

Safeguard for Privileged Passwords patch prior to version 7.0

OS Patch Release Notes

20 April 2022, 03:04

This patch includes the changes listed in the following sections. One Identity may generate additional patches for future releases of the product.

About this patch

This patch is required before upgrading to Safeguard for Privileged Passwords 7.0. Contained within the patch are updates related to Microsoft security updates. For more information, see [Resolved issues](#).

Resolved issues

The following is a list of issues resolved in this patch.

Table 1: Resolved issues

Resolved issue	Issue ID
OS patch for MS TCP/IP issues and additional security updates.	264946/265437
DCOM Security Patch KB500442 WinRM workaround for LTS. For more information, see Event 10036 in Windows Server System log - Microsoft hardening DCOM (335559) .	301490

Applicability of this patch

Table 2: Products affected by this hotfix

Product name	Version
Safeguard for Privileged Passwords	All versions prior to 7.0

Update and installation instructions

The Safeguard for Privileged Passwords 3000 and 2000 Appliances are built specifically for use only with the Safeguard for Privileged Passwords privileged management software, which is pre-installed and ready for immediate use on the hardened appliances.

Safeguard for Privileged Passwords virtual appliances and cloud applications are also available.

To set up a new deployment: 3000 Appliance, 2000 Appliance, Virtual Machine, or Cloud

If this is a new physical appliance, virtual machine, or cloud deployment, see the *Safeguard for Privileged Passwords Appliance Setup Guide*. The guide is also included in the package with a physical appliance.

To update an existing physical appliance or virtual appliance with this patch

It is the responsibility of the Appliance Administrator to upgrade Safeguard for Privileged Passwords by installing an update file (patch). Consider the following:

- **Minimum patch version:** 6.0.0.12276. If you are running an earlier version of the Safeguard for Privileged Passwords Appliance, you must upgrade to this version before applying the pre-7.0 patch.
- **Clustered environment:** See the Patching cluster members section in the *Safeguard for Privileged Passwords Administration Guide* for instructions on how to deploy a patch so all appliances in the cluster are on the same version.
- During initial installation and when applying a patch, make sure the desktop client file is the one supplied with the appliance version. If the versions are not compatible, errors may occur.

Prepare to install a patch


1. Backup your appliance before you install a patch. Once you install a patch, you cannot uninstall it. See the *Safeguard for Privileged Passwords Administration Guide*, Backup and restore topic.

2. Download the latest physical appliance patch or virtual appliance patch from the One Identity Support Portal:
<https://support.oneidentity.com/one-identity-safeguard-for-privileged-passwords/download-new-releases>

To install the hardware patch

1. As an Appliance Administrator, log in to the Safeguard for Privileged Passwords 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 for Privileged Passwords uploads it to the server, but does not install it.
5. Once the file has successfully uploaded, click **Install Now**.

To install the virtual machine patch

1. Make adequate resources available. The virtual appliances default deploy does not provide adequate resources. The minimum resources required are: 4 CPUs, 10GB RAM, and a 500GB disk. Without adequate disk space, the patch will fail and you will need to expand disk space then re-upload the patch.
2. Go to the web management console and click  **Setup** and follow the wizard.

Verify successful installation

You can verify that the correct version has been successfully installed from the Safeguard for Privileged Passwords desktop client or the LCD on the Safeguard for Privileged Passwords Appliance.

To verify the uploaded patch was installed

1. Log in to the Safeguard for Privileged Passwords 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 for Privileged Passwords** <version number>. Therefore, you can verify the correct appliance version is running from there, as well.

Removing this patch

Once installed you cannot remove this patch.

Supported platforms

Safeguard for Privileged Passwords supports a variety of platforms, including custom platforms.

Safeguard for Privileged Passwords tested platforms

The following table lists the platforms and versions that have been tested for Safeguard for Privileged Passwords (SPP). Additional assets may be added to Safeguard for Privileged Passwords. If you do not see a particular platform listed when adding an asset, use the **Other**, **Other Managed**, **Other Directory**, or **Linux** selection on the **Management** tab of the **Asset** dialog.

NOTE: Prior to Safeguard for Privileged Passwords 6.8, the version and architecture information was readonly. It was stored with the platform and formed part of the platform name. As of Safeguard for Privileged Passwords 6.8, this information is no longer associated with the platform. It is now optional, and can be configured on each asset.

A new set of platforms are defined in Safeguard for Privileged Passwords 6.8 to replace the legacy platforms. See the table below for details on how the legacy platforms are mapped to the new platforms.

