



Safeguard Authentication Services 6.2

Installation Guide

**Copyright 2025 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 website (<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/trademark-information.aspx](http://www.OneIdentity.com/legal/trademark-information.aspx). 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.

Safeguard Authentication Services Installation Guide  
Updated - 18 November 2025, 10:13

For the most recent documents and product information, see [Online product documentation](#).

# Contents

<b>Privileged Access Suite for UNIX</b> .....	<b>1</b>
About this guide .....	2
<b>Introducing One Identity Safeguard Authentication Services</b> .....	<b>3</b>
About licenses .....	3
<b>Installing and configuring Safeguard Authentication Services</b> .....	<b>4</b>
Install Safeguard Authentication Services Windows components .....	4
Installing Windows components .....	5
Customizing installation options .....	5
Installing and using msiexec.exe .....	6
Configure Active Directory .....	8
Configuring Active Directory .....	9
About Active Directory configuration .....	10
Join the host to AD without the Safeguard Authentication Services application configuration .....	12
Version 3 Compatibility Mode .....	12
<b>Installing and joining from the UNIX command line</b> .....	<b>14</b>
Verifying package signature .....	14
The pre-installation diagnostic tool .....	15
Running preflight .....	17
The install script .....	17
Installing the Safeguard Authentication Services agent .....	18
Installation script options .....	18
Licensing Safeguard Authentication Services .....	20
Verifying license information .....	21
Installing licenses from the command line .....	21
Creating the application configuration from the UNIX command line .....	22
Changing the schema configuration mode .....	22
Joining the domain .....	23
Joining the domain using VASTOOL .....	23
Joining the domain using VASJOIN script .....	24

Dynamic DNS update tool .....	26
<b>Getting started with Safeguard Authentication Services .....</b>	<b>27</b>
Getting acquainted with the Control Center .....	27
Group Policy .....	28
Filtering the list of GPOs .....	28
Editing a GPO .....	29
Generating a settings report .....	29
Showing files .....	29
Launching GPMC .....	30
Tools .....	30
Preferences .....	30
Licensing .....	31
Display specifiers .....	32
Global UNIX Options .....	39
Logging Options .....	41
Schema Attributes .....	42
Use Safeguard Authentication Services PowerShell .....	44
UNIX-enabling a user and user group (PowerShell Console) .....	45
PowerShell cmdlets .....	47
Change Auditor for Authentication Services .....	49
Installing Change Auditor for Authentication Services .....	50
One Identity Defender .....	50
Installing Defender .....	50
<b>Appendix: Troubleshooting .....</b>	<b>52</b>
Getting help from technical support .....	52
Disaster recovery .....	53
Long startup delays on Windows .....	53
Pointer Record updates are rejected .....	53
Resolving DNS problems .....	54
Resolving preflight failures .....	54
Time synchronization problems .....	58
Unable to install or upgrade .....	58
Unable to join the domain .....	59
Unable to log in .....	59

vasypd has unsatisfied dependencies .....	60
<b>Appendix: Enterprise package deployment .....</b>	<b>62</b>
Installing the agent package .....	62
Agent upgrade commands .....	64
Restarting services .....	66
Uninstalling the agent packages .....	66
Oracle Solaris 10 zones/containers support .....	67
Safeguard Authentication Services and Oracle Solaris 10 Zones installation guidelines .....	67
<b>About us .....</b>	<b>69</b>
Contacting us .....	69
Technical support resources .....	69
<b>Index .....</b>	<b>70</b>

# Privileged Access Suite for UNIX

## UNIX security simplified

Privileged Access Suite for UNIX solves the intrinsic security and administration issues of UNIX-based systems (including Linux and macOS) while making satisfying compliance requirements easier. It unifies and consolidates identities, assigns individual accountability, and enables centralized reporting for user and administrator access to UNIX. The Privileged Access Suite for UNIX combines an Active Directory bridge and root delegation solutions under a unified console that grants organizations centralized visibility and streamlined administration of identities and access rights across their entire UNIX environment.

## Active Directory bridge

Achieve unified access control, authentication, authorization, and identity administration for UNIX, Linux, and macOS systems by extending them into Active Directory (AD) and taking advantage of AD's inherent benefits. Patented technology allows non-Windows resources to become part of the AD trusted realm, and extends AD's security, compliance, and Kerberos-based authentication capabilities to UNIX, Linux, and macOS. See [www.oneidentity.com/products/safeguard-authentication-services/](http://www.oneidentity.com/products/safeguard-authentication-services/) for more information about the Active Directory Bridge product.

## Root delegation

The Privileged Access Suite for UNIX offers two different approaches to delegating the UNIX root account. The suite either enhances or replaces sudo, depending on your needs.

- By choosing to enhance sudo, you will keep everything you know and love about sudo while enhancing it with features like a central sudo policy server, centralized keystroke logs, a sudo event log, and compliance reports for who can do what with sudo.

See [www.oneidentity.com/products/privilege-manager-for-sudo/](http://www.oneidentity.com/products/privilege-manager-for-sudo/) for more information about enhancing sudo.

- By choosing to replace sudo, you will still be able to delegate the UNIX root privilege based on centralized policy reporting on access rights, but with a more granular permission and the ability to log keystrokes on all activities from the time a user logs in, not just the commands that are prefixed with "sudo." In addition, this option

implements several additional security features like restricted shells, remote host command execution, and hardened binaries that remove the ability to escape out of commands and gain undetected elevated access.

For more information about replacing sudo, see [www.oneidentity.com/products/privilege-manager-for-unix/](http://www.oneidentity.com/products/privilege-manager-for-unix/).

## Privileged Access Suite for UNIX

Privileged Access Suite for UNIX offers two editions: **Standard** edition and **Advanced** edition. Both editions include the Safeguard Authentication Services patented technology that allows organizations to extend the security and compliance of Active Directory to UNIX, Linux, and macOS platforms and enterprise applications. In addition:

- The **Standard** edition licenses you for Safeguard for Sudo.
- The **Advanced** edition licenses you for Privilege Manager for Unix.

## About this guide

The *Safeguard Authentication Services Installation Guide* is intended for Windows, UNIX, Linux, and Macintosh system administrators, network administrators, consultants, analysts, and any other IT professionals who will be installing and configuring Safeguard Authentication Services for the first time. This guide walks you through the process of installing, upgrading, and uninstalling the Safeguard Authentication Services agent.

**NOTE:** The term "Unix" is used informally throughout the Safeguard Authentication Services documentation to denote any operating system that closely resembles the trademarked system, UNIX.

# Introducing One Identity Safeguard Authentication Services

One Identity Safeguard Authentication Services is patented technology that enables organizations to extend the security and compliance of Active Directory to UNIX, Linux, and macOS platforms and enterprise applications. It addresses the compliance need for cross-platform access control, the operational need for centralized authentication and single sign-on, and enables the unification of identities and directories for simplified identity and access management.

## About licenses

Safeguard Authentication Services must be licensed in order for Active Directory users to authenticate on UNIX and macOS hosts.

Considerations:

- New licenses have to be added prior to upgrade.
- You can install and configure Safeguard Authentication Services on Windows and use the included management tools to UNIX-enable users and groups in Active Directory without installing a license. However, you must have a valid Safeguard Authentication Services license installed for full functionality.

To obtain a license, use the [Licensing Assistance](#) page on the One Identity support page or contact your account representative.

For more information on installing Safeguard Authentication Services licenses, see [Licensing Safeguard Authentication Services](#).

## Installing and configuring Safeguard Authentication Services

This section describes how to extend the authentication, authorization, and administration infrastructure of Active Directory to the rest of your enterprise to allow UNIX, Linux, and macOS systems to act as full citizens within Active Directory.

***To extend the authentication, authorization, and administration infrastructure of Active Directory to the rest of your enterprise, allowing UNIX, Linux, and macOS systems to act as full citizens within Active Directory:***

1. Install and configure Safeguard Authentication Services.
2. Install Safeguard Authentication Services Windows components.
3. Configure Active Directory for Safeguard Authentication Services (one time only).
4. Configure UNIX Agent Components

Prepare the UNIX hosts for Active Directory user access:

- Add and profile a host.
- Check the host for readiness to join Active Directory.
- Install Safeguard Authentication Services agent software packages on the host to allow Active Directory user access.

**NOTE:** For users to authenticate on UNIX, Linux, and macOS hosts with Active Directory credentials, your UNIX hosts must have the Safeguard Authentication Services agent installed.

- Join the host to Active Directory.

### Install Safeguard Authentication Services Windows components

One Identity recommends that you install the Windows components and configure Active Directory before you install the UNIX components.

# Installing Windows components

Install Safeguard Authentication Services on each Windows Workstation you plan to use to administer UNIX data in Active Directory.

## *To install the Safeguard Authentication Services Windows components*

1. From the Autorun **Setup** tab, click **Safeguard Authentication Services** to launch the setup wizard.
2. In the **Software License Agreement** dialog, accept the terms of the End User License Agreement and click **Install**.

The Safeguard Authentication Services Setup wizard installs all Safeguard Authentication Services components by default.

To only install specific components, click the **Customize installation options** link. For more information, see [Customizing installation options](#) on page 5..

3. Once the installation completes successfully, click **Finish** or **Launch Control Center**.

# Customizing installation options

This section describes how to customize installation options.

## *To install specific Safeguard Authentication Services Windows components*

1. From the **Software License Agreement** dialog, click the **Customize installation options** link.
2. In the **Installation Options** dialog, select the components and options you want to install and click **OK**.

Available components:

- Core Components (required)
- ADUC Extensions
- Group Policy Extensions
- Documentation
- Safeguard Authentication Services Control Center

Available options:

- Install Start Menu Shortcuts
- Install Desktop Shortcuts

| **NOTE:** You must install the Core Components.

3. To add other Safeguard Authentication Services components later or modify the current installation of Safeguard Authentication Services, run the setup wizard again. From the root of the distribution media, double-click the autorun application.

## Installing and using msiexec.exe

You can install specific Safeguard Authentication Services components from the Windows command line using `Msiexec.exe`, the Microsoft Windows Installer program, which processes product installation files in the .MSI format. You can either double-click the individual Safeguard Authentication Services component .msi files or you can run `msiexec.exe` to install, modify, and perform other operations from the Windows command line.

The individual Safeguard Authentication Services component .msi files, located on the distribution media in the `windows` folder, are:

- `aducX64.msi`: Installs the Active Directory Users and Computers UNIX extensions for user and group management on a Windows 64-bit platforms.
- `aducX86.msi`: Installs the Active Directory Users and Computers UNIX extensions for user and group management on a Windows 32-bit platforms.
- `cc.msi`: Installs the Control Center extension.
- `corX64.msi`: Installs the core packages on a Windows 64-bit platform.
- `coreX86.msi`: Installs the core packages on a Windows 32-bit platform.
- `doc.msi`: Installs the User Documentation.
- `GpSettingsX86`: Installs the Safeguard Authentication Services Group Policy settings reporting library used by third parties such as Change Auditor and Group Policy Manager to report on Group Policy settings.
- `gpX64.msi`: Installs the Group Policy extension on a Windows 64-bit platforms.
- `gpX86.msi`: Installs the Group Policy extension on a Windows 32-bit platforms.

You can use the following properties on the command line when installing the individual Safeguard Authentication Services components.

**Table 1: MSI properties**

MSI property	Description
INSTALLFOLDER	Specifies the directory where you want to install the package. (Core X86 only.) Default: %PROGRAMFILES(X86)%\Quest Software\Authentication Services
INSTALLDESKTOPSHORTCUTS	Specifies whether or not to install desktop shortcuts.

MSI property	Description
	Default: 0 (Do not install desktop shortcuts.)
INSTALLSTARTMENUSHORTCUTS	Specifies whether or not to install <b>Start</b> menu shortcuts. Default: 0 (Do not install <b>Start</b> menu shortcuts.)
ARPSYSTEMCOMPONENT	Specifies whether or not to add an entry in the <b>Uninstall or change a program</b> interface ( <b>Add/Remove Programs</b> ) for each individual component (ADUC, Group Policy, and Control Center). Default: 0 (Add entry in Add/Remove Programs.)
NOCHANGEPSPOLICY	Specifies whether or not to allow PowerShell initialization policy modifications. (Core X86 only.) Default: 0 (Allow PowerShell policy modifications.)

The following procedures show examples of using the MSI Properties from the Windows command line.

### **To install Safeguard Authentication Services Windows components using Msiexec.exe**

1. To install the Control Center, enter the following:

```
msiexec /i cc.msi
```

**NOTE:** Run `msiexec -help` to see the full command syntax.

2. To specify the install directory path for the core packages, enter:

```
msiexec INSTALLFOLDER=%SystemDrive%:\<Directory> /i coreX86.msi
```

**NOTE:** By default, the installation directory is:

- On Windows 64-bit platforms:

```
%SystemDrive%\Program Files\Quest Software\Authentication Services
```

- On Windows 32-bit platforms:

```
%SystemDrive%\Program Files (x86)\Quest Software\Authentication Services
```

3. To install the Control Center and create a Desktop icon for it, enter:

```
msiexec INSTALLDESKTOPSHORTCUTS=1 /i cc.msi
```

4. To install the Control Center and create a **Start** menu shortcut for it, enter:

```
msiexec INSTALLSTARTMENUSHORTCUTS=1 /i cc.msi
```

5. To install the ADUC extensions and add a separate entry in the **Uninstall or change a program** interface for it, enter:

```
msiexec ARPSYSTEMCOMPONENT=0 /i aducX64.msi
```

**NOTE:** Setting ARPSYSTEMCOMPONENT to 1 prevents the application from displaying in the **Uninstall or change a program** interface (Add/Remove Programs).

