Safeguard Authentication Services 5.0.3

Release Notes

03 September 2021, 11:50

These release notes provide information about the Safeguard Authentication Services 5.0.3 release. For the most recent documents and product information, see Safeguard Authentication Services - Technical Documentation.

About this release

Safeguard Authentication Services extends the capabilities of UNIX, Linux, and Mac systems to seamlessly and transparently join Active Directory and integrate Unix identities with Active Directory Windows accounts.

Safeguard Authentication Services 5.0.3 is a minor release that includes various bug and stability fixes. See Resolved issues for a list of fixes included in this release.

End of support notice

After careful consideration, One Identity has decided to cease the development of the Management Console for Unix (MCU). Therefore, the MCU will enter limited support for all versions on April 1, 2021. Support for all versions will reach end of life on Nov 1, 2021. For definitions of support, see the Software Product Support Lifecycle Policy.

As One Identity retires the MCU, we are building its feature set into modern platforms starting with Software Distribution and Profiling. Customers that use the MCU to deploy Authentication Services and Safeguard for Sudo can now use our Ansible collections for those products, which can be found at Ansible Galaxy.

Supported platforms

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

CAUTION: In Safeguard Authentication Services version 5.1, support for the following Linux platforms and architectures will be deprecated:

- **Linux platforms**
  - **CentOS Linux 5**
  - **Oracle Enterprise (OEL) Linux 5**
  - **Red Hat Enterprise Linux (RHEL) 5**
- **Linux architectures**
  - **IA-64**
  - **s390**

Make sure that you prepare your system for an upgrade to a supported Linux platform and architecture, so that you can upgrade to Safeguard Authentication Services version 5.1 when it is released.

Table 1: Unix agent: Supported platforms

Platform	Version	Architecture
Amazon Linux AMI		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, AARCH64
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

Platform	Version	Architecture
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
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

New features

New features in version 5.0

The new feature in Safeguard Authentication Services5.0 follow.

Ansible support (224151)

Infrastructure Administrators can use Ansible 2.9 or later for the following functions, including generating reports.

- Install, upgrade, and uninstall Safeguard Authentication Services (SAS) software packages and create reports to summarize software deploy status
- Configure and join Safeguard Authentication Services to my AD domain including:
  - Perform preflight checks
  - Modify `vas.conf`
  - Modify `users/groups.allow` and `users/groups.deny`
  - Modify user/group overrides
  - Join/unjoin SAS from domain
  - Create reports to summarize configure/join status

Authentication Services Ansible Collection

The One Identity Authentication Services Ansible Collection, referred to as `ansible-authentication-services`, consists of roles, modules, plugins, report templates, and

sample playbooks to automate software deployment, configuration, Active Directory joining, profiling, and report generation for Safeguard Authentication Services. Go to: https://github.com/OneIdentity/ansible-authentication-services.

Ansible details

For Ansible information consult:

- GitHub ansible/ansible
- Ansible Documentation (includes Tower)

NOTE: One Identity open source projects are supported through One Identity GitHub issues and the One Identity Community. This includes all scripts, plugins, SDKs, modules, code snippets or other solutions. For assistance with any One Identity GitHub project, please raise a new Issue on the One Identity GitHub project page. You may also visit the One Identity Community to ask questions. Requests for assistance made through official One Identity Support will be referred back to GitHub and the One Identity Community forums where those requests can benefit all users.

Explicit mapping of users to valid certificates (smart card) (198067)

Mapping certificates to users can be done implicitly or explicitly. Authentication Services supports mapping one cert to one user or mapping multiple certs to one user. Mapping one cert to multiple users is not supported. For details, see the *Smart Cards Administration Guide*, Map certificate to user (implicit and explicit).

Group policy updates (198055)

Safeguard Authentication Services can apply additional policies to Unix systems:

- mac OS X policies are updated
- Privileged Manager Policies are updated

License validator (198066)

New licenses have to be added prior to upgrading to version 5.0. If you have a mixed environment with some clients running on 5.0 and some running on an older version, you will need to have both licenses available.

