Table 8: Clustered environment known issues

Known Issue	Issue ID
When you redeploy the sessions module, the networking settings (Network Interface X1) are not being reset properly on the replica appliances in a clustered environment. **Workaround**: After redeploying the sessions module on a replica appliance, reset the networking setting for the X1 interface: 1. Log into the Safeguard desktop client as an Appliance Administrator. 2. Navigate to **Administrative tools | Settings | Appliance | Appliance Information**. 3. Click **Edit** next to the **Network Interface X1** heading. If the correct network information is displayed, no changes are necessary. 4. Click **OK**.	724053

Table 9: Third-party known issues

Known Issue	Issue ID
Microsoft Internet Explorer and Edge: If a second user logs into the web client, using Microsoft Internet Explorer or Edge, this user will see the page of the first user. This is a known issue where Internet Explorer and Edge pull the cached page from history, thus showing the previous user's page. **Workaround**: Ensure the following Internet Options setting is defined: 1. From the Windows Start menu, open **Internet Options**.	714410

Known Issue	Issue ID

2. On the Internet Properties | General tab, select the **Settings** button under the Browsing history pane.
3. On the Temporary Internet Files tab, set the **Check for newer versions of stored pages** setting to **Automatically**.

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 10: Desktop client requirements

Component	Requirements
Technology	Microsoft .NET Framework 4.6
Windows platforms	32-bit or 64-bit editions of: • Windows 7, 8, 8.1 and 10 • Windows Server 2008, 2012 and 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).
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 11: Web client requirements

Component	Requirements
Web browsers	Desktop browsers: • Google Chrome 58 (or greater) • Microsoft Internet Explorer 11 and Edge • Mozilla Firefox 52 (or greater) Mobile device browsers: • Apple Safari iOS 8 (or greater) • 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 12: Supported platforms: Assets that can be managed

Platform	Version	Architecture
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	

Platform	Version	Architecture
Cisco PIX	7.X, 8.X	
Debian GNU/Linux	6, 7, 8	MIPS, PPC, x86, x86_64, zSeries
Dell™ iDRAC	7, 8	
VMware ESXi	5.5, 6.0	
Facebook		
Fedora	21, 22, 23, 24, 25	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	
MySQL	5.6, 5.7	
Oracle Database	11g Release 2, 12c Release 1	
Oracle Linux (OEL)	6	x86, x86_64
	7	x86_64
Macintosh OS X	10.9, 10.10, 10.11, 10.12	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	PPC, x86, x86_64, zSeries
	7	PPC, x86_64, zSeries
SAP Netweaver Application Server	7.3, 7.4	
Solaris	10	SPARC, x86, x86_64
	11	SPARC, x86_64

Platform	Version	Architecture
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
Twitter		
Ubuntu	14.04 LTS, 15.04, 15.10, 16.04 LTS, 16.10, 17.04	x86, x86_64
Windows	Vista, 7, 8, 8.1, 10	
Windows Server	2008, 2008 R2, 2012, 2012 R2, 2016	

Table 13: 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.

Upgrade and installation instructions

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/2.0.1/technical-documents.

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

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

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

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*.

To install the software patch

1. As an Appliance Administrator, log into the Safeguard Desktop Client.
2. In **Settings**, select **Appliance | Updates**.

The current appliance and client versions are displayed.

3. Click **Upload a File** and browse to select the update file you downloaded from the One Identity support site.

   NOTE: When you select a file, Safeguard uploads it to the server, but does not install it.

4. Once the file has successfully uploaded, click **Install Now**.
5. Once you install the update file you can review the details about in the Update History (**Settings | Appliance | Update History**).

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*>/en-US/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.

Verifying 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 determine if this patch is installed

1. Log into the Safeguard Desktop client as an Operations Administrator or an Appliance Administrator.
2. Select **Administrative Tools** | **Settings**.
3. In **Settings**, select **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 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/2.0.1/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

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.