Safeguard Authentication Services 5.0.5

Evaluation Guide

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 Evaluation Guide
Updated - 21 January 2022, 03:42
Version - 5.0.5

Contents

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/ 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/ 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.

See www.oneidentity.com/products/privilege-manager-for-unix/ for more information about replacing sudo.

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

Welcome to the *Safeguard Authentication Services Evaluation Guide*.

This is a self-directed, hands-on evaluation of Safeguard Authentication Services. The content includes a product overview, installation instructions, and a *Getting Started* section that will help you get acquainted with the Control Center, and how to use Safeguard Authentication Services to accomplish basic system administration tasks.

The guide is divided into three sections:

- Introducing One Identity Safeguard Authentication Services on page 7
- Installing and configuring Safeguard Authentication Services on page 19
- Getting started with Safeguard Authentication Services on page 25

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.
- In order to use Starling Two-Factor Authentication, you must have a valid license for Safeguard Authentication Services.

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 Adding licenses using the Control Center.

System requirements

Prior to installing Safeguard Authentication Services, ensure your system meets the minimum hardware and software requirements for your platform. Safeguard Authentication Services consists of Windows management tools and Unix client agent components.

Windows and cloud requirements

The following are the minimum requirements for using Safeguard Authentication Services in your environment.

Table 1: Authentication Services requirements

System requirements	
Supported Windows Platforms	Prerequisite Windows software If the following prerequisite is missing, the Safeguard Authentication Services installer suspends the installation process to allow you to download the required component. It then continues the install: • Microsoft .NET Framework 4.5 You can install Safeguard Authentication Services on 64-bit editions of the following configurations: • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 NOTE: Due to tightened security, when running Safeguard Authentication Services Control Center on Windows 2008 R2 (or later) operating system, functioning as a domain controller, the process must be elevated or you must add authenticated users to the Distributed COM Users group on the computer. As a best practice, One Identity does not recommend that you install or run the Safeguard Authentication Services Windows components on Active Directory domain controllers. The recommended configuration is to install the Safeguard Authentication Services Windows components on an administrative workstation.
Supported cloud	• AWS Directory Service for Microsoft Active Directory (also called AWS Managed Microsoft AD)

System requirements	
services	• Azure Active Directory Domain Services • Google Cloud Platform Managed Service for Microsoft Active Directory

Windows components

Safeguard Authentication Services includes the following Windows components.

Table 2: Windows components

Windows component	Description
Safeguard Authentication Services Control Center	A single console for access to all of the tools and configuration settings for Safeguard Authentication Services.
Active Directory Users and Computers MMC Snapin Extensions	Unix management extensions for Active Directory users and groups.
Group Policy Management Editor MMC Snapin Extensions	Group Policy extensions for management of Unix, Linux, and macOS.
RFC2307 NIS Map Editor MMC Snapin	Provides the ability to manage NIS data in Active Directory.
NIS Map Import Wizard	Imports NIS data into Active Directory.
Unix Account Import Wizard	Imports Unix identity data into Active Directory.
Safeguard Authentication Services PowerShell cmdlets	Provides the ability to script Unix management tasks.
Documentation	Full product documentation and online help.

Windows permissions

To install Safeguard Authentication Services on Windows, you must have:

- Local administrator rights
- Rights to create and delete all child objects in the container where you will install the configuration settings (first-time only)

Authenticated Users must have rights to read `cn`, `displayName`, `description`, and `whenCreated` attributes for container objects in the application configuration location. To change Active Directory configuration settings, Administrators must have rights to Create

Child Object (container) and Write Attribute for `cn`, `displayName`, `description`, and `showInAdvancedViewOnly` in the application configuration location.

Table 3: Required Windows permissions

Rights required	For user	Object class	Attributes
Create Child Object	Safeguard Authentication Services Administrators Only	Container	
Delete Child Object	Safeguard Authentication Services Administrators Only	Container	
Delete Child Object	Safeguard Authentication Services Administrators Only	Container	
Write Attribute	Safeguard Authentication Services Administrators Only	Container	`cn, displayName, description, showInAdvancedViewOnly`
Read Attribute	Authenticated Users	Container	`cn, displayName, description, whenCreated`

Unix agent requirements

NOTE: To install Safeguard Authentication Services on Unix, Linux, or macOS, you must have root access rights.

NOTE: With Safeguard Authentication Services 4.2 and later, Linux platforms require glibc 2.4 (or later).