6. You can apply several MSI properties simultaneously, as in the following example:

```
Msiexec.exe INSTALLFOLDER=C:\foo INSTALLDESKTOPSHORTCUTS=1  
INSTALLSTARTMENUSHORTCUTS=0 ARPSYSTEMCOMPONENT=1 NOCHANGEPSPOLICY=1 /i  
corex86.msi
```

If you run this command line, the Core X86 package will be installed into C:\foo, icons will be added to the Desktop, but no **Start** menu shortcut will be added. Furthermore, this package will not be listed in the **Uninstall or change a program** interface (**Add/Remove Programs**) and the PowerShell Execution Policy will not be updated.

### ***To uninstall Safeguard Authentication Services components from the Windows command line***

1. To uninstall the Control Center, enter the following:

```
msiexec /uninstall cc.msi
```

**NOTE:** You can specify either /uninstall or /x.

If you manually install MSI files, take care to uninstall them in the reverse order that they are installed. For example, if you install CoreX86 and AducExtensionsx86, remove them in this order: AducExtensionsx86, then Corex86.

## **Configure Active Directory**

To utilize full Active Directory functionality, when you install Safeguard Authentication Services in your environment, One Identity recommends that you prepare Active Directory to store the configuration settings that it uses. Safeguard Authentication Services adds the UNIX properties of Active Directory users and groups to Active Directory and allows you to map a UNIX user to an Active Directory user. This is a one-time process that creates the Safeguard Authentication Services application configuration in your forest.

**NOTE:** To use the Safeguard Authentication Services Active Directory Configuration Wizard, you must have rights to create and delete all child objects in the Active Directory container.

If you do not configure Active Directory for Safeguard Authentication Services, you can run your Safeguard Authentication Services client agent in Version 3 Compatibility Mode, which allows you to join a host to an Active Directory domain.

For more information, see For more information, see [Version 3 Compatibility Mode](#) on page 12..

You can also create the Safeguard Authentication Services application configuration from the UNIX command line, if you prefer. For more information, see [Creating the application configuration from the UNIX command line](#) on page 22..

## Configuring Active Directory

The first time you install Safeguard Authentication Services in your environment, One Identity recommends that you perform this one-time Active Directory configuration step to utilize full Safeguard Authentication Services functionality.

**NOTE:** If you do not configure Active Directory for Safeguard Authentication Services, you can run your Safeguard Authentication Services client agent in Version 3 Compatibility Mode, which allows you to join a host to an Active Directory domain.

For more information, see For more information, see [Version 3 Compatibility Mode](#) on page 12..

### **To configure Active Directory for Safeguard Authentication Services**

1. In the **Safeguard Authentication Services Active Directory Configuration Wizard Welcome** dialog, click **Next**.
2. In the **Connect to Active Directory** dialog:
  - a. Provide Active Directory login credentials for the wizard to use for this task:
    - Select **Use my current AD logon credentials** if you are a user with permission to create a container in Active Directory.
    - Select **Use different AD logon credentials** to specify the Active Directory credentials of another user, enter the **User name** and **Password**.

**NOTE:** The wizard does not save these credentials; it only uses them for this setup task.

- b. Indicate how you want to connect to Active Directory:

Select whether to connect to an **Active Directory** domain controller or One Identity **Active Roles Server**.

**NOTE:** If you have not installed the One Identity Active Roles Server Console

- on your computer, the **ActiveRoles Server** option is not available.
- c. Optionally enter the domain or domain controller and click **Next**.
  3. In the **License Safeguard Authentication Services** dialog, for **Add a license**, browse to select your license file and click **Next**.

For more information about licensing requirements, see [About licenses](#) on page 3.

**NOTE:** You can add additional licenses later from **Safeguard Authentication Services Control Center > Preferences > Licensing**.

4. In the **Configure Settings in Active Directory** dialog, accept the default location in which to store the configuration or browse to select the Active Directory location where you want to create the container and click **Setup**.

**NOTE:** You must have rights to create and delete all child objects in the selected location. For more information on the structure and rights required see [Windows Permissions](#).

5. Once you have configured Active Directory for Safeguard Authentication Services a message like this displays: You've successfully completed the setup. Click **Close**.

The Control Center opens. You are now ready to configure your UNIX Agent Components.

Proceed to [Configure UNIX agent components](#)

## About Active Directory configuration

The first time you install or upgrade the Safeguard Authentication Services Windows components in your environment, One Identity recommends that you configure Active Directory for Safeguard Authentication Services to utilize full functionality. This is a one-time Active Directory configuration step that creates the application configuration in your forest. Safeguard Authentication Services uses the information found in the application configuration to maintain consistency across the enterprise. Without the application configuration, store UNIX attributes in the RFC2307 standard attributes to achieve the most functionality.

**NOTE:** If you do not configure Active Directory for Safeguard Authentication Services, you can run your client agent in Version 3 Compatibility Mode, which allows you to join a host to an Active Directory domain.

For more information, see [For more information, see Version 3 Compatibility Mode](#) on page 12..

The Safeguard Authentication Services application configuration stores the following information in Active Directory:

- Application Licenses
- Settings controlling default values and behavior for UNIX-enabled users and groups
- Schema configuration

The UNIX agents use the Active Directory configuration to validate license information and determine schema mappings. Windows management tools read this information to

determine the schema mappings and the default values it uses when UNIX-enabling new users and groups.

The Safeguard Authentication Services application configuration information is stored inside a container object with the specific naming of: `cn={786E0064-A470-46B9-83FB-C7539C9FA27C}`. The default location for this container is `cn=Program Data,cn=Quest Software,cn=Authentication Services,dc=<your domain>`. This location is configurable.

There can only be one Active Directory configuration per forest. If Safeguard Authentication Services finds multiple configurations, it uses the one created first as determined by reading the `whenCreated` attribute. The only time this would be a problem is if different groups were using different schema mappings for UNIX attributes in Active Directory. In that case, standardize on one schema and use local override files to resolve conflicts.

You can use the `Set-QasUnixUser` and `Set-QasUnixGroup` PowerShell commands to migrate UNIX attributes from one schema configuration to another. Refer to the PowerShell help for more information.

The first time you run the Control Center, the Safeguard Authentication Services Active Directory Configuration Wizard walks you through the setup.

**NOTE:** You can also create the Safeguard Authentication Services application configuration from the UNIX command line, if you prefer.

For more information, see [For more information, see \*Creating the application configuration from the UNIX command line\* on page 22.](#)

You can modify the settings using **Safeguard Authentication ServicesControl Center > Preferences**. To change Active Directory configuration settings, you must have rights to Create Child Object (container) and Write Attribute for `cn`, `displayName`, `description`, `showInAdvancedViewOnly` for the Active Directory configuration root container and all child objects.

In order for UNIX clients to read the configuration, authenticated users must have rights to read `cn`, `displayName`, `description`, and `whenCreated` attributes for container objects in the application configuration. For most Active Directory configurations, this does not require any change.

The following table summarizes the required rights.

**Table 2: Safeguard Authentication ServicesRequired rights**

<b>Rights required</b>	<b>For user</b>	<b>Object class</b>	<b>Attributes</b>
Create Child Object	Safeguard Authentication Services Administrators Only	Container	<code>cn</code> , <code>displayName</code> , <code>description</code> , <code>showInAdvancedViewOnly</code>
Write Attribute	Safeguard Authentication Services Administrators Only	Container	
Read Attribute	Authenticated Users	Container	<code>cn</code> , <code>displayName</code> , <code>description</code> , <code>whenCreated</code>

At any time you can completely remove the Safeguard Authentication Services application configuration using the `Remove-QasConfiguration` cmdlet. However, without the application configuration, Safeguard Authentication Services Active Directory-based management tools do not function.

## Join the host to AD without the Safeguard Authentication Services application configuration

You can install the Safeguard Authentication Services Agent on a UNIX system and join it to Active Directory without installing Safeguard Authentication Services on Windows and setting up the Safeguard Authentication Services Application Configuration.

The Safeguard Authentication Services 4.x client-side agent required detection of a directory-based Application Configuration data object within the Active Directory forest in order to join the host computer to the Active Directory Domain. Safeguard Authentication Services 4.0.2 removed this requirement for environments where directory-based User and/or Group identity information is not needed on the host UNIX computer. These environments include full Mapped-User environments, GSSAPI based authentication-only environments, or configurations where the Safeguard Authentication Services agent will auto-generate posix attributes for Active Directory Users and Groups objects.

### Version 3 Compatibility Mode

When upgrading to or installing Safeguard Authentication Services 4.x, you can choose not to configure Active Directory for Safeguard Authentication Services and run your Safeguard Authentication Services client agent in Version 3 Compatibility Mode. While this prevents you from running the Control Center and accessing its many features and tools, you can join a host to an Active Directory domain when operating in Version 3 Compatibility Mode.

**NOTE:** When you run the `join` command without first creating a One Identity Application Configuration, Safeguard Authentication Services displays a warning.

Without the Safeguard Authentication Services application configuration the following information is stored locally:

- Application Licenses
- Settings controlling default values and behavior for UNIX-enabled users and groups
- Schema configuration

#### Best practice

Because Version 3 Compatibility Mode does not allow you run the Control Center and access its many features and tools, One Identity recommends that you create the application configuration so you can utilize full Safeguard Authentication Services functionality.

There are two ways to create the application configuration:

- When you start the Control Center from a Windows workstation, the **Set up Safeguard Authentication Services Active Directory Configuration Wizard** starts automatically to lead you through the process of configuring Active Directory for Safeguard Authentication Services.
- Alternatively, you can run `vastool configure ad` from the UNIX command line to create the One Identity Application Configuration in Active Directory.

## Installing and joining from the UNIX command line

You can manually install the Safeguard Authentication Services agent on each UNIX, Linux, or macOS host from the command line.

This section walks you through the process of installing the Safeguard Authentication Services UNIX agent directly from the command line. For information about installing, upgrading, and uninstalling the Safeguard Authentication Services agent on supported platforms in an enterprise environment using platform package management tools, see [Enterprise package deployment](#) on page 62.

Before installing and configuring the Safeguard Authentication Services UNIX agent, One Identity recommends that you run the `preflight` tool to check a host's suitability to run Safeguard Authentication Services. After you determine that the UNIX host is ready, run the Safeguard Authentication Services installation script, `install.sh`, to install the UNIX/Linux agent.

### Verifying package signature

All packages shipped by One Identity come with a signature. Signature verification depends on the platform:

- MacOS packages are signed by an Apple developer certificate.
- Windows packages are signed by a Microsoft developer certificate.
- Linux, FreeBSD, AIX, Solaris and HP-UX packages are signed with a PGP key.

You can find the public key at [pgp.mit.edu](http://pgp.mit.edu) and at [keyserver.ubuntu.com](http://keyserver.ubuntu.com).

To fetch the public key, use its id:

```
gpg --keyserver <keyserver> --recv C5C4EC20AFB5B8E678085F81B161CD624417450C
```

You can also find the same public key in the `oneidentity_pgpkey.pub` file. To import it, use the following command:

```
gpg --import oneidentity_gpgkey.pub
```

### **To verify package signature**

1. Download the public key.
2. Verify the files.
  - For platforms with separate .sig file signatures, use gpg2:

```
gpg --verify <file>.sig <file>
```

- For rpm packages, import the public key into the rpm's database:

```
gpg --export -a "C5C4EC20AFB5B8E678085F81B161CD624417450C" >pubkey
```

```
rpm --import pubkey
```

And verify with:

```
rpm --checksig --verbose <file>
```

- For debian packages, use debsig-verify.

## **The pre-installation diagnostic tool**

One Identity provides the `preflight` utility to check a host's suitability to run Safeguard Authentication Services by verifying a number of environmental considerations necessary for joining an Active Directory domain.

This utility obtains answers to the following questions:

- Does Safeguard Authentication Services support the host on which this utility is being run?
- Are the operating system and any patches at requisite levels?
- Is there at least one visible domain controller (DC)?
- Are global catalogs available on any of the domain controllers?
- Are all services needed by Safeguard Authentication Services available?
- Is an Safeguard Authentication Services application configuration set up on the target domain?

The `preflight` command-line utility performs the following verifications.

## Install checks:

- Check for supported operating system and correct operating system patches.
- Check for sufficient disk space to install Safeguard Authentication Services.

## Join checks:

- Check that the hostname of the system is not localhost.
- Check if the name service is configured to use DNS.
- Check `resolv.conf` for proper formatting of name service entries and that the host can be resolved.
- Check for a name server that has the appropriate DNS SRV records for Active Directory.
- Detect a writable domain controller with UDP port 389 open.
- Detect Active Directory site, if available.
- Check if TCP port 464 is open for Kerberos kpasswd.
- Check if UDP port 88 and TCP port 88 are open for Kerberos traffic.
- Check if TCP port 389 is open for LDAP.
- Check for a global catalog server and if TCP port 3268 is open for communication with global catalog servers.
- Check for a valid time skew against Active Directory.
- Check for the Safeguard Authentication Services application configuration in Active Directory.

## Post-join checks:

- Check if TCP port 445 is open for Microsoft CIFS traffic.

You can find the `preflight.sh` script at the root of the ISO. This script runs the correct `preflight` version for your system.

The most important options and arguments to `preflight` are:

- **domain-name**

The domain you want to join with Safeguard Authentication Services.

- **-u username**

An identity with administrator rights for the Active Directory domain you want to join.

**NOTE:** The `preflight` utility does not make any changes to your system.

# Running preflight

You can verify whether your host is suitable to run Safeguard Authentication Services by running a preflight check.

