Standalone Sentry 9.13.0 Release and Upgrade Notes

for Core and Cloud

Revised: October, 2021

Contents

Revision history

TABLE 1. REVISION HISTORY

Date	Revision
October 08, 2021	Added AL-15149 to "Limitations for Standalone Sentry" on page 17.
June 11, 2021	Added IBM Lotus Notes Traveler support for 11.0.1. For more information, see "Standalone Sentry new features" on page 5 and "Support and compatibility for Standalone Sentry " on page 7.

About Standalone Sentry

Sentry is a part of Ivanti deployment that interacts with your company ActiveSync server, such as a Microsoft Exchange Server, or with a backend resource such as a SharePoint server. Sentry, with input from the Unified Endpoint Management (UEM) platform, does the following:

- Standalone Sentry configured for ActiveSync protects the ActiveSync server from wrongful access from devices.
- Standalone Sentry configured for AppTunnel provides authenticated apps secure access to the backend resource.

The UEM platform is either Core or Cloud.

For complete product documentation, see Sentry Product Documentation

Standalone Sentry new features

For new features and enhancements provided in previous versions, see the release notes for those versions.

This section provides summaries of new features and enhancements available in this release. References to documentation describing these features and enhancements are also provided, when available.

Standalone Sentry features common to UEM platforms

The following new Standalone Sentry features and enhancements are available for the UEM platforms:

- **Support for IBM Lotus Notes Traveler**: IBM Lotus Notes Traveler 11.0.1 is now supported with this release.
- **Support for VMware ESXi 7.0**: VMware EXSi 7.0 is now supported for Sentry 9.13.0.
- **Support for AWS inplace upgrade**: The AWS inplace upgrade is now supported with Sentry 9.13.0.
- **Support to enable HSTS on web services that talk to web browsers**: Enabling HSTS (RFC 6797) enforces secure HTTPS connection between web services that talk to the web browsers and Standalone Sentry. By default, HSTS is disabled. For more information, see "Enabling and disabling webservice HSTS" in the *Standalone Sentry Guide*.
- **Validate signature for authentication requests**: When configuring a Federated Pair in Access, the checkbox labeled "Validate signature for authentication requests" should be enabled. For backward compatibility, this option is unchecked for the existing pairs. Ensure that the SP/IdP metadata is updated and enable the checkbox.
- **Support for Netapp ONTAP share v9.6P4**: Netapp ONTAP share v9.6P4 is now supported with Standalone Sentry 9.13.0.
- **Support for open-vm-tools**: The open-vm-tools rpm is now installed by default when Sentry runs on VMware platform and is not required to install the VMware tools manually. For more information, see "Installing VMware tools" in the Standalone Sentry Installation Guide.
- **Support to add Login Banner**: Login Banner can now be added to display disclaimers on the login screen. For more information, see "Login" in the *Standalone Sentry Guide*.
- **Support to add idle Timeout**: You can now add idle session timeout for Sentry System Manager. For more information, see "Timeout" in the *Standalone Sentry Guide*.

Standalone Sentry features for Core

This release does not include new features or enhancements for Core.

Standalone Sentry features for Cloud

This release does not include new features or enhancements for Cloud.

Support and compatibility for Standalone Sentry

This section includes the components that are supported, or are compatible, with this release of the product.

The information provided is current at the time of this release. For product versions available after this release, see that product version's release notes for the most current support and compatibility information.

This section contains the following information:

Support policy

Ivanti defines supported and compatible as follows:

TABLE 1. SUPPORTED AND COMPATIBLE DEFINITIONS

Term	Definition
Supported product versions	The functionality of the product and version with currently supported releases was systematically tested as part of the current release and, therefore, will be supported.
Compatible product versions	The functionality of the product and version with currently supported releases has not been systematically tested as part of the current release, and therefore not supported. Based on previous testing (if applicable), the product and version is expected to function with currently supported releases.

Ivanti end of sale and support policy

See the End of Sale and Support Policy.