The following table provides a list of supported Unix and Linux platforms for Safeguard Authentication Services.

Table 4: Unix agent: Supported platforms

Platform	Version	Architecture
Alma Linux	8	x86_64, AARCH64, PPC64le
Amazon Linux	AMI, 2	x86_64
Apple MacOS	10.14 or later	x86_64, ARM64
CentOS Linux	5, 6, 7, 8	Current Linux architectures: s390, s390x, PPC64, PPC64le, IA-64, x86, x86_64,

Platform	Version	Architecture
		AARCH64
CentOS Stream	8	x86_64,
Debian	Current supported releases	x86_64, x86, AARCH64
Fedora Linux	Current supported releases	x86_64, x86, AARCH64
FreeBSD	10.x, 11.x, 12.x	x32, x64
HP-UX	11.31	PA, IA-64
IBM AIX	6.1, 7.1, 7.2	Power 4+
OpenSuSE	Current supported releases	x86_64, x86, AARCH64
Oracle Enterprise Linux (OEL)	5, 6, 7, 8	Current Linux architectures: s390, s390x, PPC64, PPC64le, IA-64, x86, x86_64, AARCH64
Oracle Solaris	10 8/11 (Update 10), 11.x	SPARC, x64
Red Hat Enterprise Linux (RHEL)	5, 6, 7, 8	Current Linux architectures: s390, s390x, PPC64, PPC64le, IA-64, x86, x86_64, AARCH64
Rocky Linux	8	x86_64, AARCH64
SuSE Linux Enterprise Server (SLES)/Work-station	11, 12, 15	Current Linux architectures: s390, s390x, PPC64, PPC64le, IA-64, x86, x86_64, AARCH64
Ubuntu	Current supported releases	x86_64, x86, AARCH64

NOTE: For maximum security and performance, before you begin the installation, make sure that you have the latest patches for your operating system version. One Identity recommends that you run the Preflight utility to check for supported operating systems and correct operating system patches.

For more information, see *Running Preflight* in the *Safeguard Authentication Services Installation Guide*.

Unix components

Safeguard Authentication Services includes the following Unix components.

Table 5: Unix components

Unix component	Description
vasd	The Safeguard Authentication Services agent background process that manages the persistent cache of Active Directory information used by the other Safeguard Authentication Services components. `vasd` is installed as a system service. You can start and stop `vasd` using the standard service start/stop mechanism for your platform. `vasd` is installed by the **vasclnt** package.
vastool	The Safeguard Authentication Services command line administration utility that allows you to join a Unix host to an Active Directory Domain; access and modify information about users, groups, and computers in Active Directory; and configure the Safeguard Authentication Services components. `vastool` is installed at `/opt/quest/bin/vastool`. `vastool` is installed by the **vasclnt** package.
vgptool	A command line utility that allows you to manage the application of Group Policy settings to Safeguard Authentication Services clients. `vgptool` is installed at `/opt/quest/bin/vgptool`. `vgptool` is installed by the **vasgp** package.
oat (Ownership Alignment Tool)	A command line utility that allows you to modify file ownership on local Unix hosts to match user accounts in Active Directory. `oat` is installed at `/opt/quest/libexec/oat/oat`. `oat` is installed by the **vasclnt** package.
LDAP proxy	A background process that secures the authentication channel for applications using LDAP bind to authenticate users without introducing the overhead of configuring secure LDAP (LDAPS). The LDAP proxy is installed by the **vasproxy** package.
NIS proxy	A background process that acts as a NIS server which can provide backwards compatibility with existing NIS infrastructure. The NIS proxy is installed by the **vasyp** package.
SDK package	The **vasdev** package, the Safeguard Authentication Services programming API.

Permissions matrix

The following table details the permissions required for full Safeguard Authentication Services functionality.