For customers upgrading from a pre-6.8 version of Safeguard for Privileged Passwords, the legacy platform will automatically be mapped to the corresponding new platform for each existing asset. Following an upgrade, the platform id of each existing asset will have changed. Some platform names may also have changed. From the desktop UI, only the new platforms are available when creating an asset. By default, the API will also only report the new platforms. For example, a GET request to the following URI will report only the new platforms:

```
https://<appliance>/serve/core/V3/Platforms
```

The legacy platforms still exist within Safeguard for Privileged Passwords for reference, but can only be retrieved using a filter query with the API. For example, the following will retrieve the legacy Active Directory platform:

```
https://<appliance>/serve/core/V3/Platforms?filter=Id%20eq%203
```

SPP linked to SPS: Sessions platforms

CAUTION: When linking your One Identity Safeguard for Privileged Sessions (SPS) deployment to your One Identity Safeguard for Privileged Passwords (SPP) deployment, ensure that the SPS and SPP versions match exactly, and keep the versions synchronized during an upgrade. For example, you can only link SPS version 6.6 to SPP version 6.6, and if you upgrade SPS to version 6.7, you must also upgrade SPP to 6.7.

Make sure that you do not mix Long Term Supported (LTS) and feature releases. For example, do not link an SPS version 6.0 to an SPP version 6.1.

When Safeguard for Privileged Passwords (SPP) is linked with a Safeguard for Privileged Sessions (SPS) appliance, platforms are supported that use one of these protocols:

- SPP 2.8 or lower: RDP, SSH
- SPP 2.9 or higher: RDP, SSH, or Telnet

Some platforms may support more than one protocol. For example, a Linux (or Linux variation) platform supports both SSH and Telnet protocols.

Table 3: Supported platforms: Assets that can be managed

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
ACF2 - Mainframe	ACF2 - Mainframe LDAP r14 zSeries ACF2 - Mainframe LDAP r15 zSeries	True	True
ACF2 - Mainframe LDAP	ACF2 - Mainframe LDAP r14 zSeries ACF2 - Mainframe LDAP r15 zSeries	True	False
Active Directory	Active Directory	True	False
AIX	AIX 6.1 PPC AIX 7.1 PPC AIX 7.2 PPC AIX Other	True	True
Amazon Linux	Amazon Linux 2 x86_64 Amazon Linux Other x86_64	True	True
Amazon Web Services	Amazon Web Services 1	True	False
CentOS Linux	CentOS Linux 6 x86 CentOS Linux 6 x86_64 CentOS Linux 7 x86_64	True	True

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
	CentOS Linux 8 x86_64 CentOS Linux Other		
Check Point GAIa (SSH)	Check Point GAIa (SSH) R76 Check Point GAIa (SSH) R77 Check Point GAIa (SSH) R80.30	True	True
Cisco ASA	Cisco ASA 7.X Cisco ASA 8.X Cisco ASA 9.X Cisco ASA Other	True	True
Cisco IOS (510)	Cisco IOS 12.X Cisco IOS 15.X Cisco IOS 16.X Cisco IOS Other	True	True
Cisco ISE	Cisco ISE 2.7 Cisco ISE 3	True	False
Cisco ISE CLI	Cisco ISE CLI 2.7 Cisco ISE CLI 3	True	True
Cisco NX-OS	Cisco NX-OS 9.3(7) Cisco NX-OS 9.3(7a)	True	True
Debian GNU/Linux (511)	Debian GNU/Linux 10 MIPS Debian GNU/Linux 10 PPC Debian GNU/Linux 10 x86 Debian GNU/Linux 10 x86_64 Debian GNU/Linux 10 zSeries Debian GNU/Linux 6 MIPS Debian GNU/Linux 6 PPC Debian GNU/Linux 6 x86 Debian GNU/Linux 6 x86_64 Debian GNU/Linux 6 zSeries Debian GNU/Linux 7 MIPS Debian GNU/Linux 7 PPC	True	True