## To run preflight

1. Mount the Safeguard Authentication Services distribution media.
2. Enter the following command at the root of the Safeguard Authentication Services ISO:

```
# ./preflight.sh -u Administrator example.com
```

where `Administrator` is your user name and `example.com` is the name of your domain.

By default, `preflight` outputs the results of the verifications for the three types of checks (Install checks, Join checks, and Post-join checks) to the console. Run the `preflight` utility with the `--verbose` option to obtain detailed information about the various checks in those categories.

The last line of the output tells you whether you are ready to continue deploying Safeguard Authentication Services.

If you did not get a Preflight Checks complete with status Success message, correct any failures indicated before continuing with the Safeguard Authentication Services installation. Be aware of any "Advisories" that it returns, as they may effect your ability to install or join.

**NOTE:** If you receive the message Unable to locate Safeguard Authentication Services Application Configuration, you can ignore that error at this stage, and proceed with the Safeguard Authentication Services installation. The Safeguard Authentication Services Active Directory Configuration Wizard starts automatically to help you configure Active Directory for Safeguard Authentication Services the first time you start the Control Center. Or, you can create the Safeguard Authentication Services application configuration from the command line, as explained in [Creating the application configuration from the UNIX command line](#) on page 22.

**NOTE:** For information about other preflight options, either run `preflight --help` or refer to the *preflight man page* located in the `docs` directory of the installation media. See [Resolving preflight failures](#) on page 54 for additional help in resolving issues.

# The install script

Follow the steps in this topic if you are installing a Safeguard Authentication Services 6.0 LTS for the first time; that is, if you are not upgrading from VAS 3.5.

The Safeguard Authentication Services installation script, `install.sh`, installs Safeguard Authentication Services, joins the domain, and allows you to install licenses. You can run

the install script in interactive mode by using the `-i` option. This provides you with a menu of valid operations to perform, including **Running preflight**.

You can also automate the installation process by running `install.sh` in "unattended" mode using `-q` option. In this mode you may specify a set of commands for the script to perform.

**NOTE:** For more information on the Safeguard Authentication Services installation script, run:

```
install.sh --help
```

## Installing the Safeguard Authentication Services agent

This section describes how to install the Safeguard Authentication Services agent with the installation script.

### *To install the Safeguard Authentication Services agent with the installation script*

1. Log in and open a root shell.
2. Mount the installation ISO for your selected platform and navigate to the mount point.
3. Run `install.sh` by entering the following command:

```
# ./install.sh vasclnt
```

**NOTE:** For a list of the Safeguard Authentication Services Agent installation commands, see [Installing the agent package](#) on page 62.

After installing Safeguard Authentication Services some services such as `cron`, `sshd`, and `gdm` may need to be restarted in order to reload NSS configuration. If you are unsure of which services to restart, reboot the system.

## Installation script options

If you run `install.sh` with no option, it installs (or upgrades) Safeguard Authentication Services and Safeguard Authentication Services Group Policy, installs the license, and joins the domain.

The following is a list of the available options to the Safeguard Authentication Services install script.

**Table 3: install.sh: Options**

Option	Function
-d	Turn on debug.
-h	Help; displays usage information including a brief summary of options.
--help	Displays full script help.
-v, --version	Displays version and lists products available on this ISO.
-l path	License; path to One Identity license file to copy (unattended mode). Not valid with -i (interactive mode).
-p	Specify alternate ISO path to search for install packages.
-t	Test host and ISO and report on what is installed and available.
<none>	Simple mode.
-i	Interactive mode; provides a menu showing choices based on existing Safeguard Authentication Services software installation and includes a help mode.
-q	Unattended mode; executes script in unattended (automatic) mode; requires other options.
-a	Accept License; signals acceptance of One Identity LLC EULA.

**Table 4: Special commands**

Command	Description
upgrade	Upgrades all products on the system.
remove	Removes all products from the system.
join	Executes interactive <code>vasjoin.sh</code> script. Not valid with -q (Unattended mode).
preflight	Executes interactive preflight test. Not valid with -q (Unattended mode).
license	Executes interactive install of license files (or use -l option). Not valid with -q (Unattended mode).

In unattended mode, the following arguments are useful for scripting the components you want to install or uninstall.

**Table 5: install.sh: Unattended mode arguments**

Argument	Function
vascert	Installs or upgrades Safeguard Authentication Services Certificate Autoenrollment.

Argument	Function
vasclnt	Installs or upgrades Safeguard Authentication Services agent.
vasdev	Installs or upgrades Safeguard Authentication Services SDK.
vasgp	Installs or upgrades Safeguard Authentication Services Group Policy agent.
vasproxy	Installs or upgrades Safeguard Authentication Services Proxy daemon.
vassc	Installs or upgrades Safeguard Authentication Services for Smart Cards agent.
vasyp	Installs or upgrades Safeguard Authentication Services YP server.
novascert	Uninstalls Safeguard Authentication Services Certificate Autoenrollment.
novasclnt	Uninstalls the Safeguard Authentication Services agent.
novasdev	Uninstalls the Safeguard Authentication Services SDK.
novasgp	Uninstalls the Safeguard Authentication Services Group Policy agent.
novasproxy	Uninstalls the Safeguard Authentication Services Proxy daemon.
novassc	Uninstalls the Safeguard Authentication Services for Smart Cards agent.
novasyp	Uninstalls the Safeguard Authentication Services YP server.

## Licensing Safeguard Authentication Services

You must have the Safeguard Authentication Services license installed for full Safeguard Authentication Services functionality on UNIX.

There are four ways to manage licenses:

- **Using the Control Center**

**TIP:** One Identity recommends using this method. For more information, see [Adding licenses using the Control Center](#).

- **Using the Safeguard Authentication Services Group Policy utilities**

For more information, see *Licensing Policy* in the *Safeguard Authentication Services Administration Guide*.

- **Running the install.sh script with the -l option**

This allows you to enter a path. The script then places the license in the proper location. For more information, see [Installation script options](#).

- **Installing Licenses from the command line**

For more information, see [Installing licenses from the command line](#).

To obtain a license, use the [Licensing Assistance](#) page on the One Identity support page or contact your account representative.

## Verifying license information

You can use Privilege Manager for Unix on UNIX with all its functionalities only if the Privilege Manager for Unix license is installed. For more information on licenses, see [Licensing Safeguard Authentication Services](#).

### **To verify that you have a valid Safeguard Authentication Services license**

1. Run the following `vastool` command:

```
vastool license -q
```

2. You will see an output similar to the following if you have a valid license installed:

```
Number of Unix Enabled users in use:    150
---QAS---
Number of Licensed Unix Enabled Users: 1000
Valid licenses:                        1
```

## Installing licenses from the command line

With root privileges, you can manually install a valid license by copying the new license file to the `licenses` directory on the UNIX host.

### **To install a Safeguard Authentication Services license manually**

1. Copy the license file to the `/etc/opt/quest/vas/licenses` directory.
2. Ensure the permissions on the license file are set to 0644.
3. Restart `vasd` as root by running the command corresponding to your platform:

- **Linux/Oracle Solaris:**

```
/etc/init.d/vasd restart
```

- **HPUX:**

```
/sbin/init.d/vasd restart
```

- **AIX:**

```
/etc/rc.d/init.d/vasd restart
```

- **macOS:**

```
launchctl unload /Library/LaunchDaemons/com.quest.vasd.plist  
launchctl load /Library/LaunchDaemons/com.quest.vasd.plist
```

## Creating the application configuration from the UNIX command line

Before you join a UNIX client to an Active Directory domain, One Identity recommends that you create the application configuration in the domain to which you are joining to utilize full Safeguard Authentication Services 6.0 LTS functionality. While the Safeguard Authentication Services Active Directory Configuration Wizard starts automatically to help you configure Active Directory for Safeguard Authentication Services the first time you start the Control Center, you do not need to have a Windows console to create the application configuration. You can run the `vastool configure ad` command from the UNIX command line to create it. This is typically a one-time process.

**NOTE:** You only need to create one Safeguard Authentication Services application configuration per forest. For more information, see [For more information, see Version 3 Compatibility Mode](#) on page 12..

### ***To create the Safeguard Authentication Services application configuration***

1. Run the following command from the UNIX command line:

```
# /opt/quest/bin/vastool ad -u <user> configure -d <domain>
```

By default, Safeguard Authentication Services creates the application configuration in the Program Data container; however, if you do not have rights to create an organizational unit in the Program Data container, you can create the Safeguard Authentication Services application configuration in any location you have rights to by specifying the DN (distinguished name) of the creation location, as follows:

```
vastool -u <user> configure -d <domain> ou cn=myou,dc=example,dc=com
```

2. Enter the user's password when prompted.

## Changing the schema configuration mode

When you create the Safeguard Authentication Services application configuration, you set the global schema configuration mode to R2 by default. However, you can optionally configure Safeguard Authentication Services for "schemaless" operation using the `schema configure` command.

### **To switch to a schemaless configuration**

1. Run the following command:

```
# /opt/quest/bin/vastool -u <user> schema -d <domain> configure schemaless
```

The `schema configure` command only allows you to set the schema mode to either R2 or "schemaless" modes. To set the schema configuration to any other mode, you must do so from the Control Center **Preferences**.

2. Enter the user's password when prompted.

## Joining the domain

For full Safeguard Authentication Services functionality on UNIX, you must join the UNIX system on which you installed the Safeguard Authentication Services agent to the domain. You can join an Active Directory domain either by running `vastool join` from the command line or the interactive join script, `vasjoin.sh`.

Before you join the UNIX host to the Active Directory domain, you may want to determine if you are already joined.

### **To determine if you are joined to an Active Directory domain**

1. Run the following command:

```
# /opt/quest/bin/vastool info domain
```

If you are joined to a valid domain this command returns the domain name. If you are not joined to a domain, you will see the following error:

```
ERROR: No domain could be found.  
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm  
default_realm not configured in vas.conf. Computer may not be joined  
to domain
```

## Joining the domain using VASTOOL

You can join your UNIX host to Active Directory with the `vastool join` command directly from the command line.

Before you join the Safeguard Authentication Services agent to the Active Directory domain, collect the following information:

- The DNS name of the Active Directory domain of which you want the Safeguard Authentication Services agent to be a member.
- The user name and password of a user that has sufficient administrative privileges to create computer objects in Active Directory.

### To join Active Directory using `vastool join`

1. Run the following command as the root user at a shell prompt:

```
# /opt/quest/bin/vastool -u <user> join <domain-name>
```

2. Enter the user's password when prompted.

The `vastool join` results are shown on the standard shell output.

**NOTE:** `vastool join` supports many options that allow you to customize the way the computer is joined to the domain. You can specify the name of the computer object. You can join to a specific organizational unit or use a pre-created computer object. For a list of all `vastool join` options, see the *vastool man page*.

## Joining the domain using VASJOIN script

Rather than using the `vastool join` command from the command line, you can join your UNIX host to Active Directory using the interactive join script, `vasjoin.sh`. The script walks you through the domain join process, calling the `vastool join` command.

The `vasjoin.sh` script is in `/opt/quest/libexec/vas/scripts/` directory. You can use most of the standard `vastool join` command options when running it. However, you can run the join script with no options; it only requires that you supply the domain name and the name of a user with sufficient Active Directory privileges to perform the join.

**Table 6: Common `vasjoin` script options**

Option	Function
-h	Help; displays options including how to pass <code>vastool join</code> options.
-q	Unattended or "quiet" mode; displays less verbose: no explanations, asks no questions.
-i	Interactive mode; prompts for common options.
<none>	Simple mode; installs <code>vasclnt</code> and <code>vasgp</code> with options to add license and join domain.

## To join Active Directory using the *vasjoin* script

1. Run the script as the root user at a shell prompt, as follows:

```
/opt/quest/libexec/vas/scripts/vasjoin.sh
```

The script ensures that your local host's time is synchronized with that of the controller in the domain you want to join (to satisfy Kerberos), then performs the join for you by running `vastool join` as follows:

```
vastool -u <username> join <domain-name>
```

2. Follow the prompts to complete the join process.

Run the script in interactive mode as follows:

```
/opt/quest/libexec/vas/scripts/vasjoin.sh -i
```

In interactive mode, it prompts you for specific information and allows you to either save the resulting `vastool join` command in a script or execute the command immediately.

The script presents defaults as part of the prompting and, if you accept them all, the result is identical to running the script in simple mode.

The information gathered by the full, interactive mode of `vasjoin.sh` includes the following:

- Specific domain controllers to use
- Domain to join
- User, usually administrator, to use in joining
- Keytab file
- Confirm fixing of Kerberos clock skew, if any
- Overwrite your host's existing Active Directory ComputerName object
- Change the name of the AD ComputerName object
- AD container in which to put the ComputerName object
- Site name
- UPM mode (yes or no)
- User search path on which to look for Active Directory users
- Alternate group search path
- Workstation mode (yes or no)
- Alternate domains in which to search if you want cross-domain logins
- Self-enrollment of existing `/etc/passwd` users (yes or no)
- Shows path to `lastjoin` (`/etc/opt/quest/vas/lastjoin`)

The lastjoin file contains something similar to:

```
/opt/quest/bin/vastool -u administrator join -f acme.com
```

## Dynamic DNS update tool

When Safeguard Authentication Services joins a new computer to a domain, it becomes known to the LDAP and Kerberos protocols, but not to DNS. This is because the IP address of the host is not directly under the control of this part of Active Directory.

Although Active Directory comes with an integrated DHCP and DNS servers, some sites run their own DHCP servers. This means that the leased IP addresses must be communicated to Active Directory's DNS server through another (often manual) means.

The One Identity Dynamic DNS Update Tool, `dnsupdate`, performs this communication. It can automatically and securely inform Active Directory's DNS server of any host IP address changes due to DHCP lease acquisition and renewal.