Supported platforms for Standalone Sentry

The following table provides the supported UEM and Access versions for Standalone Sentry for this release. See also the Cloud or Core Release Notes for the supported Standalone Sentry version.

TABLE 2. SUPPORTED UEM AND ACCESS VERSIONS

Product	Supported	Compatible
Core	11.2.0.0, 11.2.1.0	11.1.0.0
Cloud	R74 through the most recently released version as supported by Ivanti	Not applicable Only the latest version is available to all customers.
Access	R47 through the most recently released version as supported by Ivanti	Not applicable Only the latest version is available to all customers.

Supported ActiveSync servers for Standalone Sentry

The following table provides the supported ActiveSync server versions for Standalone Sentry for this release.

TABLE 3. ACTIVESYNC SERVER SUPPORT FOR STANDALONE SENTRY

ActiveSync Server	Supported Versions	Compatible Versions
Microsoft Exchange Server	2019 CU9 2016 CU20 2013 CU23 2010 SP3 RU32	2019 CU1 2019 CU2 2019 CU3 2019 CU4 2019 CU5 2019 CU6 2016 CU8 2016 CU9 2016 CU10 2016 CU11 2016 CU12 2016 CU13 2016 CU14 2016 CU17 2016 CU19 2013 CU19 2013 CU20 2013 CU21 2010 2010 SP1 2010 SP2 2010 SP3 RU21 2010 SP3 RU24 2010 SP3 RU26 2010 SP3 RU29 2010 SP3 RU30
Microsoft Office 365	Current version of Office 365	Not Applicable (All listed versions are tested and supported)
IBM Lotus Notes Traveler	11.0.1	10.0.1.1 10.0.0.0 9.0 9.0 (9.00.12342) 9.0.1 9.0.0.1 9.0.1.3

TABLE 3. ACTIVESYNC SERVER SUPPORT FOR STANDALONE SENTRY (CONT.)

ActiveSync Server	Supported Versions	Compatible Versions
		9.0.1.7 9.0.1.8 9.0.1.10 9.0.1.14 9.0.1.15 9.0.1.17 9.0.1.18 9.0.1.20 9.0.1.21 8.5.3 UP 1 8.5.3 UP 2 8.5.3 8.5.2.1 8.5.2 UP 2 8.5.2
Gmail	Current cloud version of Gmail	Not applicable since only the latest version is available to customers
GroupWise	18.1	GroupWise Mobility Service (GMS) 2.1.0 14.0.2, 14.2.2 GroupWise Mobility Service 18

Note The Following:

- To use IBM Lotus Domino with Standalone Sentry, install IBM Lotus Notes Traveler software on the Lotus Domino server. Lotus Traveler provides ActiveSync services for Lotus Domino.
- When you use Standalone Sentry with Gmail, end-users may attempt to configure their email clients to bypass Standalone Sentry by manually configuring an ActiveSync server of m.google.com. Google provides capabilities to set up IP access lists for ActiveSync traffic, which can be used to circumvent this.
- ActiveSync management (Wipe, Assign Policy, and Revert Policy in the ActiveSync page) is not supported with Gmail.
- If you are using Lotus Notes Traveler with Standalone Sentry, only the IBM Android client is recommended on Android devices.

- After upgrading Exchange 2010 from SP2 to SP3, Integrated Sentry stops syncing.
  Workaround: See http://support.microsoft.com/kb/2859999/en-us. The article on the Microsoft support site explains the problem and discusses a workaround.
- Microsoft only supports Standalone Sentry with dedicated Office 365 instances. Microsoft does not recommend Standalone Sentry with regular multi-tenant instances of Office 365. However, Ivanti supports the deployment of Standalone Sentry with dedicated or multi-tenant instances of Office 365, and strongly recommends deploying Standalone Sentry if you are supporting more than 5000 devices with Office 365.
- ActiveSync policies and adding multiple ActiveSync accounts are not supported with GroupWise.

Supported browsers for Standalone Sentry

The following table provides the supported browser versions for the Standalone Sentry system manager for this release.