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
	Debian GNU/Linux 7 x86 Debian GNU/Linux 7 x86_64 Debian GNU/Linux 7 zSeries Debian GNU/Linux 8 MIPS Debian GNU/Linux 8 PPC Debian GNU/Linux 8 x86 Debian GNU/Linux 8 x86_64 Debian GNU/Linux 8 zSeries Debian GNU/Linux 9 MIPS Debian GNU/Linux 9 PPC Debian GNU/Linux 9 x86 Debian GNU/Linux 9 x86_64 Debian GNU/Linux 9 zSeries Debian GNU/Linux Other		
Dell iDRAC	Dell iDRAC 7 Dell iDRAC 8 Dell iDRAC 9	True	True
eDirectory LDAP	eDirectory LDAP 9.0	True	False
ESXi	ESXi 5.5 ESXi 6.0 ESXi 6.5 ESXi 6.7 ESXi 7.0	True	False
F5 Big-IP	F5 Big-IP 12.1.2 F5 Big-IP 13.0 F5 Big-IP 14.0 F5 Big-IP 15.0	True	True
Facebook (Deprecated)	Facebook (Deprecated)		
Fedora	Fedora 21 x86 Fedora 21 x86_64	True	True

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
	Fedora 22 x86		
	Fedora 22 x86_64		
	Fedora 23 x86		
	Fedora 23 x86_64		
	Fedora 24 x86		
	Fedora 24 x86_64		
	Fedora 25 x86		
	Fedora 25 x86_64		
	Fedora 26 x86		
	Fedora 26 x86_64		
	Fedora 27 x86		
	Fedora 27 x86_64		
	Fedora 28 x86		
	Fedora 28 x86_64		
	Fedora 29 x86		
	Fedora 29 x86_64		
	Fedora 30 x86		
	Fedora 30 x86_64		
	Fedora 31 x86		
	Fedora 31 x86_64		
	Fedora 32 x86		
	Fedora 32 x86_64		
	Fedora Other		
Fortinet FortiOS	Fortinet FortiOS 5.2	True	True
	Fortinet FortiOS 5.6		
	Fortinet FortiOS 6.0		
	Fortinet FortiOS 6.2		
FreeBSD	FreeBSD 10.4 x86	True	True
	FreeBSD 10.4 x86_64		
	FreeBSD 11.1 x86		
	FreeBSD 11.1 x86_64		
	FreeBSD 11.2 x86		

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
	FreeBSD 11.2 x86_64 FreeBSD 12.0 x86 FreeBSD 12.0 x86_64		
HP iLO	HP iLO 2 x86 HP iLO 3 x86 HP iLO 4 x86 HP iLO 5 x86	True	True
HP iLO MP	HP iLO MP 2 IA-64 HP iLO MP 3 IA-64	True	True
HP-UX	HP-UX 11iv2 (B.11.23) IA-64 HP-UX 11iv2 (B.11.23) PA-RISC HP-UX 11iv3 (B.11.31) IA-64 HP-UX 11iv3 (B.11.31) PA-RISC HP-UX Other	True	True
IBM i (formerly AS400)	IBM i 7.1 PPC IBM i 7.2 PPC IBM i 7.3 PPC IBM i 7.4 PPC	True	True
Junos - Juniper Networks	Junos - Juniper Networks 12 Junos - Juniper Networks 13 Junos - Juniper Networks 14 Junos - Juniper Networks 15 Junos - Juniper Networks 16 Junos - Juniper Networks 17 Junos - Juniper Networks 18 Junos - Juniper Networks 19	True	True
LDAP	OpenLDAP 2.4	True	False
Linux	Other Linux	True	True
macOS	macOS 10.10 x86_64 macOS 10.11 x86_64 macOS 10.12 x86_64	True	True

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
	macOS 10.13 x86_64 macOS 10.14 x86_64 macOS 10.15 x86_64 macOS 10.9 x86_64 macOS Other		
MongoDB	MongoDB 3.4 MongoDB 3.6 MongoDB 4.0 MongoDB 4.2	True	False
MySQL	MySQL 5.6 MySQL 5.7 MySQL 8.0	True	False
Oracle	Oracle 11g Release 2 Oracle 12c Release 1 Oracle 12c Release 2 Oracle 18c Oracle 19c	True	False
Oracle Linux (OL)	Oracle Linux (OL) 6 x86 Oracle Linux (OL) 6 x86_64 Oracle Linux (OL) 7 x86_64 Oracle Linux (OL) 8 x86_64 Oracle Linux (OL) Other	True	True
Other	Other	False	False
Other Directory	Other Directory	True	False
Other Managed	Other Managed	True	False
PAN-OS	PAN-OS 6.0 PAN-OS 7.0 PAN-OS 8.0 PAN-OS 8.1 PAN-OS 9.0	True	True
PostgreSQL	PostgreSQL 10	True	False