Table 6: Required permissions

Function	Active Directory permissions	Local client permissions
Safeguard Authentication Services Application Configuration: creation	Location in Active Directory with Create Container Object rights	N/A
Safeguard Authentication Services Application Configuration: changes • Unix Global Settings • Licensing • Schema Attributes, including Unix Attributes	Update permission to the containers created above (no particular permissions if you are the one who created it)	N/A
Schema optimization	Schema Administrator rights	N/A
Display Specifier Registration	Enterprise Administrator rights	N/A
Editing Users	Administrator rights	N/A
Create any group policy objects	Group Policy Creator Owners rights	N/A
RFC 2307 NIS Import Map Wizard	Location in Active Directory with Create Container Object rights (you create containers for each NIS map)	N/A
Unix Account Import Wizard	Administrator rights (you are creating new accounts)	N/A
Logging Options	Write permissions to the file system folder where you want to create the logs	N/A
vasd daemon	The client computer object is expected to have read access to user and group attributes, which is the default. In order for Safeguard Authentication Services to	vasd must run as root

Function	Active Directory permissions	Local client permissions
	update the host object operating system attributes automatically, set the following rights for "SELF" on the client computer object: **Write Operating System**, **Write operatingSystemHotfix**, and **Write operatingSystemServicePack**.	
QAS/VAS PAM module	N/A (updated by means of `vasd`)	Any local user
QAS/VAS NSS module `vastool nss`	N/A (updated by means of `vasd`)	Any local user
`vastool` command-line tool	Depends on which `vastool` command is run	Any local user for most commands
`vastool join` `vastool unjoin`	Computer creation or deletion permissions in the desired container	root
`vastool configure` `vastool unconfigure`	N/A	root
`vastool search` `vastool attrs`	Read permission for the desired objects (regular Active Directory user)	Any local user
`vastool setattrs`	Write permissions for the desired object	Any local user
`vastool cache`	N/A	Run as root if you want all tables including authcache
`vastool create`	Permissions to create new users, groups, and computers as specified	Any local user; root needed to create a new local computer
`vastool delete`	Permissions to delete existing users, groups, or computers as specified; permissions to remove the keytab entry for the host object created (root or write permissions in the directory and the file)	Any local user
`vastool flush`	The client computer object is expected to have read access to user and group attributes, which should	root

Function	Active Directory permissions	Local client permissions
	be the default	
`vastool group add` `vastool group del`	Permission to modify group membership	Any local user
`vastool group hasmember`	Read permission for the desired objects (regular Active Directory user)	Any local user
`vastool info { site | domain | domain -n | forest-root | forest-root -dn | server | acl }`	N/A	Any local user
`vastool info { id | domains | domains -dn | adsecurity | toconf }`	Read permission for the desired objects (regular Active Directory user)	Any local user

`vastool isvas`
`vastool inspect`
`vastool license`
	N/A	Any local user

`vastool kinit`
`vastool klist`
`vastool kdestroy`
	Local client needs permissions to modify the keytab specified; default is the computer object, which is root.	Any local user

`vastool ktutil`	N/A	root if you are using the default `host.keytab` file
`vastool list` (with `-l` option)	Read permission for the desired objects (regular Active Directory user)	Any local user
`vastool load`	Permissions to create users and groups in the desired container	Any local user
`vastool merge` `vastool unmerge`	N/A	root

Function	Active Directory permissions	Local client permissions
`vastool passwd`	Regular Active Directory user	Any local user
`vastool passwd <AD user>`	Active Directory user with password reset permission	Any local user
`vastool schema list` `vastool schema detect`	Regular Active Directory user	Any local user
`vastool schema cache`	Regular Active Directory user	root (to modify the local cache file)
`vastool service list`	Regular Active Directory user	Any local user
`vastool service { create | delete }`	Active Directory user with permission to create/delete service principals in desired container	N/A
`vastool smartcard`	N/A	root
`vastool starling {list | detect [-d domain] | cache | check}`	Regular Active Directory user	Any local user (for list, detect, check) root (for cache)
`vastool status`	N/A	root
`vastool timesync`	N/A	root, if you only query the time from AD, you can run as any local user
`vastool user { enable | disable }`	Modify permissions on the AD Object	Any local user
`vastool user { checkaccess | checkconflict }`	N/A	Any local user
`vastool user checklogin`	Access to Active Directory users password	Any local user

Encryption types

The following table details the encryption types used in Safeguard Authentication Services.

Table 7: Encryption types

Encryption types	Specification	Active Directory version	Safeguard Authentication Services version
KERB_ENCTYPE_DES_CBC_CRC			
CRC32	RFC 3961	All	All
KERB_ENCTYPE_DES_CBC_MD5			
RSA-MD5	RFC 3961	All	All
KERB_ENCTYPE_RC4_HMAC_MD5			
RC4-HMAC-MD5	RFC 4757	All	All
KERB_ENCTYPE_AES128_CTS_HMAC_SHA1_96			
HMAC-SHA1-96-AES128	RFC 3961	Windows Server 2008 +	3.3.2+
KERB_ENCTYPE_AES256_CTS_HMAC_SHA1_96			
HMAC-SHA1-96-AES256	RFC 3961	Windows Server 2008 +	3.3.2+

Network requirements

Safeguard Authentication Services must be able to communicate with Active Directory, including domain controllers, global catalogs, and DNS servers using Kerberos, LDAP, and DNS protocols. The following table summarizes the network ports that must be open and their function.