Because `dnsupdate` uses Kerberos to authenticate itself to the DNS server, only the computer joined with that name can update its record.

When you run the Safeguard Authentication Services installation script, `install.sh`, in interactive mode (the `-i` option), it gives you an option to install the One Identity Dynamic DNS Update Tool. Dynamic DNS automatically integrates into the host's native DHCP client infrastructure to securely update DNS servers when its IP address changes. For more information about running the `install.sh` script, see [Installation script options](#) on page 18.

**NOTE:** If Pointer Record (PTR) updates are being rejected, it may be because the DHCP server is doing the update already. Refer to the documentation for the DHCP server being used in your environment. The Microsoft DHCP server does updates on behalf of the client and this is controlled by the Fully Qualified Domain Name (FQDN) option. Please refer to the Microsoft Active Directory DNS/DHCP documentation.

## Getting started with Safeguard Authentication Services

Once you have successfully installed Safeguard Authentication Services, you will want to learn how to do some basic system administration tasks.

### Getting acquainted with the Control Center

Safeguard Authentication Services consists of plugins, extensions, security modules, and utilities spread across nearly every operating system imaginable. The Control Center pulls those parts together and provides a single place for you to find the information and resources you need.

Control Center installs on Windows and is a great starting place for new users to get comfortable with some of Safeguard Authentication Services' capabilities.

You can launch the Control Center from the **Start** menu or by double-clicking the desktop icon, or by double-clicking the Control Center application file from %SystemDrive%\Program Files (x86)\Quest Software\Authentication Services.

**Table 7: Control Center: Navigation links**

Control Center pane	Description
Home	The <b>Welcome</b> page provides information about how to use the Control Center tools and features.
Group Policy	The Control Center provides the ability to search on Active Directory Group Policy Objects that have UNIX and macOS settings defined. Also provides links to edit these GPOs and run reports that show the detailed settings of the Group Policy Objects.
Tools	The Control Center provides links to additional tools and resources

Control Center pane	Description
	available with Safeguard Authentication Services. A great starting place for anyone new to the product.
Preferences	The Control Center allows you to centrally manage the default values generated by the various Safeguard Authentication Services management tools, including the ADUC snap-in, the PowerShell cmdlets, and the UNIX command-line tools.
Log into remote host	The Control Center provides a simple SSH client (built on PuTTY) for remote access to UNIX systems; simplifies new installs from having to find and install a separate PuTTY client.

To run the Control Center, you must be logged in as a domain user. To make changes to global settings, you must have rights in Active Directory to create, delete, and modify objects in the Safeguard Authentication Services configuration area of Active Directory.

## Group Policy

Microsoft Group Policy provides excellent policy-based configuration management tools for Windows. Group Policy allows you to manage UNIX resources in much the same way. Group Policy allows you to consolidate configuration management tasks by using the Group Policy functionality of Microsoft Windows Server to manage UNIX operating systems and UNIX application settings.

To open Group Policy, click **Group Policy** on the left navigation panel of the Safeguard Authentication Services Control Center.

## Filtering the list of GPOs

This section describes how to filter the list of Group Policy Objects.

### *To filter the list of GPOs*

1. Open the Control Center and click **Group Policy** on the left navigation pane.
2. Expand the **Filter Options** section.
3. Enter all or part of a name to filter the list of GPOs.
4. Open the **Domain** drop-down menu to choose a domain.
5. Select the **UNIX Settings** or **Mac Settings List Only** options to further filter the GPO list.

If you select both options, only the GPOs configured for both UNIX and macOS display.

## Editing a GPO

This section describes how to edit a group policy object.

### **To edit a group policy object**

1. Open the Control Center and click **Group Policy** on the left navigation pane.
2. From the **Group Policy** window, select a GPO in the list and click **Actions > Edit GPO**.

The **Group Policy Object Editor** opens for the selected GPO.

**NOTE:** For more information about the group policies, see the *Safeguard Authentication Services Administration Guide*, which can be found on the [Safeguard Authentication Services - Technical Documentation](#) page of the One Identity support site.

## Generating a settings report

A settings report displays all of the Safeguard Authentication Services Group Policy object settings that apply to UNIX or macOS systems.

### **To generate a settings report**

1. Open the Control Center and click **Group Policy** on the left navigation pane.
2. From the **Group Policy** window, select a GPO Name and click **Actions > Settings Report**.

An HTML report of the currently configured UNIX and macOS settings displays.

**NOTE:** You can select multiple GPOs to run several reports simultaneously.

## Showing files

You can display the Group Policy Templates for the selected GPO by performing the following steps.

### **To open the Windows Explorer**

1. Open the Control Center and click **Group Policy** on the left navigation pane.
2. From the **Group Policy** window, select a GPO in the list and click **Actions > Show Files**.

The Windows Explorer opens and displays the Group Policy Templates for the selected GPO.

## Launching GPMC

This section describes how to launch the Group Policy Management Console. For more information on the GPMC, see [Integrating with GPMC](#).

**NOTE:** Microsoft does not support Group Policy Management Console (GPMC) on 64-bit platforms of Windows. Because of this, One Identity does not support managing group policies through the Control Center on Windows 2003 64-bit and Windows 2003 R2 64-bit, XP 64-bit platforms. See [Group Policy Management Console with Service Pack 1](#) for more information.

### **To launch the Group Policy Management Console**

1. Open the Control Center and click **Group Policy** on the left navigation pane.
2. From the **Group Policy** window, click **Actions** > **Launch GPMC**.

## Tools

The **Tools** link on the Control Center gives you access to:

- **Safeguard Authentication Services**  
Direct links to installed applications and tools related to Safeguard Authentication Services.
- **Additional One Identity Products**  
Direct links to other One Identity product plugins. The **Additional One Identity Products** link is only available if you have installed other One Identity products such as Defender, Safeguard Authentication Services for Smart Cards, or One Identity Active Roles.
- **Other Tools**  
Direct links to tools related to Safeguard Authentication Services. The **Other Tools** link is only available if you have installed the Group Policy Management Console.
- **Documentation**  
Direct links to the Safeguard Authentication Services documentation.

## Preferences

Safeguard Authentication Services stores certain preferences and settings in Active Directory. This information is used by Safeguard Authentication Services clients and management tools so that behavior remains consistent across all platforms and tools. The **Preferences** window allows you to configure these settings and preferences:

- [Licensing](#)
- [Display specifiers](#)
- [Global UNIX Options](#)
- [Logging Options](#)
- [Schema Attributes](#)
- [Management Console for UNIX](#)
- [UNIX Attributes](#)

## Licensing


The **Licensing** section of the **Preferences** window in the Control Center displays a list of installed license files. You can add and remove license files at any time. The license files are stored in Active Directory and Safeguard Authentication Services UNIX hosts automatically download and apply new license files from Active Directory.

For more information about licensing requirements, see [About licenses](#) on page 3.

## Adding licenses using the Control Center

This section describes how to add licenses using the Control Center. For more information on licenses, see [Licensing Safeguard Authentication Services](#).

### *To add licenses using the Control Center*

1. Open the Control Center and click **Preferences** on the left navigation pane.
2. Expand the **Licensing** section. The list box displays all licenses currently installed in Active Directory. You can click  to see the detail information for a license and copy the information, if needed.
3. Under **Options**, select **Add a license**.
4. Browse for one or more license files and click **Open**. The license appears in the list box.

If the license is not valid, a message like the following displays: Failed to add license. The license file specified is not a valid license. The license number, the product, the reason for the failure (such as not valid or duplicate), and the path where the license file resides is shown.

**NOTE:** UNIX hosts check for new licenses when the host is joined to the domain or every 24 hours by default. This can be changed by modifying the configuration-refresh-interval setting in vas.conf.

To remove a license, select the license and click **Remove license**.

To restore a removed license, click **Undo Remove**.

## Display specifiers

Display specifiers are Active Directory objects that provide information about how other objects in the directory display in client applications.

**NOTE:** The **Register Display Specifiers** link is only displayed in the Control Center when display specifiers are not already registered with Active Directory. If the display specifiers are registered, Control Center does not display the link.

## Registering display specifiers

Because it is common to use the **Find** dialog in ADUC to manage users and groups, One Identity recommends that you register display specifiers with Active Directory. Registering display specifiers provides the following benefits:

- UNIX Account properties appear in ADUC **Find** dialog results.
- UNIX Personality objects are displayed correctly in ADUC. This only applies if the UNIX Personality schema has been installed.

**NOTE:** You must have Enterprise Administrator rights to register display specifiers.

You can inspect exactly which changes are made during the display specifier registration process by viewing the `DsReg.vbs` script found in the Safeguard Authentication Services installation directory. You can use this script to unregister display specifiers at a later time.

### *To register display specifiers with Active Directory*

1. From a Windows management workstation with Safeguard Authentication Services installed, navigate to **Start > Quest Software > Safeguard Authentication Services > Control Center**.
2. Click **Preferences** on the left navigation panel.
3. Expand the **Display Specifiers** section.

**NOTE:** The **Register Display Specifiers** link is only displayed in the Control Center when display specifiers are not already registered with Active Directory. If the display specifiers are registered, Control Center does not display the link.

4. Click the **Register Display Specifiers** link to register display specifiers with Active Directory.

While it is registering the display specifiers with Active Directory, Control Center displays a progress indicator. When the process is complete, Control Center indicates that display specifiers are registered.

Alternatively, you can register display specifiers from the command line, as follows:

- a. Log in as a user with Enterprise Administrator rights.
- b. Open a command prompt, navigate to the Safeguard Authentication Services installation directory, and run this command:

```
DsReg.vbs /add
```

**NOTE:** To register One Identity Active Directory display specifiers with One Identity Active Directory, navigate to the installed location for Safeguard Authentication Services and run the following command:

```
DsReg.vbs /add /provider:EDMS
```

You must install the One Identity Active Directory management package locally or DsReg.vbs returns an "Invalid Syntax" error.

To see all the DsReg.vbs options, run the following command:

```
DsReg.vbs /help
```

## Unregistering display specifiers

If you want to unregister display specifiers, perform the following steps.

**NOTE:** You must have Enterprise Administrator rights to unregister display specifiers.

### ***To unregister display specifiers in Active Directory***

1. Log in as a user with Enterprise Administrator rights.
2. Open a command prompt and navigate to the Safeguard Authentication Services installation directory.
3. Run the DsReg.vbs script with the /remove option:

```
DsReg.vbs /remove
```

**NOTE:** To unregister display specifiers with One Identity Active Roles, run the following command:

```
DsReg.vbs /remove /provider:EDMS
```

To see all the DsReg.vbs options, run the following command:

```
DsReg.vbs /help
```

A SUCCESS message appears indicating that the display specifiers were removed successfully.

## Display specifier registration tables

Display specifiers are stored in the Active Directory configuration partition under the DisplaySpecifiers container. The DisplaySpecifiers container has child containers named for a corresponding locale ID. US English display specifiers are in cn=409,cn=DisplaySpecifiers,cn=Configuration,dc=domain. The following modifications are made for each locale by the display specifier registration script, DsReg.vbs.

**Table 8: Object: User-Display**

Attribute	Change type	Value	Description
adminPropertyPages	modify, insert	10,{E399C9A2-E7ED-4DDF-9C5A-BA4EACC34316}	Registers the UNIX Account property page extension with User objects.
adminPropertyPages	modify, insert	11,{53108A01-9B68-4DFB-A16D-4945D26A38A9}	Registers the UNIX Personality property page extension with User objects.
attributeDisplayNames	modify, insert	uidNumber, UID Number	Provides a more user-friendly name for the UNIX user ID number attribute. Allows this attribute to display in the UNIX Object find dialog results.
attributeDisplayNames	modify, insert	uid, Login Name	Provides a more user-friendly name for the UNIX login name attribute. Allows this attribute to display in the UNIX Object find dialog results.
attributeDisplayNames	modify, insert	gidNumber, GID Number	Provides a more user-friendly name for the UNIX group ID number attribute. Allows this attribute to display in the UNIX Object find dialog results.
attributeDisplayNames	modify, insert	canonicalName, Path	Provides a more user-friendly name for the UNIX canonical name attribute. Allows this attribute to display in the UNIX Object find dialog results.

**Table 9: Object: Group-Display**

Attribute	Change type	Value	Description
adminPropertyPages	modify, insert	10,{E399C9A2-E7ED-4DDF-9C5A-BA4EACC34316}	Registers the UNIX Account property page extension with User objects.
attributeDisplayNames	modify, insert	gidNumber, GID Number	Provides a more user-friendly name for the UNIX group ID number attribute. Allows this attribute to display in the UNIX Object find dialog results.
attributeDisplayNames	modify, insert	canonicalName, Path	Provides a more user-friendly name for the UNIX canonical name attribute. Allows this attribute to display in the UNIX Object find dialog results.