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
	PostgreSQL 10.2 PostgreSQL 10.3 PostgreSQL 10.4 PostgreSQL 10.5 PostgreSQL 11 PostgreSQL 12 PostgreSQL 9.6		
RACF - Mainframe	RACF - Mainframe z/OS V2.1 Security Server zSeries RACF - Mainframe z/OS V2.2 Security Server zSeries RACF - Mainframe z/OS V2.3 Security Server zSeries	True	True
RACF - RACF - Mainframe LDAP	RACF - Mainframe LDAP z/OS V2.1 Security Server zSeries RACF - RACF - Mainframe LDAP z/OS V2.2 Security Server zSeries RACF - RACF - Mainframe LDAP z/OS V2.3 Security Server zSeries	True	False
Red Hat Enterprise Linux (RHEL)	Red Hat Enterprise Linux (RHEL) 6 PPC Red Hat Enterprise Linux (RHEL) 6 x86 Red Hat Enterprise Linux (RHEL) 6 x86_64 Red Hat Enterprise Linux (RHEL) 6 zSeries Red Hat Enterprise Linux (RHEL) 7 PPC Red Hat Enterprise Linux (RHEL) 7 x86_64 Red Hat Enterprise Linux (RHEL) 7 zSeries Red Hat Enterprise Linux (RHEL) 8 PPC	True	True

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
	Red Hat Enterprise Linux (RHEL) 8 x86_64 Red Hat Enterprise Linux (RHEL) 8 zSeries Red Hat Enterprise Linux (RHEL) Other		
Red Hat Directory Server	Red Hat Directory Server 11	True	False
SAP HANA	SAP HANA 2.0 Other	True	False
SAP Netweaver Application Server	SAP Netweaver Application Server 7.3 SAP Netweaver Application Server 7.4 SAP Netweaver Application Server 7.5	True	False
Solaris	Solaris 10 SPARC Solaris 10 x86 Solaris 10 x86_64 Solaris 11 SPARC Solaris 11 x86_64 Solaris Other	True	True
SonicOS	SonicOS 5.9 SonicOS 6.2 SonicOS 6.4 SonicOS 6.5	True	False
SonicWALL SMA or CMS	SonicWALL SMA or CMS 11.3.0	True	False
SQL Server	SQL Server 2012 SQL Server 2014 SQL Server 2016 SQL Server 2017 SQL Server 2019	True	False
SUSE Linux Enterprise Server (SLES)	SUSE Linux Enterprise Server (SLES) 11 IA-64 SUSE Linux Enterprise Server (SLES) 11 PPC	True	True

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
	SUSE Linux Enterprise Server (SLES) 11 x86		
	SUSE Linux Enterprise Server (SLES) 11 x86_64		
	SUSE Linux Enterprise Server (SLES) 11 zSeries		
	SUSE Linux Enterprise Server (SLES) 12 PPC		
	SUSE Linux Enterprise Server (SLES) 12 x86_64		
	SUSE Linux Enterprise Server (SLES) 12 zSeries		
	SUSE Linux Enterprise Server (SLES) 15 PPC		
	SUSE Linux Enterprise Server (SLES) 15 x86_64		
	SUSE Linux Enterprise Server (SLES) 15 zSeries		
	SUSE Linux Enterprise Server (SLES) Other		
Sybase (Adaptive Server Enterprise)	Sybase (Adaptive Server Enterprise) 15.7	True	False
	Sybase (Adaptive Server Enterprise) 16		
	Sybase (Adaptive Server Enterprise) 17		
Top Secret - Mainframe	Top Secret - Mainframe r14 zSeries	True	False
	Top Secret - Mainframe r15 zSeries		
	Top Secret - Mainframe r16 zSeries		
Top Secret - Mainframe LDAP	Top Secret - Mainframe LDAP r14 zSeries	True	True
	Top Secret - Mainframe LDAP r15 zSeries		
	Top Secret - Mainframe LDAP r16 zSeries		
Twitter (Deprecated)	Twitter (Deprecated)		

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
Ubuntu	Ubuntu 14.04 LTS x86	True	True
	Ubuntu 14.04 LTS x86_64		
	Ubuntu 15.04 x86		
	Ubuntu 15.04 x86_64		
	Ubuntu 15.10 x86		
	Ubuntu 15.10 x86_64		
	Ubuntu 16.04 LTS x86		
	Ubuntu 16.04 LTS x86_64		
	Ubuntu 16.10 x86		
	Ubuntu 16.10 x86_64		
	Ubuntu 17.04 x86		
	Ubuntu 17.04 x86_64		
	Ubuntu 17.10 x86		
	Ubuntu 17.10 x86_64		
	Ubuntu 18.04 LTS x86		
	Ubuntu 18.04 LTS x86_64		
	Ubuntu 18.10 x86		
	Ubuntu 18.10 x86_64		
	Ubuntu 19.04 x86		
	Ubuntu 19.04 x86_64		
Ubuntu 19.10 x86_64			
Ubuntu 20.04 x86_64			
Ubuntu Other			
Windows Desktop	Windows (SSH) 10	True	True
Windows Desktop (SSH)	Windows (SSH) 7		
	Windows (SSH) 8		
Windows Desktop (WinRM)	Windows (SSH) 8.1		
Windows Server	Windows (SSH) Other		
Windows Server (SSH)	Windows (SSH) Server 2008 R2		
	Windows (SSH) Server 2012		
Windows Server (WinRM)	Windows (SSH) Server 2012 R2		
	Windows (SSH) Server 2016		