CAUTION: If you upgrade Safeguard for Authentication Services before adding the license, the caches will empty and SAS will be unusable. You can add the license then either rejoin or restart vasd and run vastool flush. You can update the Control Center any time without issue.

Windows Administrators can load the Safeguard Authentication Services license into Active Directory.

Unix Administrators must have a current license.

macOS: Added functionality (198050)

The following functionality was added for macOS platforms. For additional information, see KB 322901.

- Installation is from the One Identity Support page.
- In Application Properties, an Options tab has been added to control App Store and Game Center settings. For example, you can choose to allow software update notifications.
- In Media Access Properties, there are two new settings:
  - Allow AirDrop
  - Allow transfers with Finder or iTunes
- Software Update Properties have been added related to purchasing or installing apps.
- System Preference Properties selection was enhanced.
- Wireless Profile Properties now include the ability to use hidden networks, auto join networks, proxies, protocol configurations, and authentication. This policy also works with `vascert` to provide a certificate that can be used to join a network.

Support for unattended join using Windows Offline Domain Join (ODJ) credentials (198057)

An Administrator can use a Windows Offline Domain Join (ODJ) credential instead of a keytab for scripting an unattended installation of Safeguard Authentication Services to enhance security.

There must be connectivity from the Unix machine to domain controllers. When using this method of joining AD, the `[domain]` is not needed on the `vastool join` command, nor credentials. That information will come from the file. More information is in the `vastool` man page.

The join can work in the following ways:

- `vastool join [some flag] <path to the offline join file>`
- `vastool join` to use a newly defined environment variable that points to the location of the offline join file
- `vastool join` to use if the flag wasn't passed and the environment variable is not set, a predefined location is checked for the offline join file

Resolved issues

The following is a list of issues addressed in this release.

Table 2: General resolved issues in version 5.0.3

Resolved Issue	Issue ID
The network interface used by the ipmond tool cannot be configured from the dnsupdate.conf configuration file and cannot be autodetected. The network interface used by the ipmond tool now can be specified in the	199551

Resolved Issue	Issue ID
dnsupdate.conf configuration file using the "NetworkInterface" option. If the "NetworkInterface" option is not specified or if the "NetworkInterface" option is set to "auto", the ipmond tool attempts to detect the interface that belongs to the default network route ("0.0.0.0"). This detection can work through the "/proc/net/route" (on Linux systems), or using the "netstat" command (if the "netstat" is available on the system). To restore the previous behavior (that is, listening on all interfaces) set the "NetworkInterface" option to "all".	
On systems with the "authselect" tool and "nscd" daemon, users could not log in right after joining the Active Directory. Users can now log in right after joining the Active Directory.	267078
The "vastool status" command has a test that was supposed to detect and report timesync errors but it did not detect and report them. The "vastool status" command now detects and reports timesync errors.	273371
The "vastool create <user>" command replaced space and dot characters with an underscore. The "vastool create <user>" command now does not replace space and dot characters.	273374
When logging in as a local user using password-less authentication, the PAM module was triggering a lot of unnecessary "vasd" calls. These calls caused potential performance issues by slowing down the system. The login process for a local user using password-less authentication could take too long. The number of calls from the PAM module to the "vasd" daemon is significantly reduced in password-less authentication. The login process for a local user using password-less authentication is faster now.	274626
The default value of the "kdc_timeout" parameter was documented as 3 seconds in the man page of the "vas.conf" configuration file, but the actual default value was 30 seconds. The default value of the "kdc_timeout" parameter is fixed to 3 seconds. The documented default value and the actual default value of the "kdc_timeout" parameter are now identical.	276218
The "vasd" daemon crashes when the number of open file descriptors exceeds 1024 with the following message: AuthChild::HandleGetNextMessageFailure Error processing message. rc=71 ("Protocol error"). The "vasd" daemon can now handle more than 1024 open file descriptors.	276395
Invalid license file is reported on an ERROR logging level even though it should be reported on a DEBUG logging level. The "vgptool" tool verifies the license file. The invalid license file is now reported on a DEBUG logging level. This is now an expected behavior in	277273