**Table 10: Object: vintela-UnixUserPersonality-Display**

Attribute	Change type	Value	Description
cn	create object	vintela-UnixUserPersonality-Display	The display specifier object is created.
adminPropertyPages	modify, insert	10,{E399C9A2-E7ED-4DDF-9C5A-BA4EACC34316}	This registers the UNIX User Personality property page extension with user personality objects.
classDisplayName	modify, set	UNIX User Personality	Sets the friendly name of the object class. This is the text displayed in the New Object menu and elsewhere in ADUC.
creationWizard	modify, set	{57AC8F6B-5EA8-4DC9-AB9A-C0ED6420C7F9}	This registers the "New UNIX User Personality" object creation wizard. This creation wizard registration mechanism works in ADUC, but is not yet supported in Active Roles. To create

Attribute	Change type	Value	Description
			personality objects in Active Roles, use the Advanced Create Wizard and select the UNIX User Personality object class.
iconPath	modify, insert	0,vas_dua_user.ico	This is the default personality icon. This icon is installed by Safeguard Authentication Services in the %SYSTEMROOT%\system32 folder so that it is available to all applications that might need it.
iconPath	modify, insert	1,vas_dua_user_disabled.ico	This icon is not currently used.
iconPath	modify, insert	2,vas_dua_user_orphaned.ico	This icon is not currently used.
attributeDisplayNames	modify, insert	uidNumber, UID Number	Provides a more user-friendly name for the UNIX user ID number attribute. Allows this attribute to display in the UNIX Object find dialog results.
attributeDisplayNames	modify, insert	gidNumber, GID Number	Provides a more user-friendly name for the UNIX group ID number attribute. Allows this attribute to display in the UNIX Object find dialog results.
attributeDisplayNames	modify, insert	uid, UNIX Login Name	Provides a more user-friendly name for the UNIX login name attribute. Allows this attribute to display in the UNIX Object find dialog results.

Attribute	Change type	Value	Description
attributeDisplayNames	modify, insert	description, Description	Provides a more user-friendly name for the description attribute. Allows this attribute to display in the UNIX Object find dialog results.
attributeDisplayNames	modify, insert	canonicalName, Path	Provides a more user-friendly name for the UNIX canonical name attribute. Allows this attribute to display in the UNIX Object find dialog results.
attributeDisplayNames	modify, insert	managedBy, Linked To	Provides a more descriptive name for the managed by attribute to indicate how this attribute is used on personality objects. Allows this attribute to display in the UNIX Object find dialog results.

**Table 11: Object: vintela-UnixGroupPersonality-Display**

Attribute	Change type	Value	Description
cn	create object	vintela-UnixGroupPersonality-Display	The display specifier object is created.
adminPropertyPages	modify, insert	10,{E399C9A2-E7ED-4DDF-9C5A-BA4EACC34316}	This registers the UNIX User Personality property page extension with user personality objects.
classDisplayName	modify, set	UNIX Group Personality	Sets the friendly name of the object class. This is the text displayed in the New Object menu and elsewhere in ADUC.
creationWizard	modify, set	{A7C4A545-C7C8-49C8-8C96-8C665E166D0C}	This registers the "New UNIX User Personality"

Attribute	Change type	Value	Description
			object creation wizard. This creation wizard registration mechanism works in ADUC, but is not yet supported in ARS. To create personality objects in ARS, use the Advanced Create Wizard and select the UNIX User Personality object class.
iconPath	modify, insert	0, vas_unix_group.ico	This is the default personality icon. This icon is installed by Safeguard Authentication Services in the %SYSTEMROOT%\system32 folder so that it is available to all applications that might need it.
attributeDisplayNames	modify, insert	gidNumber, GID Number	Provides a more user-friendly name for the UNIX group ID number attribute. Allows this attribute to display in the UNIX Object find dialog results.
attributeDisplayNames	modify, insert	cn, Name	Provides a more user-friendly name for the UNIX login name attribute. Allows this attribute to display in the UNIX Object find dialog results.
attributeDisplayNames	modify, insert	description, Description	Provides a more user-friendly name for the description attribute. Allows this attribute to display in the UNIX Object find dialog results.

Attribute	Change type	Value	Description
attributeDisplayNames	modify, insert	canonicalName, Path	Provides a more user-friendly name for the UNIX canonical name attribute. Allows this attribute to display in the UNIX Object find dialog results.
attributeDisplayNames	modify, insert	managedBy, Linked To	Provides a more descriptive name for the managed by attribute to indicate how this attribute is used on personality objects.

## Global UNIX Options

The **Global UNIX Options** section displays the currently configured options for UNIX-enabling users and groups.

Click **Modify Global UNIX Options** to change these settings.

**NOTE:** Safeguard Authentication Services uses the **Global UNIX Options** when enabling users and groups for UNIX login.

**Table 12: UNIX user defaults**

Option	Description
Require unique User Names	Select to require a unique user login name attribute within the forest.
Require unique UID Numbers	Select to require a unique user's UNIX ID (UID) number within the forest.
Minimum UID Number	Enter a minimum value for the UNIX User ID (UID) number. Typically, you set this to a value higher than the highest UID among local UNIX users to avoid conflicts with users in Active Directory and local user accounts.
Maximum UID Number	Enter a maximum value for the UNIX User ID (UID) number. Typically, you would not change this value unless you have a legacy UNIX platform that does not support the full 32-bit integer range for UID number.
Default Primary GID Number	Enter the default value for the Primary GID number when UNIX-enabling a user.

Option	Description
Set primary GID to UID	Select to set the primary GID number to the User ID number.
Default Comments (GECOS)	Enter any text in this box.
Default Login Shell	Enter the default value for the login shell used when UNIX-enabling a user.
Default Home Directory	Enter the default prefix used when generating the home directory attribute when UNIX-enabling a user.  The default value is /home/; use a different value if your UNIX user home directories are stored in another location on the file system. Safeguard Authentication Services uses the user's effective UNIX name when generating the full home directory path.
Use lowercase User Name for Home Directory	Select to use a lower-case representation of the user's effective UNIX name when generating the full home directory path as a user is UNIX-enabled.

**Table 13: UNIX group defaults**

Option	Description
Require unique Group Names	Select to require a unique UNIX group name attribute within the forest.
Require unique GID Numbers	Select to require a unique UNIX Group ID (GID) attribute within the forest.
Minimum GID Number	Enter the minimum value for the UNIX Group ID (GID).  Typically, this is set to a value higher than the highest GID among local UNIX groups to avoid conflicts with groups in Active Directory and local group accounts.
Maximum GID Number	Enter the maximum value for the UNIX Group ID (GID).  Typically, you would not change this value unless you have a legacy UNIX platform that does not support the full 32-bit integer range for GID.

These options control the algorithms used to generate unique user and group IDs.

**Table 14: Unique IDs**

Option	Description
GUID Hash	An ID generated from a hash of the user or group object GUID attribute.  This is a fast way to generate an ID that is usually unique. If the

Option	Description
	generated value conflicts with an existing value, the ID is re-generated by searching the forest.
Samba Algorithm	An ID generated from the SID of the domain and the RID of the user or group object.  This method works well when there are few domains in the forest. If the generated value conflicts with an existing value, the ID is re-generated by searching the forest.
Legacy Search Algorithm	An ID generated by searching for existing ID values in the forest. This method generates an ID that is not currently in use.

Modifications you make to these **Global UNIX Options** take effect after you restart the Microsoft Management Console (MMC).

**TIP:** It is a best practice to either use the generated default IDs or set the ID manually. Mixing the two methods can lead to ID conflicts.

## Logging Options

The **Logging Options** section allows you to enable logging for all Safeguard Authentication Services Windows components. This setting only applies to the local computer. Logging can be helpful when trying to troubleshoot a particular problem. As logging causes components to run slower and use more disk space, set the **Log Level** to **Disabled** when you are finished troubleshooting.

### Enabling debug logging on Windows

This section describes how to enable debug logging on Windows.

#### ***To enable debug logging for all Safeguard Authentication Services Windows components***

1. Open Control Center and click **Preferences** on the left navigation pane.
2. Expand the **Logging Options** section.
3. Open the **Log level** drop-down menu and set the log level to **Debug**.

**Debug** generates the most log output. Higher levels generate less output. You can set the **Log level** to **Disabled** to disable logging.

4. Click  to specify a folder location where you want to write the log files.

Safeguard Authentication Services Windows components log information into the specified log folder the next time they are loaded. Each component logs to a text file named after the DLL or EXE that generates the log message.

# Schema Attributes

To view and update schema configurations, from the Control Center, select **Preferences** then **Schema Attributes**. You can customize UNIX attribute mappings as described in [UNIX Attributes](#).

## UNIX Attributes

The UNIX schema attributes are fully customizable in Safeguard Authentication Services. The **UNIX Attributes** section allows you to see which LDAP attributes are mapped to UNIX attributes. You can modify this mapping to enable Safeguard Authentication Services to work with any schema configuration. To customize the mapping, you select a schema template or specify your own custom attributes. A schema template is a pre-defined set of common mappings which adhere to common schema extensions for storing UNIX data in Active Directory.

From the Control Center, select **Preferences > Schema Attributes**. Click the **UNIX Attributes** link in the upper right to display the Customize Schema Attributes dialog.

Safeguard Authentication Services supports the following schema templates if the required schema is installed:

**Table 15: UNIX schema attributes**

Schema Template	Description
Schemaless	A template that encodes UNIX attribute data in an existing multi-valued attribute.
Windows R2	A template that uses attributes from the Windows 2003 R2 schema extension.
Services for UNIX 2.0	A template that uses attributes from the SFU 2.0 schema extension.
Services for UNIX 3.0	A template that uses attributes from the SFU 3.0 schema extension.

**TIP:** Use a schema designed for storing UNIX data in Active Directory whenever possible. Schemas designed for storing UNIX data in Active Directory include: Windows 2003 R2, SFU 2, and SFU 3. Only use "schemaless" or custom mappings if it is impossible to make schema extensions in your environment.

**NOTE:** If you are running Safeguard Authentication Services without an application configuration in your forest and your domain supports Windows R2, you can enable Safeguard Authentication Services to use the Windows R2 schema. However, note that some functionality provided by the Safeguard Authentication Services application configuration will be unavailable.

## Active Directory schema extensions

Safeguard Authentication Services stores UNIX identity and login information in Active Directory. One Identity designed Safeguard Authentication Services to provide support for the following standard Active Directory schema extensions.

**Table 16: Active Directory schema extensions**

Schema extension	Description
Windows 2003 R2 Schema	This schema extension is provided by Microsoft and adds support for the PosixAccount auxiliary class, used to store UNIX attributes on user and group objects.
Services for UNIX 2.0	Microsoft provides this schema extension with the Services for UNIX 2.0 set of tools. It adds custom attributes to user and group objects, used to store UNIX account information.
Services for UNIX 3.0	Microsoft provides this schema extension with the Services for UNIX 3.0 set of tools. It adds custom attributes to user and group objects, used to store UNIX account information.

It is possible to customize the schema setup to work with any schema configuration with Safeguard Authentication Services. No schema extensions are necessary with the new "schemaless" storage feature. When you configure Safeguard Authentication Services for the first time, Safeguard Authentication Services attempts to auto-detect the best schema configuration for your environment. The schema configuration is a global application setting that applies to all Safeguard Authentication Services management tools and UNIX agents. You can change the detected settings at any time using Control Center.

### Configuring a custom schema mapping

If you do not have a schema that supports UNIX data storage in Active Directory, you can configure Safeguard Authentication Services to use existing, unused attributes of users and groups to store UNIX information in Active Directory.

#### *To configure a custom schema mapping*

1. Open the Control Center and click **Preferences** then **Schema Attributes** on the left navigation pane.
2. Click the **UNIX Attributes** link in the upper right to display the Customize Schema Attributes dialog.
3. Type the LDAP display names of the attributes that you want to use for UNIX data. All attributes must be string-type attributes except **User ID Number**, **User Primary Group ID**, and **Group ID Number**, which may be integers. If an attribute does not exist or is of the wrong type, the border will turn red indicating that the LDAP attribute is invalid.

**NOTE:** When customizing the schema mapping, ensure that the attributes used for **User ID Number** and **Group ID Number** are indexed and replicated to the global

catalog.

For more information, see [Active Directory optimization](#) on page 44..

4. Click **OK** to validate and save the specified mappings in Active Directory.

## Active Directory optimization

Indexing certain attributes used by the Safeguard Authentication Services UNIX agent can have a dramatic effect on the performance and scalability of your UNIX and Active Directory integration project.

The Control Center, **Preferences** > **Schema Attributes** > **UNIX Attributes** panel displays a warning if the Active Directory configuration is not optimized according to best practices.

One Identity recommends that you index the following attributes in Active Directory:

- User UID Number
- User UNIX Name
- Group GID Number
- Group UNIX Name

**NOTE:** LDAP display names vary depending on your UNIX attribute mappings.

It is also a best practice to add all UNIX identity attributes to the global catalog. This reduces the number of Active Directory lookups that need to be performed by Safeguard Authentication Services UNIX agents.

Click the **Optimize Schema** link to run a script that updates these attributes as necessary. The **Optimize Schema** option is only available if you have not optimized the UNIX schema attributes defined for use in Active Directory.

This operation requires administrative rights in Active Directory. If you do not have the necessary rights to optimize your schema, it generates a schema optimization script. You can send the script to an Active Directory administrator who has rights to make the necessary changes.

All schema optimizations are reversible and no schema extensions are applied in the process.

## Use Safeguard Authentication Services PowerShell

Safeguard Authentication Services includes PowerShell modules that provide a "scriptable" interface to many Safeguard Authentication Services management tasks. You can access a customized PowerShell console from the Control Center **Tools** navigation link.

You can perform the following tasks using PowerShell cmdlets:

- UNIX-enable Active Directory users and groups.
- UNIX-disable Active Directory users and groups.
- Manage UNIX attributes on Active Directory users and groups.
- Search for and report on UNIX-enabled users and groups in Active Directory.
- Install product license files.
- Manage Safeguard Authentication Services global configuration settings.
- Find Group Policy objects with UNIX/macOS settings configured.

Using the Safeguard Authentication Services PowerShell modules, it is possible to script the import of UNIX account information into Active Directory.

## UNIX-enabling a user and user group (PowerShell Console)

The following procedure explains how to UNIX-enable a user and user group using the Safeguard Authentication Services PowerShell Console.

