One Identity Safeguard 2.0

Release Notes

August 2017

These release notes provide information about the One Identity Safeguard 2.0 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 is a major release with new features and functionality. See New features.

New features

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

Feature	Description
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. 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).
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.

Feature	Description
Protocol support	Safeguard for Privileged Sessions provides full support for the SSH and RDP protocols. In addition, administrators can decide what options within the protocols they want to enable/disable.
Secure access to legacy systems	Use smartcard, two-factor authentication or other strong authentication methods to gain access to systems. Because Safeguard acts as a gateway or proxy to the system, it enables strong authentication to targets that cannot or do not support those methods natively.

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

Safeguard 2000	Feature / Specification
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

Known issues

The following is a list of issues, including those attributed to third-party products, known to exist at the time of release.

Table 4: General known issues

Known Issue	Issue ID
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.	715676

Known Issue	Issue ID
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.	
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

Table 5: 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
Unable to initiate an RDP session by copying the "User Connection String" from the web or desktop client and pasting it directly into the Microsoft Remote Desktop client. **Workaround**: From the Safeguard Desktop Client, click the launch arrow for the RDP session request to successfully initiate an RDP session.	712884
Running more than 75 concurrent RDP sessions with **Command Detection** enabled may cause issues with the Privileged Sessions module. **Workaround**: Run RDP sessions **without Command Detection** enabled. This will allow you to run a greater number of concurrent sessions.	715948
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

Table 6: Clustered environment known issues

Known Issue	Issue ID
The primary appliance in a cluster goes into quarantine when performing a cluster reset. **Workaround**: Perform a manual cluster reset to recover a cluster that has lost consensus: 1. Take a backup of a functional appliance (primary or replica).	713441

Known Issue	Issue ID

2. Restore the backup to an appliance and activate that appliance as the new primary.
3. Factory reset the other appliances.
4. Re-join them to the primary.

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, 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 8: 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 9: 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	x86, x86_64
	7	x86_64

Platform	Version	Architecture
Cisco IOS	12.X, 15.x	
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

Platform	Version	Architecture
	11	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
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 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 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.

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 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.

More resources

Additional information is available from the following:

- Online product documentation: https://support.oneidentity.com/one-identity-safeguard/2.0/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 - August 2017
Version - 2.0