



# **Ivanti Standalone Sentry 9.14.0 - 9.20.0 Release Notes**

**March 2024**

# Contents

---

- Revision history** ..... 3
- New features summary** ..... 4
  - Ivanti Standalone Sentry features for Ivanti Email+ ..... 4
  - Related information from previous releases ..... 4
- Support and compatibility** ..... 5
  - Supported platforms for Ivanti Standalone Sentry ..... 5
  - Supported ActiveSync servers for Ivanti Standalone Sentry ..... 6
  - Supported browsers for Standalone Sentry ..... 8
  - Supported protocols for Ivanti Standalone Sentry ..... 8
  - Supported content repositories for Standalone Sentry ..... 9
  - Supported Microsoft Azure Resource Manager CLI version ..... 10
  - Support policy ..... 11
  - Ivanti end of sale and support policy ..... 11
  - Related information from previous releases ..... 11
- Resolved issues** ..... 13
  - Related information from previous releases ..... 13
- Known issues** ..... 14
  - Related information from previous releases ..... 14
- Limitations** ..... 15
  - Related information from previous releases ..... 15
- Software download** ..... 16
- Upgrade information** ..... 18
  - Before you upgrade Ivanti Standalone Sentry ..... 18
  - Supported upgrade paths for Ivanti Standalone Sentry ..... 19
  - Upgrade URL for CLI upgrades for Ivanti Standalone Sentry ..... 19
  - TLS compliance utility ..... 19
  - Upgrade notes for Standalone Sentry ..... 20
  - Upgrade steps for Ivanti Standalone Sentry ..... 21
- Documentation resources** ..... 22
- Sentry documentation** ..... 23

# Revision history

**TABLE 1.** REVISION HISTORY

Date	Revision
March 28, 2024	<ul style="list-style-type: none"><li>Updated for 9.14.0 - 9.20.0 Ivanti Sentry Release.</li><li>Updated the <a href="#">"Resolved issues" on page 13</a> for 9.18.0 with mutual authentication information.</li></ul>
March 20, 2024	<b>Patch Release:</b> The Ivanti Standalone Sentry 9.19.1, 9.18.1, and 9.17.1 release addresses an important security fix. For the upgrade path, see <a href="#">"Upgrade information" on page 18</a> .
February 29, 2024	Updated the <a href="#">"Support and compatibility" on page 5</a> with ActiveSync server support for Standalone Sentry supported versions.
October 23, 2023	Updated for 9.14.0 - 9.19.0 Ivanti Sentry Release.
July 18, 2023	Updated for 9.14.0 - 9.18.0 Ivanti Sentry Release.
December 15, 2022	Updated for 9.14.0 - 9.17.0 Ivanti Sentry.
August 08, 2022	Updated for 9.14.0 - 9.16.0 Ivanti Sentry.
May 20, 2022	<ul style="list-style-type: none"><li>Updated the <a href="#">"Support and compatibility" on page 5</a> with Ivanti EPMM 11.6.0.1 version.</li><li>Updated the <a href="#">"Resolved issues" on page 13</a> for AL-14997 with the link to Ivanti Sentry Guide.</li></ul>
May 02, 2022	<ul style="list-style-type: none"><li>Updated the <a href="#">"Support and compatibility" on page 5</a> for 9.15.0 with Exchange server information.</li><li>Updated the <a href="#">"Resolved issues" on page 13</a> with AL-15694 issue.</li></ul>
April 05, 2022	Updated for 9.14.0 - 9.15.0 Ivanti Sentry.

# New features summary

These are cumulative release notes. If a release does not appear in this section, then there were no associated new features and enhancements.

## Ivanti Standalone Sentry features for Ivanti Email+

- **Support to connect Email+ to Sentry using MSAL library:** Starting from Ivanti Standalone Sentry release 9.20.0, Sentry now supports MSAL library for Email+.

## Related information from previous releases

If a release does not appear in this section, then there were no associated new features and enhancements.

- [Ivanti Standalone Sentry 9.18.0 - New features summary](#)
- [Ivanti Standalone Sentry 9.17.0 - New features summary](#)
- [Ivanti Standalone Sentry 9.16.0 - New features summary](#)
- [Ivanti Standalone Sentry 9.15.0 - New features summary](#)
- [Ivanti Standalone Sentry 9.14.0 - New features summary](#)

# Support and compatibility

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" on page 11](#)
- ["Ivanti end of sale and support policy" on page 11](#)
- ["Supported platforms for Ivanti Standalone Sentry" below](#)
- ["Supported ActiveSync servers for Ivanti Standalone Sentry" on the next page](#)
- ["Supported browsers for Standalone Sentry" on page 8](#)
- ["Supported protocols for Ivanti Standalone Sentry" on page 8](#)
- ["Supported content repositories for Standalone Sentry" on page 9](#)
- ["Supported Microsoft Azure Resource Manager CLI version" on page 10](#)

## Supported platforms for Ivanti Standalone Sentry

The following table provides the supported UEM and Access versions for Standalone Sentry for this release. See also the Ivanti Neurons for MDM Release Notes or Ivanti EPMM Release Notes for the supported Standalone Sentry version.