### To UNIX-enable a user and user group

1. From the Control Center, navigate to **Tools > Safeguard Authentication Services**.
2. Click **Safeguard Authentication Services PowerShell Console**.

**NOTE:** The first time you launch the PowerShell Console, it asks you if you want to run software from this untrusted publisher. Enter A at the PowerShell prompt to import the digital certificate to your system as a trusted entity. Once you have done this, you will never be asked this question again on this machine.

3. At the PowerShell prompt, enter the following:

```
Enable-QasUnixGroup UNIXusers | Set-QasUnixGroup -GidNumber 1234567
```

**NOTE:** You created the UNIXusers group in a previous exercise. See [Add an Active Directory group account](#).

UNIX attributes are generated automatically based on the Default UNIX Attributes settings that were configured earlier and look similar to the following:

```
ObjectClass           : group
DistinguishedName     : CN=UNIXusers,CN=Users,DC=example,DC=com
ObjectGuid            : 71aaa88-d164-43e4-a72a-459365e84a25
GroupName             : UNIXusers
UnixEnabled           : True
```

```
GidNumber           : 1234567
AdsPath             :
LDAP://windows.example.com/CN=UNIXusers,CN=Users,
DC=example,DC=com
CommonName          : UNIXusers
```

4. At the PowerShell prompt, to UNIX-enable an Active Directory user using the default UNIX attribute values, enter:

```
Enable-QasUnixUser ADuser | Set-QasUnixUser -PrimaryGidNumber 1234567
```

The UNIX properties of the user display:

```
ObjectClass         : user
DistinguishedName   : CN=ADuser,CN=Users,DC=example,DC=com
ObjectGuid          : 5f83687c-e29d-448f-9795-54d272cf9f25
UserName            : ADuser
UnixEnabled         : True
UidNumber           : 80791532
PrimaryGidNumber    : 1234567
Gecos               :
HomeDirectory       : /home/ADuser
LoginShell          : /bin/sh
AdsPath             : LDAP://windows.example.com/CN=ADuser,CN=Users,
DC=example,DC=com
CommonName          : ADuser
```

5. To disable the ADuser user for UNIX login, at the PowerShell prompt enter:

```
Disable-QasUnixUser ADuser
```

**NOTE:** To clear all UNIX attribute information, enter:

```
Clear-QasUnixUser ADuser
```

Now that you have UNIX-disabled the user, that user can no longer log in to systems running the Safeguard Authentication Services agent.

6. From the Control Center, under **Login to remote host**, enter:

- **Host name:** The UNIX host name.
- **User name:** The Active Directory user name, **ADuser**.

Click **Login** to log in to the UNIX host with your Active Directory user account.

A PuTTY window displays.

**NOTE:** PuTTY attempts to log in using Kerberos, but will fail over to password authentication if Kerberos is not enabled or properly configured for the remote SSH service.

7. Enter the password for the Active Directory user account.

You will receive a message that says `Access denied`.

## PowerShell cmdlets

Safeguard Authentication Services supports the flexible scripting capabilities of PowerShell to automate administrative, installation, and configuration tasks. A wide range of new PowerShell cmdlets are included in Safeguard Authentication Services.

**Table 17: PowerShell cmdlets**

cmdlet name	Description
Add-QasLicense	Installs an Safeguard Authentication Services license file in Active Directory. Licenses installed this way are downloaded by all UNIX clients.
Clear-QasUnixGroup	Clears the UNIX identity information from group object in Active Directory. The group is no longer UNIX-enabled and will be removed from the cache on the Safeguard Authentication Services UNIX clients.
Clear-QasUnixUser	Clears the UNIX identity information from a user object in Active Directory. The user is no longer UNIX-enabled will be removed from the cache on the Safeguard Authentication Services UNIX clients.
Disable-QasUnixGroup	UNIX-disables a group and will be removed from the cache on the Safeguard Authentication Services UNIX clients. Similar to Clear-QasUnixGroup except the UNIX group name is retained.
Disable-QasUnixUser	Removes an Active Directory user's ability to log in on UNIX hosts. (The user will still be cached on the Safeguard Authentication Services UNIX clients.)
Enable-QasUnixGroup	Enables an Active Directory group for UNIX by giving a UNIX GID number. The GID number is automatically generated.
Enable-QasUnixUser	Enables an Active Directory user for UNIX. The required account attributes UID number, primary GID number, GECOS, login shell, and home directory are generated automatically.
Get-QasConfiguration	Returns an object representing the Safeguard Authentication Services application configuration data stored in Active Directory.
Get-QasGpo	Returns a set of objects representing GPOs with UNIX

<b>cmdlet name</b>	<b>Description</b>
	and/or macOS settings configured. This cmdlet is in the <code>Quest.AuthenticationServices.GroupPolicy</code> module.
Get-QasLicense	Returns objects representing the Safeguard Authentication Services product licenses stored in Active Directory.
Get-QasOption	Returns a set of configurable global options stored in Active Directory that affect the behavior of Safeguard Authentication Services.
Get-QasSchema	Returns the currently configured schema definition from the Safeguard Authentication Services application configuration.
Get-QasSchemaDefinition	Returns a set of schema templates that are supported by the current Active Directory forest.
Get-QasUnixGroup	Returns an object that represents an Active Directory group as a UNIX group. The returned object can be piped into other cmdlets such as <code>Clear-QasUnixGroup</code> or <code>Enable-QasUnixGroup</code> .
Get-QasUnixUser	Returns an object that represents an Active Directory user as a UNIX user. The returned object can be piped into other cmdlets such as <code>Clear-QasUnixUser</code> or <code>Enable-QasUnixUser</code> .
Get-QasVersion	Returns the version of Safeguard Authentication Services currently installed on the local host.
Move-QasConfiguration	Moves the Safeguard Authentication Services application configuration information from one container to another in Active Directory.
New-QasAdConnection	Creates an object that represents a connection to Active Directory using specified credentials. You can pass a connection object to most Safeguard Authentication Services cmdlets to execute commands using different credentials.
New-QasArsConnection	Creates an object that represents a connection to an Active Roles Server using the specified credentials. You can pass a connection object to most Safeguard Authentication Services cmdlets to execute commands using different credentials.
New-QasConfiguration	Creates a default Safeguard Authentication Services application configuration in Active Directory and returns an object representing the newly created configuration.

<b>cmdlet name</b>	<b>Description</b>
Remove-QasConfiguration	Accepts a Safeguard Authentication Services application configuration object as input and removes it from Active Directory. This cmdlet produces no output.
Remove-QasLicense	Accepts an Safeguard Authentication Services product license object as input and removes the license from Active Directory. This cmdlet produces no output.
Set-QasOption	Accepts an Safeguard Authentication Services options set as input and saves it to Active Directory.
Set-QasSchema	Accepts an Safeguard Authentication Services schema template as input and saves it to Active Directory as the schema template that will be used by all Safeguard Authentication Services UNIX clients.
Set-QasUnixGroup	Accepts a UNIX group object as input and saves it to Active Directory. You can also set specific attributes using command line options.
Set-QasUnixUser	Accepts a UNIX user object as input and saves it to Active Directory. You can also set specific attributes using command line options.

Safeguard Authentication Services PowerShell cmdlets are contained in PowerShell modules named `Quest.AuthenticationServices` and `Quest.AuthenticationServices.GroupPolicy`. Use the `Import-Module` command to import the Safeguard Authentication Services commands into an existing PowerShell session.

## Change Auditor for Authentication Services

Change Auditor for Authentication Services allows you to track changes and send alerts on:

- Changes to Active Directory objects and attributes.
- Changes to UNIX and macOS settings in Group Policy Objects.
- Changes to product settings and configuration.

# Installing Change Auditor for Authentication Services

The following steps outline the basic procedure for installing Change Auditor for Authentication Services. For detailed steps on installing Change Auditor for Authentication Services, see the *Change Auditor Installation Guide*.

## To install Change Auditor for Authentication Services

1. Insert the Safeguard Authentication Services distribution media.  
The Autorun **Home** page displays.  
**NOTE:** If the Autorun **Home** page does not display, navigate to the root of the distribution media and double-click **autorun.exe**.
2. Click the **Setup** tab and select **Change Auditor for Authentication Services**.  
The **Change Auditor for Authentication Services for Active Directory** web page opens.
3. Click **Download** on the left navigation panel.
4. Follow the online instructions to gain access to the **Trial Download** page.
5. From the **Trial Download: Change Auditor for Active Directory** page, click the **Installation Guide** link.

## One Identity Defender

One Identity Defender, another One Identity product, provides strong authentication functionality that makes it possible for an Active Directory user to use a hardware or software token to authenticate to UNIX, Linux, or macOS platforms.

## Installing Defender

To use strong authentication, you must download and install Safeguard Authentication Services Defender. For detailed steps on installing Safeguard Authentication Services Defender, see the *Defender Installation Guide*.

**NOTE:** Defender installation requires a license file. A fully-functional 25-user license for it is included with Safeguard Authentication Services.

The following steps outline the basic procedure for installing Defender. See the

## **To install Defender**

1. Insert the Safeguard Authentication Services distribution media.

The Autorun **Home** page displays.

**NOTE:** If the Autorun **Home** page does not display, navigate to the root of the distribution media and double-click **autorun.exe**.

2. From the **Home** page, click the **Setup** tab.
3. From the **Setup** tab, click **One Identity Defender**.  
The **One Identity Defender** web page opens.
4. Click the **Download** on the left navigation panel.
5. Follow the online instructions to gain access to the **Trial Download** page.
6. From the **Trial Download: Defender** page, click the **Defender Documentation Archive** link.
7. Once you have installed One Identity Defender, see the *One Identity Defender Integration Guide* for detailed configuration instructions about integrating Safeguard Authentication Services Defender with Safeguard Authentication Services.

## Troubleshooting

To help you troubleshoot, One Identity recommends the following resolutions to some of the common problems you might encounter as you deploy and use Safeguard Authentication Services.

### Getting help from technical support

If you are unable to determine the solution to a problem, contact Technical Support for help. For more information, see [About us](#).

Before you contact Support, please collect the following information:

1. Take a system information snapshot. To do this, run the following command as root:

```
/opt/quest/libexec/vas/scripts/vas_snapshot.sh
```

This produces an output file in /tmp.

2. Make note of the UNIX attributes for the user that cannot log in (if applicable). To do this, capture the output from the following commands:

```
vastool -u host/ attrs <username>  
id <username>
```

| **NOTE:** Depending on your platform, you may need to run `id -a` instead of `id`.

3. Copy the text from any error messages that you see.
4. Save the results of running a "double su." To do this, log in as root and run `su <username>` note any error messages. Then run `su <username>` again and note any error messages.

Once you have collected the information listed above, contact Support at <https://support.oneidentity.com/authentication-services/>.

# Disaster recovery

Since Safeguard Authentication Services relies on Active Directory, follow Microsoft's best practices for keeping the database highly available. The administration tools are not critical to the operation of Safeguard Authentication Services and can quickly be reinstalled from scratch if needed.

## Long startup delays on Windows

You may experience long delays (over a minute) when starting the Safeguard Authentication Services Windows installer or certain Windows management tools such as Control Center. All Safeguard Authentication Services Windows binaries are Authenticode-signed so that you can be sure that the binaries are authentic and have not been tampered with.

This problem occurs when the .NET runtime attempts to verify the Authenticode signature by checking against certificate revocation lists (CRLs) at `cr1.microsoft.com`. If this site cannot be reached, the .NET framework check will time out (up to 60 seconds). This timeout occurs every time a signed assembly is loaded which can lead to very long load times. You can fix this problem by allowing access to `cr1.microsoft.com`.

If the computer is not connected to the internet, you can disable CRL checks for the entire system in Internet Explorer. Go to **Options**, select the **Advanced** tab, and under **Settings** clear the **Check for publisher's certification revocation** option.

It is also possible to specify a `generatePublisherEvidence` element in an `<app>.exe.config` that will disable CRL checks for the specific application that you are running. Keep in mind that if you are using Safeguard Authentication Services components in PowerShell or MMC, you will need to add this configuration for the `powershell.exe.config` and/or `mmc.exe.config`. Refer to [<generatePublisherEvidence> Element](#) for details.

## Pointer Record updates are rejected

If Pointer Record (PTR) updates are being rejected, it may be because the DHCP server is doing the update already. Refer to the documentation for the DHCP server used in your environment. The Microsoft DHCP server does updates on behalf of the host and this is controlled by the FQDN option. Refer to the Microsoft Active Directory DNS/DHCP documentation.

# Resolving DNS problems

It is imperative that DNS is correctly configured. Safeguard Authentication Services relies on DNS in order to locate domain controllers. Follow these steps to verify that domain controllers can be located using DNS:

1. Use `dig` to test whether your DNS configuration can locate a domain controller. Enter the following at the UNIX command prompt, replacing `<DNS Domain Name>` with your Active Directory DNS domain name:

```
dig -t any _ldap._tcp.dc._msdcs.<DNS Domain Name>
```

If DNS is configured correctly, you will see a list of domain controllers for your domain. If not, work with your DNS administrator to resolve the issue.

2. Use `dig` to test whether you can locate a domain controller in your site. Enter the following at the UNIX command prompt, replacing `<Site Name>` with the name of your Active Directory site and `<DNS Domain Name>` with your Active Directory DNS domain name.

```
dig -t _ldap._tcp.<Site Name>._sites.dc._msdcs.<DNS Domain Name>
```

If DNS is configured correctly, you will see a list of domain controllers for your site. If not, work with your DNS administrator to resolve the issue.