Table 8: Network ports

Port	Function
389	Used for LDAP searches against Active Directory Domain Controllers. TCP is normally used, but UDP is used when detecting Active Directory site membership.
3268	Used for LDAP searches against Active Directory Global Catalogs. TCP is always used when searching against the Global Catalog.
88	Used for Kerberos authentication and Kerberos service ticket requests against

Port	Function
	Active Directory Domain Controllers. TCP is used by default.
464	Used for changing and setting passwords against Active Directory using the Kerberos change password protocol. Safeguard Authentication Services always uses TCP for password operations.
53	Used for DNS. Since Safeguard Authentication Services uses DNS to locate domain controllers, DNS servers used by the Unix hosts must serve Active Directory DNS SRV records. Both UDP and TCP are used.
123	UDP only. Used for time-synchronization with Active Directory.
445	CIFS port used to enable the client to retrieve configured group policy.

NOTE: Safeguard Authentication Services, by default, operates as a client, initiating connections. It does not require any firewall exceptions for incoming traffic.

3

Installing and configuring Safeguard Authentication Services

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, you must install and configure Safeguard Authentication Services:

1. Install Safeguard Authentication Services Windows components.
2. Configure Active Directory for Safeguard Authentication Services (one time only).
3. Configure Unix Agent Components
    a. 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 *Customize Installation Options* in the *Safeguard Authentication Services Installation Guide*.
3. Once the installation completes successfully, click **Finish** or **Launch Control Center**.

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 *Version 3 Compatibility Mode* in the *Safeguard Authentication Services Installation Guide*.

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* in the *Safeguard Authentication Services Installation Guide*.

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 *Version 3 Compatibility Mode* in the *Safeguard Authentication Services Installation Guide*.

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 MMC 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**.

    Refer to About licenses on page 7 for more information about licensing requirements.

    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 on page 9.

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.

   Refer to *Configure Unix Agent Components* in the *Safeguard Authentication Services Installation Guide* for more information.

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.

See *Version 3 Compatibility Mode* in the *Safeguard Authentication Services Installation Guide* for details.

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 *Creating the Application Configuration from the Unix Command Line* in the *Safeguard Authentication Services Installation Guide*.

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 9: Safeguard Authentication Services Required rights

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

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.

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 10: Control Center: Navigation links

Control Center pane	Description
Home	The **Welcome** 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

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

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, refer to 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

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

NOTE: Microsoft does not support Group Policy Management Console (GPMC) on 64-bit platforms of Windows; thus, 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 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
- 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.

Refer to About licenses on page 7 for more information about licensing requirements.

Adding licenses using the Control Center

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 vlaid 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 only displays 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 | Authentication Services | Control Center**.
2. Click **Preferences** on the left navigation panel.
3. Expand the **Display Specifiers** section.

   NOTE: The **Register Display Specifiers** link only displays 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 Roles Server display specifiers with One Identity Active Roles Server, 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 Roles Server 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

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 Role, 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=DisplaySpecifers,cn=Configuration,dc=domain`. The following modifications are made for each locale by the display specifier registration script, `DsReg.vbs`.

Table 11: 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 12: 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 13: Object: vintela-UnixUserPersonality-Display

Attribute	Change type	Value	Description
cn	create object	vintela-UnixUser-Personality- 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 ARS. To create personality objects in ARS, use the Advanced

Attribute	Change type	Value	Description
			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.
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. Allows this attribute to display in the Unix Object find dialog results.

Table 14: 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" 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

Attribute	Change type	Value	Description
			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.
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

Attribute	Change type	Value	Description
			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 15: 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.
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.

Option	Description
	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 16: 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 17: 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 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).

BEST PRACTICE: 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. Because logging causes components to run slower and use more disk space, you should set the **Log Level** to **Disabled** when you are finished troubleshooting.

Enabling 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.

Starling Two-Factor Authentication

From the Control Center, select **Preferences** then **Starling Two-Factor Authentication** to view and update configurations.

