Safeguard Authentication Services 5.0.2

Safeguard Authentication Services Release Notes

07 May 2021, 10:16

These release notes provide information about the Safeguard Authentication Services 5.0.2 release.

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 5.0.2 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.

Resolved issues

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

Table 1: General resolved issues in version 5.0.2

Resolved Issue	Issue ID
Fixed issue when the `preflight` tool mistakenly detects that `88` / TCP port is blocked.	198217
Fixed issue when Azure Active Directory refuses to import / create service accounts with invalid UPN format.	198971
We provide newer format rpm packages, which can be installed on RHEL 8 that is switched to FIPS compliant mode as well.	251223
Fixed issue when a communication failure with the AD erroneously leads to user being removed from the user cache.	256249
`vastool`: Added proper warning message when `vastool` cannot find an entry in AD if the search-base setting is incorrect.	261831
Fixed crash of SAS Control Center when a user without the appropriate permission attempts to modify Starling proxy settings.	264357
Fixed issue with Starling Two Factor Authentication tokens that are not precisely 7 characters long. Safeguard Authentication Services now accepts tokens of dynamic length, within the valid range of 6 - 8 characters.	267194
Fixed issue where Safeguard Authentication Services version 5.0.1 could not be installed on macOS 11.2+ 'Big Sur'.	268744
Fixed bug when Unix attributes are not visible due to QAC / Windows client version mismatch.	270055
Fixed bug when adding / removing users to / from mapped user file caused other, random users to become unmapped.	270424

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 2: Unix agent: Supported platforms

Platform	Version	Architecture
Amazon Linux AMI		x86_64
Apple macOS	10.13 or later	x86_64
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	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

Platform	Version	Architecture
SuSE Linux Enterprise Server (SLES)/Workstation	11, 12, 15	Current Linux architectures: s390, s390x, PPC64, PPC64le, IA-64, x86, x86_64, AARCH64
Ubuntu	Current supported releases	x86_64, x86, AARCH64

System requirements

Before installing Safeguard Authentication Services 5.0.2, 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

System requirements	
	- 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 services	- AWS Directory Service for Microsoft Active Directory (also called AWS Managed Microsoft AD) - 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

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

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

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

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

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.**