TABLE 4. BROWSER SUPPORT FOR THE STANDALONE SENTRY WEB PORTAL (SYSTEM MANAGER)

Browser	Supported	Compatible
Internet Explorer	11	9, 10
Chrome	89	84
Firefox	86	79
Safari	14	13.1

Supported protocols for Standalone Sentry

Standalone Sentry supports only HTTP 1.1 to communicate with devices and backend resources.

Exchange ActiveSync, also known as ActiveSync, is the protocol that the ActiveSync server uses to communicate over HTTP or HTTPS with devices. Standalone Sentry supports up to ActiveSync protocol version 16.1 for its communication with the ActiveSync server and with ActiveSync devices.

Note The Following:

- For devices that are already registered, you have to push the Exchange profile to the device to force the device to use the new protocol version. If the protocol version is limited to 14.0 or 14.1, devices will use the selected version to communicate with the ActiveSync server. Alternately, device users can go to iOS device **Settings > Mail > Accounts**, select the enterprise mail account, and toggle to disable and re-enable the mail account.
- EAS 16.0, 16.1 are only supported on the following:
  - iOS native client on iOS 10 through the latest version as supported by Ivanti.
  - Windows 10 devices through the latest version as supported by Ivanti.
- Exchange ActiveSync (EAS) version 16.1, provides a policy to 'Exchange Account Remote Wipe.' For the policy to be applied to the device, the **Default ActiveSync Policy behavior** for Standalone Sentry in Core must be set to **Apply AS Server Policy**. For registered devices, the default on Core is set to **Remove AS Server policy**. If the **Default ActiveSync Policy behavior** is set to **Remove AS Server policy**, the policy from the EAS server is not applied. This causes the device and the EAS server to be out of sync. The status on the device remains as 'Access Granted.' However, the status for the device on the server is 'Account Only Remote Wipe.'

  NOTE: If the Default ActiveSync Policy behavior is set as **Apply AS Server Policy**, the EAS server's policy is applied rather than the policies configured in Core.
- Integrated Sentry does not use the ActiveSync protocol to communicate with the Microsoft Exchange Server. Also, the Microsoft Exchange Server, not the Integrated Sentry, communicates with the ActiveSync devices. Therefore, ActiveSync protocol version support is not applicable to Integrated Sentry.
- Exchange 2010 SP2 reports the MS-Server-ActiveSync version as 14.2. This refers to the Exchange 2010 server version and not the ActiveSync protocol version.

Supported content repositories for Standalone Sentry

The following table provides the supported content repositories for Standalone Sentry for this release.

TABLE 5. SUPPORTED CONTENT REPOSITORIES

Content Repository	Supported	Compatible
SharePoint	• Microsoft SharePoint 2007 • Microsoft SharePoint 2010 • Microsoft SharePoint 2013 • Microsoft SharePoint Office 365 • OneDrive for Business Only OneDrive for Business (with SharePoint and Office 365) is supported. OneDrive (personal online storage for consumers) is not supported. NOTE: Users on SharePoint must have at least Contribute permissions.	Not applicable since all versions are supported.
Network Drive	• CIFS Windows 2012 R2 • CIFS Windows 2008 R2 SP1 • CIFS Samba CentOS 6.2 • NetApp 8.3 RC2 • WebDAV • Apache-based WebDAV content repositories • IIS-based WebDAV content repositories • SMB 2.0, 2.1 only • DFS	Not applicable since all versions are supported.

Supported Microsoft Azure Resource Manager CLI version

Azure CLI 2.7.

Resolved issues for Standalone Sentry

For resolved issues fixed in previous releases, see the "Resolved issues" section in the release notes for those releases.