The following sections provide a comprehensive look at Starling Two-Factor Authentication.

From **Preferences | Starling Two-Factor Authentication**you can perform these actions.

- Configuring Starling to use a proxy server
- Starling Attributes: Configure LDAP attributes for use with push notifications
- Unjoining from Starling

For more details on Starling Two-Factor Authentication, see the *Safeguard Authentication Services Administration Guide*, One Identity Starling Integration.

One Identity Starling integration

One Identity Starling Two-Factor Authentication is a SaaS solution that provides two-factor authentication on a product enabling organizations to quickly and easily verify a user's identity. This service is provided as part of the One Identity Starling cloud platform. Joining Safeguard Authentication Services to One Identity Starling allows you to take advantage of these companion features from Starling services. For more information on Starling, see the One Identity Starling *User Guide*.

In order to use Starling 2FA with Safeguard Authentication Services, you must join Safeguard Authentication Services to Starling. This is done from the **Preferences | Starling Two-Factor Authentication** pane in the Control Center. From this pane, you can also configure Starling to use a proxy server and customize the attributes to be used in push notifications.

Help links that provide assistance with Starling are available on the dialogs displayed when setting up the **Starling Join Settings** or **Starling Proxy Settings**:

- **Visit us Online** displays the Starling login page where you can create a new Starling account. This help link is available on both dialogs.
- **Trouble Joining** displays the Starling support page with information on the requirements and process for joining with Starling. This help link is available on the **Starling Two-Factor Authentication** dialog.
- **Trouble With Proxy** displays the Starling support page with additional information on troubleshooting the proxy configuration. This help link is available on the **Starling Proxy Configuration** dialog.

Starling Two-Factor Authentication requirements

In order to use Starling Two-Factor Authentication with Safeguard Authentication Services, you will need the following:

- A valid license for Safeguard Authentication Services.
- A Starling Organization Admin account or a Collaborator account. For more information on Starling, see the One Identity Starling Hosted User Guide.
- An Active Directory group for Starling users.

  NOTE: All Starling users must have the following defined in order to work with Starling 2FA:

  - Valid email address
  - Valid mobile phone number in E.164 format. (that is, +<country code><area code><phone number>)
  - Be a member of this Starling group dictated by GPO.

  For more information, see Setting up Starling users on page 41..
- Safeguard Authentication Services 4.2 (or later)

The following table provides a list of supported platforms for integrating Safeguard Authentication Services with Starling Two-Factor Authentication.

NOTE: PPC64 and PPC64LE architectures require a kernel greater than 2.6.37.

Table 18: Starling 2FA: Supported platforms

Platform	Version	Architecture
CentOS Linux	5, 6, 7, 8	Current Linux architectures: s390, s390x, PPC64, PPC64le, IA-64, x86, x86_64, AARCH64
Debian	Current supported releases	x86_64, x86, AARCH64
Fedora Linux	Current supported releases	x86_64, x86, AARCH64
FreeBSD	10.x, 11.x	x32, x64
IBM AIX	7.1, 7.2	Power 4+
OpenSuSE	Current supported releases	x86_64, x86, AARCH64
Oracle Enterprise Linux (OEL)	5, 6, 7, 8	Current Linux architectures: s390, s390x, PPC64, PPC64le, IA-64, x86, x86_64, AARCH64
Oracle Solaris	10 8/11, 11.x	SPARC, x64
Red Hat Enterprise Linux (RHEL)	5, 6, 7, 8	Current Linux architectures: s390, s390x, PPC64, PPC64le, IA-64, x86, x86_64, AARCH64
SuSE Linux Enterprise Server (SLES)/Work-station	11, 12, 15	Current Linux architectures: s390, s390x, PPC64, PPC64le, IA-64, x86, x86_64, AARCH64
Ubuntu	Current supported releases	x86_64, x86, AARCH64

Setting up Starling users

A new Group Policy Object has been added to Safeguard Authentication Services to manage the group file for Starling, which is located in `/etc/opt/quest/vas/users.starling`.

Sample users.starling file

```
# This assumes that the host has been joined to the example.com domain.
# To validate the users.starling file, run:
# vastool info acl
#
# This file controls which user's have Starling appled to them during login based
# on group membership.
# For entries:
# If DOMAIN is omitted ( simple name given )it is assumed to be the joined domain.
# Entries are case insensitive.
# DOMAIN can be either long(fqdn) or short(netbios).
# Apply Starling to members of the sales and engineering groups.
# The entry DOMAIN\SamAccountName format is preferred.
EXAMPLE\sales
engineering
```

This file can be manually created or set using the GPO.

