MobileIron Standalone Sentry 9.9.0 Release and Upgrade Notes

for MobileIron Core and MobileIron Cloud

September 09, 2020

For complete product documentation see:
MobileIron Sentry Product Documentation

Contents

Contents **3**

About Standalone Sentry **5**

Standalone Sentry new features **5**

Standalone Sentry features common to MobileIron UEM platforms 5

Standalone Sentry features for MobileIron Core 6

Standalone Sentry features for MobileIron Cloud 6

Support and compatibility for Standalone Sentry **6**

Support policy 6

MobileIron end of sale and support policy 7

Supported MobileIron platforms for Standalone Sentry 7

Supported ActiveSync servers for Standalone Sentry 7

Supported browsers for Standalone Sentry 9

Supported protocols for Standalone Sentry 9

Supported content repositories for Standalone Sentry 10

Supported Microsoft Azure Resource Manager CLI version 11

Resolved issues for Standalone Sentry **11**

General resolved issues for Standalone Sentry 9.9.0 11

Standalone Sentry resolved issues for MobileIron Access 11

Standalone Sentry resolved issues for MobileIron Core 12

Standalone Sentry resolved issues for MobileIron Cloud 12

Known issues for Standalone Sentry **12**

Limitations for Standalone Sentry **12**

Software download for Standalone Sentry **12**

Upgrade information for Standalone Sentry **13**

Before you upgrade Standalone Sentry 13

Supported upgrades paths for Standalone Sentry 13

Upgrade URL for CLI upgrades for Standalone Sentry 14
TLS compliance utility 14
Upgrade notes for Standalone Sentry 14
Telnet 15
Support for SMB 15
Supported upgrade versions for Standalone Sentry 15
IBM Lotus Notes Traveler 15
Missing command outputs in archived showtech.txt file 16
Upgrade steps for Standalone Sentry 16
Documentation resources 16

About Standalone Sentry

MobileIron Sentry is a part of a MobileIron 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 MobileIron Enterprise Mobility Management (EMM) 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 MobileIron EMM platform is either MobileIron Core or MobileIron Cloud.

For complete product documentation, see MobileIron Sentry Product Documentation

Standalone Sentry new features

For new features provided in previous releases, see MobileIron Sentry Product Documentation for that release.

The following are new features and enhancements available in this release and are divided into the following categories:

- Standalone Sentry features common to MobileIron UEM platforms
- Standalone Sentry features for MobileIron Core
- Standalone Sentry features for MobileIron Cloud

Standalone Sentry features common to MobileIron UEM platforms

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

- **Shorter lifespan for self-signed TLS certificates**: Beginning September 1, 2020, Apple requires that valid Transport Layer Security (TLS) certificates expire in 397 days or less. From Sentry 9.9.0 through the latest release supported by MobileIron, the lifespan of self-signed TLS certificates will be limited to fewer than 398 days.

- **Support for adding authentication to Outbound HTTP proxy**: The Outbound HTTP proxy page allows the administrator the flexibility to configure Standalone Sentry with outbound HTTP proxy server settings. The traffic from Sentry passes through the proxy to Cloud or Access. Sentry will use the User Name and Password for authentication if requested by the proxy. For more information, see "Configuring Outbound HTTP Proxy" in the *MobileIron Sentry Guide*.

Standalone Sentry features for MobileIron Core

There are no new Standalone Sentry features and enhancements available for MobileIron Core only.

Standalone Sentry features for MobileIron Cloud

There are no new Standalone Sentry features and enhancement available for MobileIron Cloud only.

Support and compatibility for Standalone Sentry

The information in this section includes the components MobileIron supports with this product.

NOTE: This information is current at the time of this release. For MobileIron product versions released 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
- MobileIron end of sale and support policy
- Supported MobileIron platforms for Standalone Sentry
- Supported ActiveSync servers for Standalone Sentry
- Supported browsers for Standalone Sentry
- Supported protocols for Standalone Sentry
- Support and compatibility for Standalone Sentry
- Supported Microsoft Azure Resource Manager CLI version

Support policy

MobileIron 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.

MobileIron end of sale and support policy

See the MobileIron End of Sale and Support Policy.

Supported MobileIron platforms for Standalone Sentry

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

TABLE 2. SUPPORTED MOBILEIRON UEM AND ACCESS VERSIONS

Product	Supported	Compatible
MobileIron Core	10.8.0.0	10.5.2.1, 10.6.0.1, 10.7.0.0
MobileIron Cloud	R72 through the most recently released version as supported by MobileIron	Not applicable Only the latest version is available to all customers.
MobileIron Access	R41 through the most recently released version as supported by MobileIron	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 CU1 2019 CU2 2019 CU3 2019 CU4 2019 CU5 2019 CU6 2016 CU12 2016 CU13 2016 CU14 2016 CU17 2013 CU23	2016 CU8 2016 CU9 2016 CU10 2016 CU11 2013 CU19 2013 CU20 2013 CU21 2010 2010 SP1 2010 SP2 2010 SP3 RU21

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

ActiveSync Server	Supported Versions	Compatible Versions
	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	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 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, MobileIron 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	84	74, 78
Firefox	79	67, 70
Safari	13.1	12.1.2

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 MobileIron.
  - Windows 10 devices through the latest version as supported by MobileIron.
- 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 MobileIron Core must be set to **Apply AS Server Policy**. For registered devices, the default on MobileIron 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 MobileIron 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 2.0.