TABLE 2. SUPPORTED UEM AND ACCESS VERSIONS

Product	Supported	Compatible
Ivanti EPMM	12.0.0.0	11.12.0.1, 11.12.0.0, 11.11.0.0
Ivanti Neurons for MDM	R98 through the most recently released version as supported by Ivanti.	Not applicable Only the latest version is available to all customers.
Ivanti Access	R60 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 Ivanti 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 CU13 (KB5020999)  2016 CU23 (KB5011155)  2019 CU14 (EP Enabled by default)  2016 CU23 (EP Enabled)	2019 CU10 2019 CU11 2019 CU12  2016 CU21 2016 CU22 (KB5012698)
Microsoft Office 365	Current version of Office 365	Not Applicable (All listed versions are tested and supported)
IBM Lotus Notes Traveler	12.1	10.0.1.1  10.0.0.0  9.0.1.18 9.0.1.20 9.0.1.21
Gmail	The 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

- To use IBM Lotus Domino with Ivanti 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](https://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.
- Microsoft only supports Standalone Sentry with dedicated Office 365 instances. Microsoft does not recommend Ivanti 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 recommends deploying Ivanti 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 IVANTI STANDALONE SENTRY WEB PORTAL (SYSTEM MANAGER)

Browser	Supported	Compatible	Notes
Chrome	121	90 - 120	Version 116.0.5845.110
Firefox	122	90 - 121	

## Supported protocols for Ivanti Standalone Sentry

Ivanti 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.

- 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 Ivanti EPMM must be set to **Apply AS Server Policy**. For registered devices, the default on Ivanti EPMM 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.'



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 Ivanti EPMM.


---

- 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	<ul style="list-style-type: none"><li>• Microsoft SharePoint 2016</li><li>• Microsoft SharePoint 2019</li><li>• Microsoft SharePoint Office 365</li><li>• OneDrive for Business</li></ul> <p>Only OneDrive for Business (with SharePoint and Office 365) is supported. OneDrive (personal online storage for consumers) is not supported.</p> <div> NOTE: Users on SharePoint must have at least Contribute permissions.</div> <p>Users on SharePoint must have at least Contribute permissions.</p>	Not applicable since all versions are supported.
Network Drive	<ul style="list-style-type: none"><li>• CIFS Windows 2022</li><li>• CIFS Samba CentOS 6.2</li><li>• WebDAV</li><li>• Apache-based WebDAV content repositories</li><li>• IIS-based WebDAV content repositories</li><li>• SMB 2.0, 3.0</li><li>• DFS</li></ul>	<ul style="list-style-type: none"><li>• NetApp 8.3 RC2</li></ul>

## Supported Microsoft Azure Resource Manager CLI version

Azure CLI 2.7

# Support policy

Ivanti defines supported and compatible as follows:

**TABLE 6.** 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](#).

## Related information from previous releases

If a release does not appear in this section, then there was no associated support and compatibility.

- [Ivanti Standalone Sentry 9.19.1 - Support and compatibility](#)
- [Ivanti Standalone Sentry 9.18.1 - Support and compatibility](#)
- [Ivanti Standalone Sentry 9.17.1 - Support and compatibility](#)
- [Ivanti Standalone Sentry 9.19.0 - Support and compatibility](#)
- [Ivanti Standalone Sentry 9.18.0 - Support and compatibility](#)
- [Ivanti Standalone Sentry 9.17.0 - Support and compatibility](#)
- [Ivanti Standalone Sentry 9.16.0 - Support and compatibility](#)

- [Ivanti Standalone Sentry 9.15.0 - Support and compatibility](#)
- [Ivanti Standalone Sentry 9.14.0 - Support and compatibility](#)

# Resolved issues

These are cumulative release notes. If a release does not appear in this section, then there were no associated new resolved issues.

- **AL-16442:** When you attempted to save the email configuration on the Sentry MICS portal, previously, the message No message error displayed. After the fix, you must save the configuration, and you can view the message Email settings configured successfully.
- **AL-16207:** After an upgrade to Sentry 9.17.0, Sentry connections to some CIFS servers (likely CIFS server clusters) can fail.
- **AL-16019:** Previously, the Sentry OAuth feature's conditional access policy was failing. Starting from the Ivanti Standalone Sentry 9.20.0 release, the conditional access policy is operating as intended, and the sentry IP displays in the Azure portal rather than the device IP.