To enable Starling for users using the GPO

1. Open your Group Policy management system.
2. Select the applicable group policy.
3. Navigate to **Computer configuration | Unix Settings | Starling**.
4. Double-click **users.starling**.
5. Add the groups that contain the users to be enabled to use Starling 2FA.

It may take up to 90 minutes to apply this configuration change. Use `vgptool apply` to apply the changes quicker.

Joining Safeguard Authentication Services with Starling

Joining Safeguard Authentication Services to Starling allows you to use features from Starling Two-Factor Authentication.

To join Safeguard Authentication Services with Starling

1. From the Control Center, navigate to **Preferences | Starling Two-Factor Authentication**.
2. In the **Join to Starling and enable Two-Factor Authentication** pane, click **Starling Join Settings**.

3. On the **Starling Two-Factor Authentication** dialog, use the **Product TIMs** drop-down to select a valid Safeguard Authentication Services license.

   NOTE: The other fields on this dialog are read-only and contain the following information after you successfully join to Starling:

   - **Product Name**: Displays Safeguard Authentication Services.
   - **Product Instance**: Displays the unique identifier for Starling.

4. Click **Join to Starling**.

   NOTE: The following additional information may be required:

   - If you do not have an existing session with Starling, you will be prompted to authenticate.
   - If your Starling account belongs to multiple organizations, you will be prompted to select which organization Safeguard Authentication Services will be joined with.

   After the join has successfully completed, you will be returned to the Safeguard Authentication Services Control Center and the **Join to Starling and enable Two-Factor Authentication** pane will display the following:

   - **Product Instance**: Displays the unique identifier for Starling. You can click the **Copy** button to the right of this field to copy the product instance identifier to your desktop.
   - **Starling Join State**: Displays either **Joined** or **Unjoined**.

Configuring Starling to use a proxy server

The **Starling Proxy Settings** must be configured if your company policies do not allow devices to connect directly to the web. Once configured, Safeguard Authentication Services uses the configured proxy server for outbound web requests to Starling.

NOTE: One Identity recommends you use an automatic configuration script (proxy PAC file). To specify a previously configured PAC file, select the **Use automatic configuration script** check box and enter the address of the proxy.pac file.

To configure Starling to use a proxy server

1. From the Control Center, navigate to **Preferences | Starling Two-Factor Authentication**.
2. In the **Starling Proxy Configuration** pane, click **Starling Proxy Settings**.
3. On the **Starling Proxy Configuration** dialog, enter the following information about the proxy server to be used:

   To specify a previously configured PAC file (recommended):

   - **Use automatic configuration script**: Select this check box.
   - **Address**: Enter the address of the proxy.pac file.

   To use username/password to specify the proxy server:

- **Address**: Enter the URL for the proxy server.
- **Port**: Enter the port number to be used.
- **Username**: Enter the user name of a service account that is to be used to access the proxy server.
- **Password**: Enter the password associated with the user name specified. The password will be displayed in clear text.

4. Click **OK** to save your selections.

Starling Attributes: Configure LDAP attributes for use with push notifications

You can specify the user mobile number and user email address attributes to be used by the Starling push notifications.

Modifications to the Starling schema attributes configuration are global and apply to all Safeguard Authentication Services clients in the forest. For users configured to use Starling, this could cause user logins to fail.

To configure custom LDAP attributes for use with Starling push notifications

1. From the Control Center, navigate to the Starling Attributes in one of the following two ways:
   - **Preferences | Starling Two-Factor Authentication** and click the **Starling Attributes** link.
   - **Preferences | Schema Attributes**
2. Click the **Unix Attributes** link in the upper right to display the Customize Schema Attributes dialog.
3. Enter the LDAP display name for one or both of the Starling attributes used by the Starling push notifications:
   - **User Mobile Number**
   - **User Email Address**
4. Click **OK**.
5. Click **Yes** to confirm that you want to modify the Starling schema attributes configuration.
6. Back on the **Starling Two-Factor Authentication** preference pane, the Starling attributes to be used are displayed.