It is possible to work around DNS problems using the `vastool join` command to specify the domain controller host name on the command line. Safeguard Authentication Services can work without DNS configured as long as the forward lookup in the `/etc/hosts` file exists. The forward lookup resolves the domain controller host name to an IP address.

You can test this on Linux by firewalling DNS (port 53) with `iptables`. Make sure that you have an entry for your domain controller in `/etc/hosts`, then as root, enter the following commands replacing `<administrator>` with the name of an Active Directory administrator `<DNS Domain Name>` with your Active Directory DNS domain name and `<DC Host Name>` with the host name of your domain controller:

```
iptables -A INPUT -p udp --dport 53 -j DROP
iptables -A OUTPUT -p udp --dport 53 -j DROP
/opt/quest/bin/vastool -u <administrator> join <DNS Domain Name> <DC Host Name>
```

# Resolving preflight failures

If one of the `preflight` checks fail, `preflight` prints a suggested resolution. The following table provides additional problem resolution information. The checks are listed by the associated command-line flags.

**Table 18: Install checks**

Preflight option	Check	Resolution
--os-patch	Checks for supported operating system and correct operating system patches.	Install the Safeguard Authentication Services agent on a supported operating system that has the required operating system patches. Click <a href="https://www.oneidentity.com/products/one-identity-safeguard-authentication-services/">https://www.oneidentity.com/products/one-identity-safeguard-authentication-services/</a> to view a list of supported UNIX and Linux platforms that run Safeguard Authentication Services.
--disk-space	Checks for sufficient disk space to install Safeguard Authentication Services.	Free up more disk space. Safeguard Authentication Services requires disk space in /opt, /etc, and /var to install.

**Table 19: Join checks**

Preflight option	Check	Resolution
--tld	Checks that the DNS Top Level Domain (TLD) is not '.local'.	Ensure that mDNS is disabled in /etc/nsswitch.conf or use a domain other than .local.
--hostname	Checks that the hostname of the system is not 'localhost'.	One Identity recommends that you have a unique hostname to maintain uniqueness of computer names in Active Directory. Another option is to ignore this check and use -n computer_name when joining. For more information, see the <i>vastool man page</i> .
--name-service	Checks if the name service is configured to use DNS.	Ensure your host is configured to use DNS properly. Consult your platform documentation to determine the proper method to enable DNS for hostname resolution. For solutions, see <a href="#">Resolving DNS problems</a> on page 54.
--host-resolve	Ensures that the host can resolve names using DNS.	Check your /etc/resolv.conf file to ensure that name server entries are correct and reachable. Make sure that UDP port 53 (DNS) is open. This check attempts to resolve the domain name and can fail if your DNS configuration is invalid. This check expects to find properly formatted IPv4 addresses. Invalid or unreachable name server entries will cause delays even though the check will pass if at least one valid name server is found.

Preflight option	Check	Resolution
		If you notice delays when running this check, make sure that your name server configuration does not reference invalid name servers. For solutions, see <a href="#">Resolving DNS problems</a> on page 54.
--srv-records	Checks for a nameserver that has the appropriate DNS SRV records for Active Directory.	SRV records advertise various Active Directory services. Your configured name server must provide SRV records in order for Safeguard Authentication Services to take advantage of automatic detection and fail over. Ensure that UDP port 53 (DNS) is open.
--dc	Detects a writable domain controller with UDP port 389 open.	<p>If a domain controller is passed on the preflight command line, <code>preflight</code> checks that UDP port 389 is open and that the domain controller is writable. In this case, you may be able to specify a different domain controller.</p> <p>If you do not pass in the name of a domain controller, this check attempts to locate a writable domain controller using DNS SRV records. Ensure that your DNS SRV records are up to date in the configured DNS server. Safeguard Authentication Services can work with read-only domain controllers, but the computer object must have already been created with the proper settings in Active Directory.</p>
--site	Detects the Active Directory site, if available.	This check warns you if Safeguard Authentication Services was unable to locate an Active Directory site based on your computer's network address. A site configuration is not necessary, but Safeguard Authentication Services performs better if site information is configured in Active Directory. To resolve this problem, configure a site in Active Directory.
--kerberos-password	Checks if TCP port 464 is open for Kerberos <code>kpasswd</code> .	Ensure that TCP port 464 ( <code>kpasswd</code> ) is open. This port must be open to have Safeguard Authentication Services set the computer object's password.
--kerberos-traffic	Checks if UDP port 88 and TCP port 88 are open for	These ports are the main Kerberos communication channels; they must be open for Safeguard Authentication Services to authenticate to Active Directory. By default Safeguard Authentication

Preflight option	Check	Resolution
	Kerberos traffic.	Services uses TCP, but may be configured to prefer UDP.
--ldap	Checks if TCP port 389 is open for LDAP.	This port must be open for Safeguard Authentication Services to communicate with domain controllers using LDAP. This communication is GSS SASL encrypted and signed.
--global-catalog	Checks whether the Global Catalog is accessible on TCP port 3268.	Safeguard Authentication Services can function in a limited way without a global catalog server; however, Safeguard Authentication Services will be unable to resolve Active Directory users and groups from domains in the forest other than the one to which the host is joined. In addition, some searches may be slower. Make sure that TCP port 3268 (global catalog) is open and that you have configured at least one domain controller as a global catalog and that the global catalog server is up and reachable.
--timesync	Checks the machine's time is not skewed too far from Active Directory.	If the time difference between the UNIX host and the domain controller is too large, Kerberos traffic will not succeed. You can usually resolve this failure by running <code>vastool timesync</code> to synchronize time with the Active Directory domain. Port 123 UDP must be open in order to synchronize time with the domain controller. This check automatically synchronizes the time if you specify the <code>-S</code> option and run the application with root permissions.
--app-configuration	Checks for the Safeguard Authentication Services application configuration in Active Directory.	This check fails if you have not configured the Active Directory forest for Safeguard Authentication Services. Use Control Center (Windows) to create the necessary application configuration. This check can also fail due to an invalid username/password or if there is a time synchronization problem between the UNIX host and the domain controller.
--rodc	Checks against the given domain controller even if it is read-only, instead of selecting another domain controller.	The <code>--rodc</code> option runs preflight against the given domain controller instead of picking a writable DC. The <code>--rodc</code> check affects the <code>--kerberos-*</code> and <code>--ldap</code> checks. If the <code>--rodc</code> check fails, resolve preflight port check failures.

**NOTE:** If you get a message that says Unable to locate Safeguard Authentication Services Application Configuration, you can ignore that error and proceed with the Safeguard Authentication Services installation. The Safeguard Authentication Services Active Directory Configuration Wizard starts automatically to help you configure Active Directory for Safeguard Authentication Services the first time you start the Control Center.

**Table 20: Post-join checks**

Preflight option	Check	Resolution
--ms-cifs	Checks if TCP port 445 is open for Microsoft Directory Services CIFS traffic.	To use Group Policy on UNIX, this port must be open to allow Safeguard Authentication Services to use the CIFS protocol to download Group Policy objects from domain controllers.

## Time synchronization problems

Kerberos is a time-sensitive protocol. Your UNIX hosts must be synchronized within five minutes of your Active Directory domain controllers. Run the following command as root to have Safeguard Authentication Services synchronize the local time with Active Directory:

```
vastool timesync
```

## Unable to install or upgrade

The most common installation or upgrade failure is that the UNIX host cannot read the Safeguard Authentication Services application configuration in Active Directory. Ensure that you have followed the instructions in [Configure Active Directory](#) on page 8 and that the configuration has been created successfully.

During an upgrade, you may see an error that Safeguard Authentication Services cannot upgrade because the application configuration cannot be located. If you previously joined to a specific domain controller, Safeguard Authentication Services disabled DNS SRV record lookups. This means that Safeguard Authentication Services cannot resolve other domains in the forest and may be unable to locate the application configuration. In this case, you must ensure that the domain controller you specified is a global catalog. Otherwise, you must create the Safeguard Authentication Services application configuration in the domain that you join or you must properly configure DNS to return SRV records and join normally, rather than specifying a domain controller when you join.

For more information, see [About Active Directory configuration](#) on page 10.

## Unable to join the domain

If you are unable to join the domain, run the `preflight` utility to validate your environment. For more information, see [The pre-installation diagnostic tool](#) on page 15..

Then, verify the following:

- Check that the Active Directory account specified during join has rights to join the computer to the domain.
- Check that the UNIX host is able to properly resolve the domain name through DNS.

If you are joining to a specific domain controller you must ensure that Safeguard Authentication Services can locate and read the configuration information in Active Directory. To do so, perform one of the following steps::

- Make sure the domain controller you specify is a global catalog.
- Create the Safeguard Authentication Services application configuration in the domain to which you are joining.

For more information, see [About Active Directory configuration](#) on page 10..

- Properly configure DNS to return `srv`-records and avoid joining to a specific domain controller.

## Unable to log in

If you are unable to log in as an Active Directory user after installing, check the following:

1. Log in as root on the UNIX host.
2. Check the status of the Safeguard Authentication Services subsystems. To do this, run the following command:

```
vastool status
```

Correct any errors reported by the status command, then try logging in again.

3. Ensure the user exists locally and is allowed to log in. To check this, run the following command:

```
vastool user checklogin <username>
```

The output displays whether the user is a known Active Directory user. If not, you may need to map the user to an Active Directory account or UNIX-enable the Active Directory account. If the user is known, an access control rule may prevent them

from logging in. The output of the command displays which access control rules are in effect for the user.

You may need to restart window managers such as `gdm` in order for the window manager to reload NSS modules. Until the window manager reloads the NSS configuration, you will be unable to log in with an Active Directory user. Other services such as `cron` may also be affected by NSS changes. If you are unsure which services need to be reloaded, reboot the system.

**NOTE:**

If you are configuring on VMware ESX Server vSphere (ESX 4.0) the reason you can not log in may be related to access control issues. See *Configuring Access Control on ESX 4* in the *Safeguard Authentication Services Administration Guide*.

## vasypd has unsatisfied dependencies

If you receive the following error message while installing the Safeguard Authentication Services `vasypd` UNIX component, the `rpcbind` service may not be enabled.

```
svcadm: Instance "svc:/quest/vas/vasypd:default" has unsatisfied dependencies.  
Error 4 starting vasypd
```

### To enable the `rpcbind` service

1. Check the dependencies of `vasypd`:

```
# svcs -d quest/vas/vasypd  
STATE      STIME     FMRI  
disabled   Sep_14    svc:/network/rpc/bind:default  
online     Sep_14    svc:/milestone/single-user:default  
online     Sep_14    svc:/system/filesystem/local:default
```

2. If `rpcbind` is disabled, run this command to enable it:

```
# /usr/sbin/svcadm enable -s /network/rpc/bind
```

3. Run the following command to start `vasypd`:

```
# /etc/init.d/vasypd start
```

If `yp-tools` dependency is not available from rpm package manager, perform the following steps.

***yp-tools dependency is not available from rpm package manager***

1. Enable [Extra Packages for Enterprise Linux \(EPEL\)](#).
2. Install Development Tools on RHEL, CentOS, Fedora, Scientific or Red Hat Enterprise Linux.
3. Install ns1 library, ti-rpc and rpcbind `yum install libns12-devel libtirpc-devel rpcbind`.
4. Get the yp-tools source codes from [Github.com/thkukuk](https://github.com/thkukuk)  
<https://github.com/thkukuk>  
<https://www.thkukuk.de/nis/nis/>

The required repositories are:

- yp-tools
- ypbind-mt

The repositories contain an INSTALL helper guide.

5. Create a systemd service file for ybind-mt.

## Enterprise package deployment

This section details how to install, upgrade, and uninstall the Safeguard Authentication Services agent on supported platforms in an enterprise environment using platform package management tools.

### Installing the agent package

This section describes how to install the agent package.

#### *To install the Safeguard Authentication Services agent package*

1. Log in and open a root shell.
2. Mount the installation ISO and run the appropriate command.  
See [Additional configuration information](#) that follows the table.

**Table 21: Safeguard Authentication Services: Agent commands**

Platform	Command
Linux x86 - RPM	# rpm -Uhv /<mount>/client/linux-x86/vasclnt-<version>-<build>.i386.rpm
Linux x64 - RPM	# rpm -Uhv /<mount>/client/linux-x86_64/vasclnt-<version>-<build>.x86_64.rpm
Linux x86 - DEB	# dpkg -i /<mount>/client/linux-x86/vasclnt-<version>-<build>.i386.deb
Linux x64 - DEB	# dpkg -i /<mount>/client/linux-x86_64/vasclnt-<version>-<build>_amd64.deb
Linux s390	# rpm -Uhv /<mount>/client/linux-s390/vasclnt-<version>-<build>.s390.rpm
Linux s390x	# rpm -Uhv /<mount>/client/linux-s390x/vasclnt-<version>-

Platform	Command
	<build>.s390x.rpm
SLES 11, 12, and 15 PPC	# rpm -Uhv /<mount>/client/linux-glibc23-ppc64/vasclnt-glibc23-<version>-<build>.ppc64.rpm
Oracle Solaris 10 and 11 x64	# pkgadd -d /<mount>/client/solaris10-x64/vasclnt_SunOS_5.10_i386-<version>-<build>.pkg vasclnt
Oracle Solaris 10 and 11 SPARC	# pkgadd -d /<mount>/client/solaris10-sparc/vasclnt_SunOS_5.8_sparc-<version>-<build>.pkg vasclnt
HP-UX PA-RISC 11i v3 (B.11.31)	# swinstall -s /<mount>/client/hpux-pa-11v1/vasclnt_hpux-11.11-<version>-<build>.depot vasclnt
HP-UX IA64 11i v3 (B.11.31)	# swinstall -s /<mount>/client/hpux-ia64/vasclnt_ia64-<version>-<build>.depot vasclnt
AIX 7.1 and 7.2	# installp -acXd /<mount>/client/aix-71/vasclnt.AIX_5.3.<version>-<build>.bff all
Mac OS X	/usr/sbin/installer -pkg '/<mount>/VAS.mpkg/Contents/Packages/vasclnt.pkg' -target /
FreeBSD 10 and 11	pkg /<mount>/client/freebsd-x86_64/vasclnt-<build>.txz
Amazon Linux AMI	# rpm -Uhv /<mount>/client/linux-x86_64/vasclnt-<build>.x86_64.rpm

### Additional configuration information:

- To enable Safeguard Authentication Services authentication for all services, you must restart all services that require Safeguard Authentication Services authentication or restart the system.
- **Linux - RPM:** The x86\_64 Safeguard Authentication Services rpm contains 64-bit and 32-bit libraries, and has an RPM dependency on both the 32-bit libpam library and the 64-bit libpam library. If the 64-bit Oracle Solaris operating system on which you are installing Safeguard Authentication Services does not have any 32-bit supporting libraries installed, use the -- nodeps RPM flag to force the installation and avoid error messages about missing dependencies.
- **Oracle Solaris:** For information on Oracle Solaris 10 Zones support and installation, see [Oracle Solaris 10 zones/containers support](#) on page 67.