General resolved issues for Standalone Sentry 9.13.0

The following issues are resolved in this release:

- **AL-12694**: Previously, Sentry miaudit log files were not purged/rotated correctly and system log file was flooded with 'mi-logrotate: ALERT exited abnormally with [1]'.
  This issue is now fixed.
- **AL-14616**: Previously, after 2 GB of device cache entries, new entries were not being reported.
  This issue is now fixed.
  A cleanup occurs every 10 minutes, which removes the oldest entry and the new entry is appended to all devices.
- **AL-15200**: Previously, for IpTunnel, Sentry had a maximum HTTP header size of 8192 and the value was not configurable.
  This issue is now fixed.
- **AL-15311**: Previously, rebooting a physical appliance would sometimes result in network interface card (NIC) swapping, which caused problems with interface configuration.
  This issue is now fixed.
- **AL-15321**: Previously, when a virtual machine was configured with 2 hard disks of same size, the upgrade from Sentry 9.9.0 to Sentry 9.12.0 failed.
  This issue is now fixed
- **AL-15411**: Previously, show system top CLI command failed with 'permission denied' error message.
  This issue is now fixed.
- **AL-15416**: Previously, the iptables enable/disable status was not displayed correctly with show service command.
  This issue is now fixed.

Standalone Sentry resolved issues for Access

There are no new resolved issues found in this release.

Standalone Sentry resolved issues for Core

There are no new resolved issues found in this release.

Standalone Sentry resolved issues for Cloud

There are no new resolved issues found in this release.

Known issues for Standalone Sentry

For known issues found in previous releases, see the "Known issues" section in the release notes for those releases.

This release includes the following known issues.

- **AL-15278**: The AWS Sentry CLI update for DNS configuration does not populate back on Standalone Sentry System Manager UI.
- **AL-15403**: The Sentry Access Control List (ACL) rules are not working correctly when a user tries to block SSH from all machines and allows access only from one machine.
- **AL-15405**: Delegated IDP for ADFS set up is not working correctly after upgrading from Sentry 9.8.1 to Sentry 9.9.0. Authentication fails with ADFS.
- **AL-15415**: After upgrading AWS from Sentry 9.9.0 to Sentry 9.13.0, an NTP error is observed only once.
  This error does not affect any functionality.
- **AL-15431**: The CLI command debug sentry device-cache size default fails to run in CLI Config mode.
  Workaround: Enter a value for cache size and then run the command.
  For example: `debug sentry device-cache size 110000`.

Limitations for Standalone Sentry

For third-party limitations found in previous releases, see the "Limitations" section in the release notes for those releases.

This release includes the following limitations.

- **AL-15149**: On MobileIron Core and MobileIron Cloud, OAuth is not supported using device authentication with ID cert.
- **AL-15356**: Access to CIFS shares fails on a NetApp filer that uses Kerberos authentication.
- **AL-15407**: Sentry MICS SMC (Sentry Monitoring System) displays multiple exceptions when external websites are opened with Web@Work.

Software download for Standalone Sentry

- The Standalone Sentry ISO file for installing on-premise is available for download at https://support.mobileiron.com/support/CDL.html
- The Standalone Sentry ISO file for installing on Microsoft Azure is available at https://mobileironsentry.blob.core.windows.net/mobileironsentrycontainer/sentry-mobileiron-9.13.0-18.vhd
    - Json files needed for installation: https://mobileironsentry.blob.core.windows.net/mobileironsentrycontainer/SentryAzureDeploy.parameters-9.13.0-18.json
    - https://mobileironsentry.blob.core.windows.net/mobileironsentrycontainer/SentryAzureDeploy-9.13.0-18.json
- The Standalone Sentry ISO file for installing on Amazon Web Services (AWS) is available on the AWS community as a public Amazon Machine Image (AMI) in multiple AWS regions. The Standalone Sentry AWS AMI is published with the owner ID: 0555540e173cb462b.

The instructions for installing Standalone Sentry are provided in the *Standalone Sentry Installation Guide* for the release.