Logging in with Starling Two-Factor Authentication

Once Starling Two-Factor Authentication is enabled (that is, Safeguard Authentication Services is joined to Starling and users are authorized to use Starling Two-Factor Authentication), anytime an authorized user attempts to log in to an integrated Unix-based host, they will see an additional login screen informing them that an additional authentication step is required.

The default prompt contains the following:

Enter a token or select one of the following options:

1. Starling Push
2. Phone call
3. Send an SMS

Token or option (1-3) [1]: <Token or option number>

This default prompt can be modified in `vas.conf`.

vas.conf example:

[STARLING] OPTIONS

The behavior of QAS Starling can be modified by using the following options in the [starling] section.

[starling]

prompt = <boolean>

prompt = <message-text>

Default value: "Enter a token or select one of the following options:\n\n 1. Starling Push\n 2. Phone

call\n 3. Send an SMS\n \nToken or option (1-3)[1]: "

This is the message that is initially displayed during a Starling authentication.

This prompt can span multiple lines, line separation is specified by adding \n to the prompt string.

NOTE: Changing the prompt will not change what is accepted as input.

[starling]

prompt = "Enter 1 for a push request, 2 for a phone call, 3 for a txt, or enter a token.\n "

NOTE: In order to display the prompts, the application must be able to handle pam conversations, such as sshd(keyboard-interactive). If the application can not handle pam conversations, such as sshd(password), a push authentication is sent instead of a prompt.

Unjoining from Starling

Unjoining Safeguard Authentication Services from Starling disables Starling Two-Factor Authentication in Safeguard Authentication Services.

To unjoin Safeguard Authentication Services from Starling

1. From the Control Center, navigate to **Preferences | Starling Two-Factor Authentication**.

2. In the **Join to Starling and enable Two-Factor Authentication** pane, click **Starling Join Settings**.
3. On the **Starling Two-Factor Authentication** dialog, click **Unjoin Starling**.

A Starling Organization Admin account or Collaborator account can rejoin Safeguard Authentication Services at any time.

Disabling Starling 2FA for a specific PAM service

To disable Starling 2FA for a specific PAM service, edit the PAM configuration file (`/etc/pam.conf` or `/etc/pam.d/<service>`). Modify the `auth pam_vas` line for the desired service.

To disable Starling 2FA for a specific PAM service

1. As root, add the following line to the PAM configuration file, on the first `auth pam_vas` line for the service:

   ```
   disable_starling
   ```

Schema Attributes

From the Control Center, select **Preferences** then **Schema Attributes** to view and update schema configurations. These attribute mappings can be customized:

- Unix Attributes
- Starling Attributes: Configure LDAP attributes for use with push notifications

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 19: 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.

BEST PRACTICE: 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 20: 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 48. .
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.

Starling Attributes: Configure LDAP attributes for use with push notifications

You can specify the user mobile number and user email address attributes to be used by the Starling push notifications.

Modifications to the Starling schema attributes configuration are global and apply to all Safeguard Authentication Services clients in the forest. For users configured to use Starling, this could cause user logins to fail.

To configure custom LDAP attributes for use with Starling push notifications

1. From the Control Center, navigate to the Starling Attributes in one of the following two ways:
    - **Preferences | Starling Two-Factor Authentication** and click the **Starling Attributes** link.
    - **Preferences | Schema Attributes**
2. Click the **Unix Attributes** link in the upper right to display the Customize Schema Attributes dialog.
3. Enter the LDAP display name for one or both of the Starling attributes used by the Starling push notifications:
    - **User Mobile Number**
    - **User Email Address**
4. Click **OK**.
5. Click **Yes** to confirm that you want to modify the Starling schema attributes configuration.
6. Back on the **Starling Two-Factor Authentication** preference pane, the Starling attributes to be used are displayed.

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 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 | Seet-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 21: 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

cmdlet name	Description
	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 and/or macOS settings configured. This cmdlet is in the `Quest.AuthenticationServices.GroupPolicy` 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 Clear-QasUnixGroup or Enable-QasUnixGroup.
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 Clear-QasUnixUser or Enable-QasUnixUser.
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.

cmdlet name	Description
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.
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. See the *Change Auditor Installation Guide* to obtain detailed steps for installing Change Auditor for Authentication Services.

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

In order to use strong authentication, you must download and install Safeguard Authentication Services Defender. See the *Defender Installation Guide* to obtain detailed steps for installing Safeguard Authentication Services Defender.

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 IdentityDefender** 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.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

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

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Index

S

T

U