## Related information from previous releases

If a release does not appear in this section, then there were no associated resolved issues.

- [Ivanti Standalone Sentry 9.19.0 - Resolved issues](#)
- [Ivanti Standalone Sentry 9.18.0 - Resolved issues](#)
- [Ivanti Standalone Sentry 9.17.0 - Resolved issues](#)
- [Ivanti Standalone Sentry 9.16.0 - Resolved issues](#)
- [Ivanti Standalone Sentry 9.15.0 - Resolved issues](#)
- [Ivanti Standalone Sentry 9.14.0 - Resolved issues](#)

# Known issues

These are cumulative release notes. If a release does not appear in this section, then there were no associated new known issues.

## Related information from previous releases

If a release does not appear in this section, then there were no associated known issues.

- [Ivanti Standalone Sentry 9.19.0 - Known issues](#)
- [Ivanti Standalone Sentry 9.18.0 - Known issues](#)
- [Ivanti Standalone Sentry 9.17.0 - Known issues](#)
- [Ivanti Standalone Sentry 9.16.0 - Known issues](#)
- [Ivanti Standalone Sentry 9.15.0 - Known issues](#)
- [Ivanti Standalone Sentry 9.14.0 - Known issues](#)

# Limitations

These are cumulative release notes. If a release does not appear in this section, then there were no associated new limitations.

## Related information from previous releases

If a release does not appear in this section, then there were no associated limitations.

- [Ivanti Standalone Sentry 9.15.0 - Limitations](#)
- [Ivanti Standalone Sentry 9.14.0 - Limitations](#)

# Software download

- The Standalone Sentry ISO file for installing on-premise is available for download at <https://support.mobileiron.com/support/CDL.html>

The following files are available for installing Ivanti Standalone Sentry on Microsoft Azure and Amazon Web Services:

- The Standalone Sentry ISO file for installing on Microsoft Azure is available at <https://support.mobileiron.com/mi/sentry/9.20.0-18/sentry-mobileiron-9.20.0-18.vhd>
  - Json files needed for installation:  
<https://support.mobileiron.com/mi/sentry/9.20.0-18/SentryAzureDeploy.parameters.json>
  - <https://support.mobileiron.com/mi/sentry/9.20.0-18/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 following owner ID for various regions:



Region	Owner ID
us-east-1	ami-00054c272b6f25cc6
us-east-2	ami-05b72ccee7f1a788e
us-west-1	ami-0d6584790dfbed2a6
us-west-2	ami-0a7d88e7c1906eece
ap-south-1	ami-01a35995936bf0038
ap-southeast-1	ami-0c0c09537b6b4c165
ap-southeast-2	ami-04b3b7368d85f167d
ap-northeast-1	ami-0492c16df040edf64
ap-northeast-2	ami-0efca53f682f6bba8
ca-central-1	ami-0bfe673c0d1d99608
eu-central-1	ami-047ff50e5903eaac9
eu-west-1	ami-0430c8b84df71f078
eu-west-2	ami-0c036171ef342f47f
eu-west-3	ami-06e3f54c92552b248
eu-north-1	ami-04e1142b67e308174
sa-east-1	ami-06a84d32320639784

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

# Upgrade information

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

- ["Before you upgrade Ivanti Standalone Sentry" below](#)
- ["Supported upgrade paths for Ivanti Standalone Sentry " on the next page](#)
- ["Upgrade URL for CLI upgrades for Ivanti Standalone Sentry" on the next page](#)
- ["TLS compliance utility" on the next page](#)
- ["Upgrade notes for Standalone Sentry" on page 20](#)
- ["Upgrade steps for Ivanti Standalone Sentry" on page 21](#)

## Before you upgrade Ivanti Standalone Sentry

- Ensure that the Ivanti Standalone Sentry System Manager (MICS) portal certificate has not expired. 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 installation, allow for a rolling upgrade to minimize downtime. Do not upgrade all Sentry instances at the same time.
- Ensure that Ivanti EPMM 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" on page 5](#) 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 upgrade paths for Ivanti Standalone Sentry

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

**TABLE 7.** SUPPORTED PATHS FOR SENTRY AND AWS UPGRADE

Current Ivanti Standalone Sentry version	Upgrade path to 9.20.0
9.18.0	9.18.0 > 9.20.0
9.18.1	9.18.1 > 9.20.0
9.19.0	9.19.0 > 9.20.0
9.19.1	9.19.1 > 9.20.0

 We recommend you upgrade to the latest Sentry version.


## Upgrade URL for CLI upgrades for Ivanti Standalone Sentry


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

<https://support.mobileiron.com/mi/sentry/9.20.0/>

## 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.

 **TLS 1.1 and TLS 1.0 support:** TLS 1.1 and TLS 1.0 is not supported with Sentry 9.16.0 and later versions. For more information, see [KB article](#).