Upgrade information for Standalone Sentry

This section provides the upgrade information for this release and contains the following sections:

Before you upgrade Standalone Sentry

- Ensure that the Standalone Sentry System Manager (MICS) portal certificate has not expired. AL-12204: If the Standalone Sentry portal certificate has expired prior to a software upgrade, Standalone Sentry generates a new self-signed certificate after the upgrade and does not initialize correctly. As a result, the Standalone Sentry System Manager (MICS) on port 8443 and the Standalone Sentry server on port 443 will not be accessible. The "show log message" CLI displays the following error: "portal-ca-setup: /mi/portalCA/ca-cert.pem not valid for /mi/portalCA/server-cert.pem".
- Plan for 5 to 20 minutes downtime. Email and app tunnel traffic will be down during the upgrade.
- If you have multiple Standalone Sentry in your our installation, allow for a rolling upgrade to minimize downtime. Do not upgrade all Sentry instances at the same time.
- Ensure that Core is running and reachable to allow Standalone Sentry to upgrade successfully.
- Verify that your current environment meets the requirements as listed in the "Support and compatibility for Standalone Sentry " on page 7 of this document.
- Check disk space availability. At least 5 GB of disk space must be available in the / (root) directory for an upgrade to be successful.
- Back up the Standalone Sentry installation configuration.
- Test your connection to support.mobileiron.com. You can use the following command: telnet support.mobileiron.com 443.
- Ensure that supportcdn.mobileiron.com is reachable.

- For improved security, Ivanti recommends that TLS v1.2 is used and TLS v1.0 and v1.1 are disabled. Run the TLS compliance utility to check the TLS compliance for the servers connecting to Standalone Sentry. See "TLS compliance utility" below.
- See also "Upgrade notes for Standalone Sentry" on the next page.

Supported upgrades paths for Standalone Sentry

The following table provides the supported upgrade paths for Standalone Sentry for this release.

Upgrade for Sentry 9.10.0 and Sentry 9.12.0 to Sentry 9.13.0 is not supported for AWS.

TABLE 1. SUPPORTED PATHS FOR UPGRADE

Current Standalone Sentry version	Upgrade path to 9.13.0
9.8.1	9.8.1 > 9.9.0 > 9.13.0
9.9.0	9.9.0 > 9.13.0
9.10.0	9.10.0 > 9.13.0
9.12.0	9.12.0 > 9.13.0

Upgrade URL for CLI upgrades for Standalone Sentry

Use the following URL if you are upgrading using the CLI upgrade method:

https://support.mobileiron.com/mi/sentry/9.13.0/

TLS compliance utility

Ivanti provides an utility that checks if Sentry can successfully connect with the server on TLS v1.2.

You must have Sentry 9.6.0 or later as a minimum version of TLS compliance utility.

From the Standalone Sentry command line interface, enter the following command in EXEC PRIVILEGED mode to run the utility:

```
#install rpm url https://support.mobileiron.com/tlscheck/mobileiron-sentry-tlscheck-1.0.0-1.noarch.rpm
```

The command executes a script that checks the servers that Sentry connects with and returns an OK or FAILED value for each server it checks. The script uninstalls after each run.

The results are also recorded into a log file /var/log/TLSTrafficTool-*timestamp*.log. The log file is included in ShowTech-All. In case of failure, additional error message content as provided by OpenSSL displays and is recorded in the log file. Ivanti recommends upgrading the failed servers to support TLS v1.2.

After upgrading to 9.7.0, use the tlscheck command from the Standalone Sentry command line interface (CLI) to check TSL compliance. See "Using CLI command to check TLS compliance" in the *Sentry Guide*.

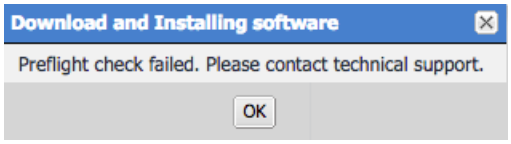
Upgrade notes for Standalone Sentry

Before you upgrade, read the following upgrade notes:

Telnet

Telnet server capability is not supported from Standalone Sentry 9.5.0 onwards. Disable Telnet before upgrading to 9.7.0. Upgrade fails if Telnet is not disabled. You will see the following **Preflight check failed** error message if Telnet is enabled.

FIGURE 1. PREFLIGHT CHECK FAILED ERROR MESSAGE



Click **OK**, then disable Telnet. To disable Telnet, in Standalone Sentry system manager, go to **Settings > CLI**.