In certain situations, pkgadd requests additional information. Respond appropriately for your system configuration. Initialization scripts that are part of the vasclnt package run during installation to help configure the system.

To install the Safeguard Authentication Servicesvasypd UNIX component on Oracle Solaris 10, you must have the rpcbind service enabled on the host. For more information, see [vasypd has unsatisfied dependencies](#) on page 60.

- **HP-UX:** Safeguard Authentication Services requires that the Unixhost system clock be synchronized with the Active Directory server’s system clock. By default, HP-UX uses xntpd for time services. To properly synchronize the system clocks either configure xntpd to sync with a Domain Controller, or disable xntpd to allow Safeguard Authentication Services to synchronize the system time.Consult the xntpd documentation for information on disabling xntpd and configuring xntpd.

You must reboot the HP-UX machine to ensure that all of the new files are installed.HP-UX does not allow you to overwrite files that are in use—this is done as part of the boot sequence.

- **macOS:** To install from the command line, you must first mount the Safeguard Authentication Services DMG image file. On macOS enter:

```
hdiutil attach <media>/client/macos-106/VAS-<version>.dmg
```

## Agent upgrade commands

This section describes how to upgrade the agent package.

### *To upgrade the Safeguard Authentication Services agent package*

1. Log in and open a root shell.
2. Mount the installation ISO and run the appropriate command.  
See [Additional configuration information](#) that follows the table.

**Table 22: Safeguard Authentication Services: Agent commands**

Platform	Command
Linux x86 - RPM	# rpm -Uhv /<mount>/client/linux-x86/vasclnt-<version>-<build>.i386.rpm
Linux x64 - RPM	# rpm -Uhv /<mount>/client/linux-x86_64/vasclnt-<version>-<build>.x86_64.rpm
Linux x86 - DEB	# dpkg -i /<mount>/client/linux-x86/vasclnt-<version>-<build>.i386.deb
Linux x64 - DEB	# dpkg -i /<mount>/client/linux-x86_64/vasclnt-<version>-<build>_amd64.deb
Linux s390	# rpm -Uhv /<mount>/client/linux-s390/vasclnt-<version>-<build>.s390.rpm

Platform	Command
Linux s390x	# rpm -Uhv /<mount>/client/linux-s390x/vasclnt-<version>-<build>.s390x.rpm
SLES 11, 12, and 15 PPC	# rpm -Uhv /<mount>/client/linux-glibc23-ppc64/vasclnt-glibc23-<version>-<build>.ppc64.rpm
Oracle Solaris 10 and 11 x64	# pkgadd -d /<mount>/client/solaris10-x64/vasclnt_SunOS_5.10_i386-<version>-<build>.pkg vasclnt
Oracle Solaris 10 and 11 SPARC	# pkgadd -d /<mount>/client/solaris10-sparc/vasclnt_SunOS_5.8_sparc-<version>-<build>.pkg vasclnt
HP-UX PA-RISC 11i v3 (B.11.31)	# swinstall -s /<mount>/client/hpux-pa-11v1/vasclnt_hpux-11.11-<version>-<build>.depot vasclnt
HP-UX IA64 11i v3 (B.11.31)	# swinstall -s /<mount>/client/hpux-ia64/vasclnt_ia64-<version>-<build>.depot vasclnt
AIX 7.1 and 7.2	# installp -acXd /<mount>/client/aix-71/vasclnt.AIX_5.3.<version>-<build>.bff all
Mac OS X	/usr/sbin/installer -pkg '/<mount>/VAS.mpkg/Contents/Packages/vasclnt.pkg' -target /
FreeBSD 10 and 11	pkg /<mount>/client/freebsd-x86_64/vasclnt-<build>.txz
Amazon Linux AMI	# rpm -Uhv /<mount>/client/linux-x86_64/vasclnt-<build>.x86_64.rpm

## Additional configuration information

**NOTE:** During the upgrade, `vasd` reloads and updates its user and group cache. To restart the Safeguard Authentication Services caching service, see [Restarting services](#) on page 66.

**NOTE:** If you are using the licensed version of the Safeguard Authentication Services agent earlier than 3.0, see [Licensing Safeguard Authentication Services](#) on page 20 for licensing instructions.

**NOTE: Oracle Solaris:** The `-a vasclient-defaults` option specifies an alternative default file for `pkgadd` administrative options that allows `pkgadd` to overwrite an existing package with a new package.

`pkgadd` does not support the concept of upgrading a package, so this allows you to upgrade without having to rejoin your machine to the Active Directory domain, or uninstalling the old version first.

**NOTE: HP-UX:** Reboot the HP-UX machine to ensure that all of the new files are installed. HP-UX does not allow you to overwrite files that are in use—this is done as part of the boot sequence.

## Restarting services

To restart services, enter:

```
vastool daemon restart vasd
```

## Uninstalling the agent packages

This section describes how to uninstall the agent package.

### *To uninstall the Safeguard Authentication Services agent packages*

1. Log in and open a root shell.
2. Run the following commands to remove the packages.  
See [Additional configuration information](#) that follows the table.

**Table 23: Agent uninstall commands**

Package	Command
RPM	# rpm -e vasclnt
DEB	# dpkg -r vasclnt
Oracle Solaris	# pkgrm vasclnt
HP-UX	# swremove vasclnt
AIX	# installp -u vasclnt
macOS	/<<mount>/Uninstall.app/Contents/MacOS/Uninstall' --console --force vasclnt
FreeBDS	pkg delete <package name>

### Additional configuration information

- **Linux:** The `rpm -e vasclnt` and the `dpkg -r vasclnt` commands run scripts that halt the daemon, unconfigure Safeguard Authentication Services, flush, and delete the Safeguard Authentication Services cache before finally removing the files.
- **HP-UX:** The `swremove vasclnt` command does not clean up the empty directories that the `vasclnt` package used. In order to clean these up, manually remove the `/opt/quest` directory after you uninstall.

# Oracle Solaris 10 zones/containers support

Zones (or containers) were introduced in Oracle Solaris 10. Zones is a partitioning technology used to virtualize operating system services and provide an isolated and secure environment for running applications. There are two types of non-global zone root filesystem models:

- sparse root
- whole root

The sparse root zone model optimizes the sharing of objects while the whole root zone model provides the maximum configurability.

## Safeguard Authentication Services and Oracle Solaris 10 Zones installation guidelines

This section describes how to install Safeguard Authentication Services in a Oracle Solaris 10 Zones configuration.

### ***To install Safeguard Authentication Services in a Oracle Solaris 10 Zones configuration***

- In Oracle Solaris 10 Zones, only the global zone is permitted to do time synchronization. Therefore, if you want to run Safeguard Authentication Services in any Oracle Solaris Zone configuration, you must `timesync` the Global Zone with Active Directory. Time synchronization is a requirement of the Kerberos protocol and since Safeguard Authentication Services is built on Kerberos, Safeguard Authentication Services also has this requirement.
- The same version of Safeguard Authentication Services should be installed in any combination of global, whole root, and sparse root zone configurations.
- To disable time synchronization for Safeguard Authentication Services on the sparse zone, run the below command:

```
vastool configure vas vasd timesync-interval 0
```

- The following symlinks must exist in the global zone in order for the sparse zones to work correctly:

- `/usr/lib/security/pam_vas3.so > /opt/quest/usr/lib/security/pam_vas3.so`
- `/usr/lib/security/sparcv9/pam_vas3.so > /opt/quest/usr/lib/security/sparcv9/pam_vas3.so`

If `/usr` is shared, you need the following symlinks in the global zone pointing to counterpart files in `/opt/quest/lib`:

- `/usr/lib/nss_vas4.so.1 > /opt/quest/lib/nss/nss_vas4.so.1`
- `/usr/lib/security/pam_vas3.so > /opt/quest/usr/lib/security/pam_vas3.so`

In such a scenario, you do not need Safeguard Authentication Services joined to a domain in the global zone in order for sparse zones to work, but the symlinks must exist.

Each zone must have its own unique copy of `/etc` and `/var` because Safeguard Authentication Services stores zone-specific information in those locations. Sharing `/etc` and `/var` with the global zone is not a supported configuration.

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](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

## A

- Active Directory configuration
  - determines schema mappings 10
  - moving the configuration data 10
  - purpose defined 10
  - updating 10
  - validates license information 10
- Active Directory schema
  - how uses 43
- ActiveRoles Server option
  - not available if ActiveRoles Server agent is not installed 9
- agent packages
  - uninstalling 66
  - upgrading 64
- agent upgrade commands 64
- application configuration
  - creating from command line 22
  - overriding requirement 12
  - running Safeguard Authentication Services without 12
- application integration
  - installing Change Auditor 50
  - installing Defender 50

## B

- Best Practice:
  - add Unix identity attributes to global catalog 44
  - index attributes in Active Directory 44
  - install only one management console

- per environment 27
- license management 20
- use generated UIDs and GIDs 39
- use schema designed for storing Unix data in AD 42
- Version 3 Compatibility Mode 12

## C

- change Active Directory configuration settings 10
- Change Auditor integration
  - installing 50
- components
  - .msi files 6
  - installing windows components with msiexec.exe 6
- Control Center
  - adding license 31
  - described 27
  - must be logged in as domain user 27
- customize the schema mapping 43

## D

- debug logging
  - enabling 41
- Defender
  - installing 50
- Display specifiers
  - defined 32
- Dynamic DNS Update Tool 26

## E

- Edit GPO 29
- enable debug logging 41

## F

- Filter Options 28

## G

- Generating 29
- global settings modifications 27
- Global Unix Options
  - Unique IDs 39
  - Unix group defaults 39
  - Unix user defaults 39
  - where to set 39
- Group Policy
  - editing GPO 29
  - filtering list of GPOs 28
  - launching GPMC 30
  - showing templates for GPO 29

## I

- install.sh
  - about 17
  - interactive mode 26
- installation script
  - using 18
- Installation Script Options 18
- installing
  - Linux agent 62
  - MSI properties 6
  - Unix agent 14

## J

- join domain in Version 3 Compatibility Mode 12
- joining domain
  - determining if joined 23
- joining the AD domain 23-24

## L

- Launch GPMC 30
- LDAP attributes
  - mapped to Unix attributes 42
- license
  - adding using Control Center 31
  - Any VAS 3.x or higher license is valid for 4.x. 3
  - installing 3
  - installing from command line 21
  - managing licenses 20
  - updating in the console 3
- Linux agent
  - installing 62
- logging
  - enabling 41
  - enabling debug logging in Windows 41
  - setting options 41

## O

- Optimize Schema
  - requires AD administrator rights 44

## P

- performance and scalability 44

PosixAccount auxiliary class schema extension 43

PowerShell cmdlets 47

PowerShell modules 44

Preferences

configuring settings 30

Global Unix Options 39

Licensing 31

Logging Options 41

Schema Attributes 42

Unix Attributes 42

preflight Diagnostic Tool

About 15

preflight utility

running 17

PTR updates are rejected 53

## R

register display specifiers 32

reload configuration settings 66

required AD rights 27

required rights 10

restart services 66

## S

schema

configuration 42

extensions 42

LDAP attributes 42

templates 42

Unix attributes 42

schema configuration

defined 43

schema extension

PosixAccount auxiliary class 43

schema mappings

customizing

index and replicate GUI and UID attributes to global catalog 43

schemaless configuration 22

set global value 39

Show Files 29

standard Active Directory schema extensions 43

## T

troubleshooting 52

using logs 41

Troubleshooting:

changes made to NSS libraries 66

determine if joined to AD 23

Diagnostic Tool 15

Getting Help from Support 52

Long Startup Delays on Windows 53

PTR updates are rejected 26

rejected PTR updates 53

Resolving DNS Problems 54

Resolving Preflight Failures 54

Time Synchronization Problems 58

Unable to Install or Upgrade 58

Unable to Join the Domain 59

Unable to Log In 59

vasypd has unsatisfied dependencies 60

## U

uninstalling agent packages 66

- Unix agent
  - about installing 14
  - packages 62
- Unix Group ID (GID)
  - set global value 39
- Unix User ID (UID)
  - set global value 39
- unregister display specifiers 33
- upgrading VAS 3.5 to QAS 4.x 17

## V

- vasd
  - restart 66
- vasjoin Script
  - using 24
- vasjoin.sh
  - using 23
- vastool join
  - using 23
- Version 3 Compatibility Mode 12