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
	Windows (SSH) Server 2019		
	Windows 10		
	Windows 7		
	Windows 8		
	Windows 8.1		
	Windows Other		
	Windows Server 2008		
	Windows Server 2008 R2		
	Windows Server 2012		
	Windows Server 2012 R2		
	Windows Server 2016		
	Windows Server 2019		
	Windows Vista		

Table 4: Supported platforms: Directories that can be searched

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

For all supported platforms, it is assumed that you are applying the latest updates. For unpatched versions of supported platforms, Support will investigate and assist on a case-by-case basis but it may be necessary for you to upgrade the platform or use SPP's custom platform feature.

Custom platforms

The following example platform scripts are available:

- Custom HTTP
- Linux SSH
- Telnet
- TN3270 transports are available

Sample custom platform scripts and command details are available at the following links available from the [Safeguard Custom Platform Home](#) wiki on GitHub:

- Command-Reference:
<https://github.com/OneIdentity/SafeguardCustomPlatform/wiki/Command-Reference>
- Writing a custom platform script:
<https://github.com/OneIdentity/SafeguardCustomPlatform/wiki/WritingACustomPlatformScript>
- Example platform scripts are available at this location:
<https://github.com/OneIdentity/SafeguardCustomPlatform/tree/master/SampleScripts>

⚠ CAUTION: Example scripts are provided for information only. Updates, error checking, and testing are required before using them in production. Safeguard for Privileged Passwords checks to ensure the values match the type of the property that include a string, boolean, integer, or password (which is called secret in the API scripts). Safeguard for Privileged Passwords cannot check the validity or system impact of values entered for custom platforms.

Product licensing

As a Safeguard for Privileged Passwords user, if you get an "appliance is unlicensed" notification, contact your Appliance Administrator.

Hardware appliance

The Safeguard for Privileged Passwords 3000 Appliance and 2000 Appliance ship with the Privileged Passwords module which requires a valid license to enable functionality.

You must install a valid license. Once the module is installed, Safeguard for Privileged Passwords shows a license state of **Licensed** and is operational. If the module license is not installed, you have limited functionality. That is, even though you will be able to configure access requests, if a Privileged Passwords module license is not installed, you will not be able to request a password release.

Virtual appliance Microsoft Windows licensing

You must license the virtual appliance with a Microsoft Windows license. We recommend using either the MAK or KMS method. Specific questions about licensing should be directed to your Sales Representative. The virtual appliance will not function unless the operating system is properly licensed.

Licensing setup and update

To enter licensing information when you first log in

The first time you log in as the Appliance Administrator, you are prompted to add a license. The **Success** dialog displays when the license is added.

On the virtual appliance, the license is added as part of Initial Setup.

To configure reminders for license expiration

To avoid disruptions in the use of Safeguard for Privileged Passwords, 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.

Users are instructed to contact their Appliance Administrator if they get an "appliance is unlicensed" notification.



As an Appliance Administrator, if you receive a "license expiring" notification, apply a new license.

To update the licensing file

Licensing update is only available using a virtual machine, not via the hardware.

web client: To perform licensing activities

Go to the licensing page:

1. Navigate to  **Appliance | Licensing**.
 - To upload a new license file, click **+Upload new license file** and browse to select the current license file.
 - To remove the license file, select the license and click  **Remove selected license**.

desktop client: To perform licensing activities

1. Navigate to **Administrative Tools | Settings | Appliance | Licensing**.
 - To upload a new license file, click **+Add License** and browse to select the license file.
 - To update a license file, select the license then select **Update License** in the lower left corner of a module's licensing information pane, select the license file, and click **Open**.

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 and other inquiries, such as licensing, support, and renewals, visit <https://www.oneidentity.com/company/contact-us.aspx>.

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

Copyright 2022 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.



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 highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.