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 TLS compliance. See "Using CLI command to check TLS compliance" in the *Sentry Guide*.

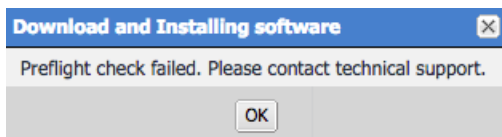
## Upgrade notes for Standalone Sentry

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 3.x, 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.



SMB 3.x is enabled by default after upgrading to 9.17.0

---

**Workaround:** Ivanti recommends updating the file server to SMB 3.x, 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 Ivanti Standalone Sentry

If you are upgrading from a version not listed in "[Supported upgrade paths for Ivanti Standalone Sentry](#)" on [page 19](#), then you need to complete one or more previous upgrades first. See the release notes for the version to which you will upgrade.

## Upgrade steps for Ivanti Standalone Sentry

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

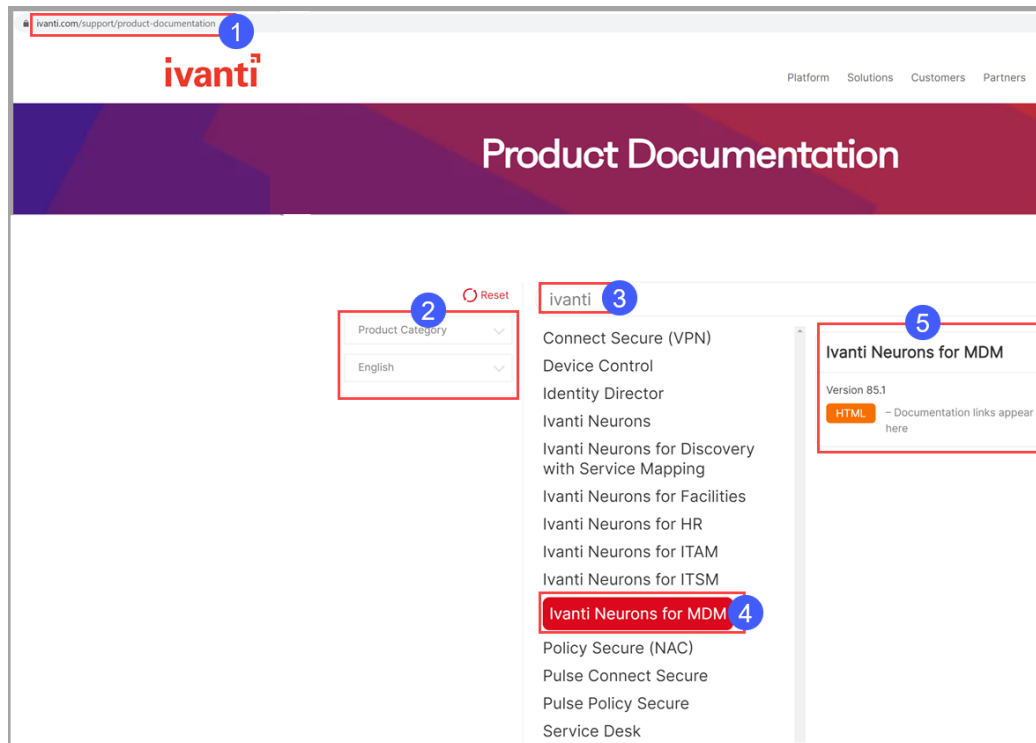
- For upgrade instructions using the Ivanti Standalone Sentry System Manager UI, see "[Standalone Sentry software updates](#)."
- For upgrade instructions using the Ivanti Standalone Sentry command line interface (CLI), see "[Upgrading using CLI](#)."
- For multiple Sentry upgrade instructions using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

# Documentation resources

Product documentation is available on the [Ivanti website](#). You can jump directly to Access at [this link](#).

To use the documentation:

1. Navigate to the [Ivanti documentation website](#). For example:



2. Optionally, select a product category and language.
3. Enter a search term.
4. Select a product from the results.
5. Click the associated documentation links.



If you have an Ivanti Neurons for MDM deployment, the Ivanti Neurons for MDM Guide is also available from your instance of Ivanti Neurons for MDM through the Help link in the user interface. See [Accessing online help](#).

# Sentry documentation

The following is a list of the documentation:

- [\*Ivanti Standalone Sentry Release Notes\*](#)

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

- [\*Ivanti Sentry Installation Guide\*](#)

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

- [\*Ivanti Sentry Guide for Ivanti Neurons for MDM\*](#)

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

- [\*Ivanti Standalone Sentry Guide for EPMM\*](#)

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