Resolved issues for Standalone Sentry

For resolved issues provided in previous releases, see MobileIron Sentry Product Documentation for that release.

The following issues are fixed in this release and are categorized into the following sections:

- General resolved issues for Standalone Sentry 9.9.0
- Standalone Sentry resolved issues for MobileIron Access
- Standalone Sentry resolved issues for MobileIron Core
- Standalone Sentry resolved issues for MobileIron Cloud

General resolved issues for Standalone Sentry 9.9.0

- **AL-14643**: Previously, connections to share point server from Chrome browser on Windows using NTLM authentication failed. This issue is fixed.
- **AL-14709**: Previously, when attachment control was enabled in Sentry and an email contained no MIME part boundaries, Sentry tried to encode the plain text mail content which caused distorted text when the mail content had umlaut characters. This issue is fixed.
- **AL-14720**: Previously, special characters such as backspaces, quotation marks, and spaces were not allowed in the tenant password when registering MobileIron Sentry to Cloud or Access. This issue is fixed.
- **AL-14736**: Previously, the tunneled proxy connect requests from a device to Sentry failed if the proxy listening port was 80. This issue is fixed.
- **AL-14842**: Previously, requests sent from a device contained HTTP chunked data format. Sentry was unable to format the data correctly and send the data in multiple buffers to the associated proxy. This issue is fixed by handling the data in a single buffer.
- **AL-14864**: Previously, the older versions of Sentry "Check Updates" displayed error "download failed" when no updates were available. This issue is fixed.

Standalone Sentry resolved issues for MobileIron Access

- **AL-14608**: Previously, when Access was configured as a delegated IdP with Microsoft ADFS and DEL IDP with SAML assertion encryption disabled, users with accent characters (such as é, ô) in DistinguishedName or CanonicalName failed to log in to service providers applications. This issue is fixed.

Standalone Sentry resolved issues for MobileIron Core

- **AL-14584**: Previously, when using a self-signed certificate for Sentry, clicking on **Edit** on Sentry settings in MobileIron Core and then saving without any changes, regenerated the self-signed certificate. This issue is fixed.

Standalone Sentry resolved issues for MobileIron Cloud

There are no new resolved issues that impact only MobileIron Cloud deployments.

Known issues for Standalone Sentry

For known issues found in previous releases, see MobileIron Sentry Product Documentation for that release.

There are no new known issues found in this release.

Limitations for Standalone Sentry

For limitations found in previous releases, see MobileIron Sentry Product Documentation for that release.

There are no new limitations for this release.

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-9.9.0-24.vhd
  Json files needed for installation:
  https://mobileironsentry.blob.core.windows.net/mobileironsentrycontainer/SentryAzureDeploy.parameters.json

  https://mobileironsentry.blob.core.windows.net/mobileironsentrycontainer/SentryAzureDeploy.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: 090bbe67e56915667.

The instructions for installing Standalone Sentry are provided in the *MobileIron 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
- Supported upgrades paths for Standalone Sentry
- Upgrade URL for CLI upgrades for Standalone Sentry
- TLS compliance utility
- Upgrade notes for Standalone Sentry
- Upgrade steps for Standalone Sentry

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 MobileIron 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 of this document.
- Check disk space availability. At least 2 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, MobileIron 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.
- See also Upgrade notes for Standalone Sentry.

Supported upgrades paths for Standalone Sentry

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

TABLE 6. SUPPORTED PATHS FOR UPGRADE

Current Standalone Sentry version	Upgrade path to 9.8.0
9.7.3	9.7.3 > 9.8.1 > 9.9.0 9.7.3 > 9.9.0

TABLE 6. SUPPORTED PATHS FOR UPGRADE (CONT.)

Current Standalone Sentry version	Upgrade path to 9.8.0
9.8.0	9.8.0 > 9.8.1 > 9.9.0 9.8.0 > 9.9.0
9.8.1	9.8.1 > 9.9.0
9.8.5	9.8.5 > 9.9.0

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/9.9.0/

TLS compliance utility

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

NOTE: 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. MobileIron 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 *MobileIron Sentry Guide*.

Upgrade notes for Standalone Sentry

Before you upgrade, read the following upgrade notes:

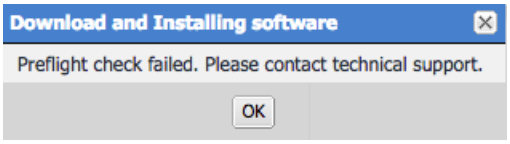
Telnet
Support for SMB

Supported upgrade versions for Standalone Sentry
IBM Lotus Notes Traveler
Missing command outputs in archived showtech.txt file

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**.

NOTE: 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

MobileIron 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 MobileIron results in users not being able to authenticate and therefore access the CIFS server.

Workaround: MobileIron 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 MobileIron.

Supported upgrade versions for Standalone Sentry

If you are upgrading from a version not listed in Supported upgrades paths for Standalone Sentry, 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 MobileIron support community at https://help.mobileiron.com.

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 *MobileIron 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

MobileIron product documentation is available at https://help.mobileiron.com/s/mil-productdocumentation.

The *MobileIron Cloud Administrator Guide* is also available from your instance of MobileIron Cloud by clicking on the **Help** link in the user interface.

MobileIron Support credentials are required to access documentation in the Support Community.