Resolved Issue	Issue ID
systems with version 4 and 5 SAS product models.	
The "${HOME}/.vas_logon_server" file was created every time during authentication. By default, the "${HOME}/.vas_logon_server" file is not created anymore. This file contains the name of the server that performed the authentication. The "pam_vas" component uses the "advertise_auth_server" option now instead of the previous "no_advertise_auth_server" option. The "${HOME}/.vas_logon_server" file is created only if the user enables the "advertise_auth_server" option.	278331
When the user is logging in as an Active Directory user, the Management Console for Unix (MCU) displays either of the following error messages: Communication error. [Error performing LDAP operation] Communication error. [Login failed because user SID could not be resolved with AD.] This error is caused while updating the Safeguard Authentication Configuration (SAC), because the "ComputerName" and the "OperatingSystem" entries may be added to the Active Directory Schema with empty descriptions. The MCU cannot handle items with empty descriptions, which causes MCU to break. The fix ensures that when updating the SAC, the "ComputerName" and the "OperatingSystem" entries always have a default description.	276393
On recent AIX, DB2 may crash in certain edge cases due to thread safety issues. Added mutexes to avoid concurrency issues on multiple threads and prevent crashing.	268477
PAM message for required password change can be customized. Wait for Pressing ENTER when connecting via ssh can be disabled. Message displayed on password change request (by default "Your password is expired. Please follow the prompts to set a new password.") can be customized. When connecting via SSH, certain messages had an additional 'Press Enter to Continue' text and were waiting for the user to press Enter. This behavior can now be disabled.	265431

System requirements

Before installing Safeguard Authentication Services 5.0.3, ensure that your system meets the minimum hardware and software requirements for your platform. The operating

system patch level, hardware, and disk requirements vary by Unix, Linux, and Active Directory platform, and are detailed in the *One Identity Safeguard Authentication Services Administration Guide*.

NOTE: When setting up a virtual environment, carefully consider the configuration aspects such as CPU, memory availability, I/O subsystem, and network infrastructure to ensure the virtual layer has the necessary resources available. Please consult One Identity's Product Support Policies for more information on environment virtualization.

Windows and cloud requirements

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

Table 3: 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

Product licensing

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

NOTE: While 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, you must have a valid Safeguard Authentication Services license installed for full functionality.

NOTE: In order to use Starling Two-Factor Authentication with Safeguard Authentication Services, you must have a valid license for Authentication Services with One Identity Hybrid Subscription included.

Upon receiving your license file from One Identity, copy this license file to your desktop or other convenient location.

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.
3. Click **Actions | Add a license**.
4. Browse for the license file and click **Open**.

   The license appears in the list box.

Upgrade and installation instructions

The process for upgrading the Safeguard Authentication Services Windows components from older versions is similar to the installation process. The Windows installer detects older versions and automatically upgrades them. The next time you launch Active Directory Users and Computers, Safeguard Authentication Services uses the updated Windows components. Refer to the *One Identity Safeguard Authentication Services Installation Guide* for detailed installation instructions.

Safeguard Authentication Services allows you to perform all of your Unix identity management tasks from the Safeguard Authentication Services Control Center. Refer to the *One Identity Safeguard Authentication Services Upgrade Guide* for more detailed

information about upgrading your current version of Safeguard Authentication Services using the Safeguard Authentication Services Control Center.

Of course, you may perform your Unix client management tasks from the Unix command line, if you prefer. You can find those instructions in the *One Identity Safeguard Authentication Services Administration Guide*.

More resources

Additional information is available from the following:

- Online product documentation: https://support.oneidentity.com/safeguard-authentication-services/technical-documents
- Unix Access Management Community forum: https://www.quest.com/community/one-identity/unix-access-management/

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan.

This release has the following known capabilities or limitations: There is no localization.

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

Third-party contributions

This product contains some third-party components (listed below). Copies of their licenses may be found at referencing https://www.oneidentity.com/legal/license-agreements.aspx. Source code for components marked with an asterisk (*) is available at http://opensource.quest.com.

Table 4: List of Third-Party Contributions

Component	License or Acknowledgement

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.