You will also see the following log message in **Monitoring > Alert Viewer**:

```
Upgrade failure: Telnet server is not supported anymore. You must first disable telnet before
upgrade. The system will continue to run as Current Sentry Version.
```

Support for SMB

Ivanti dropped support for SMB 1.0 CIFS servers and added support for SMB 2.0 and 2.1. If you were accessing an SMB 1.0 CIFS server through Standalone Sentry, upgrading to Standalone Sentry 9.4.1 through the latest version as supported by Ivanti results in users not being able to authenticate and therefore access the CIFS server.

Workaround: Ivanti recommends updating the file server to SMB 2.0 or 2.1 before upgrading to Standalone Sentry 9.4.1 through the latest version as supported by Ivanti.

Supported upgrade versions for Standalone Sentry

If you are upgrading from a version not listed in "Supported upgrades paths for Standalone Sentry " on page 20, then you need to complete one or more previous upgrades first. See the release notes for the version to which you will upgrade.

IBM Lotus Notes Traveler

If you are using IBM Lotus Notes Traveler, SSLv3 protocol is disabled by default. This may impact device connectivity if you are using older versions of IBM Lotus Notes Traveler. Some older versions of Lotus Notes Traveler have not implemented TLS 1.0, resulting in the failure to negotiate a connection after the upgrade. IBM has released an interim fix to address this issue. For more information on how this upgrade may impact your environment see the *Sentry 7.0 and Traveler Environments* Knowledge Base article in the Ivanti support community.

Missing command outputs in archived showtech.txt file

AL-9823: The *version*-showtech-*date*.txt files in the upgrades directory in showtech.zip are different from the showtech.txt in the zip file. The *version*-showtech-*date*.txt files are created soon after the system reboots and before the installation of any packages starts. Since there is no system service running at that time, some of the commands, which require system service running, have the empty outputs. This is seen in the following upgrade paths: 8.0.1 > 8.5.0 and 8.0.1 > 9.0.0.

Upgrade steps for Standalone Sentry

For upgrade instructions, see the following sections in the *Sentry Guide* for the release:

- For upgrade instructions using the Standalone Sentry System Manager UI, see “Standalone Sentry software updates.”
- For upgrade instructions using the Standalone Sentry command line interface (CLI), see “Upgrading using CLI.”
- For multiple Sentry upgrade instructions using the Standalone Sentry CLI, see "Upgrading multiple Standalone Sentry."

Documentation resources

Product documentation is available on the Ivanti documentation website.

To access documentation, navigate to a specific product and click the **>** symbol next to the name to view all documents in that product category.

Current release documentation is available in the main section. For prior versions, navigate to the **ARCHIVED DOCUMENTATION** section at the bottom of the page.

If you have a Cloud deployment, the *Cloud Administrator Guide* is also available from your instance of Cloud through the **Help** link in the user interface.

Sentry documentation

The following is a list of the documentation:

- *Standalone Sentry Release Notes and Upgrade Guide*

  Contains the following release-specific information: new feature summary, support and compatibility, upgrade notes, known and resolved issues, and limitations.

- *Standalone Sentry Installation Guide*

  The installation guide includes pre-deployment tasks, requirements, and steps to install and configure Standalone Sentry.

- *Sentry Guide for Cloud*

  The complete guide to setting up and managing Standalone Sentry for Cloud, including ActiveSync and AppTunnel.

- *Sentry Guide for Core*

  The complete guide to setting up and managing Standalone Sentry for Core, including ActiveSync and AppTunnel.

- *Authentication using Kerberos Constrained Delegation*

  This document explains how to install, configure, and use Kerberos constrained delegation for authentication for Core deployments.

- *Integrated Sentry Release Notes*

  Contains the following release-specific information: new feature summary, support and compatibility, known and resolved issues, and limitations.

- *Integrated Sentry Installation and Upgrade Guide*

  This guide contains information about installing and upgrading Integrated Sentry. For information about ActiveSync features, see the *Sentry Guide for Core*.