Tenable and Ivanti MDM Integration Guide

Last Revised: October 23, 2025

Table of Contents

Welcome to the Ivanti Mobile Device Management Integration

This document provides information and steps for integrating Tenable Vulnerability Management or Tenable Nessus Manager with the Ivanti Mobile Device Management (MDM).

For more information, refer to the following product documentation pages:

- Tenable Vulnerability Management
- Tenable Nessus

Tenable Vulnerability Management for Ivanti MDM

Ivanti is a mobile device management platform that secures, manages, and supports the full lifecycle of mobile devices across an enterprise, prioritizing security and productivity. Ivanti also provides MDM solutions to manage and secure mobile devices, ensuring they comply with organizational policies.

Tenable primarily supports two main products: Ivanti Endpoint Manager Mobile (formerly MobileIron Core) and Ivanti Neurons (formerly MobileIron Cloud).

Tenable offers integration capabilities with Ivanti, enabling the utilization of scan data and the execution of patch audits on systems for which direct credential access may be limited. This leads to enhanced device management and a clearer understanding of cyber exposure.

What information does the Ivanti integration collect?

The Ivanti integration primarily collects information that focuses on device status, configuration and security posture.

Here is a high level overview of some key categories of the information collected:

- Device and user identity Data: Device ID, MAC address, IMEI, logged-in username, user group/role
- Hardware and Operating System Data: Manufacturer, model name, OS version, patch level, build number
- App config settings: App settings, App Type, Device Count
- Policy Metadata: Policy Name & ID, Policy Type, Compliance Actions, Policy Rules

What the Ivanti integration does not collect

- Information regarding users who are not currently logged in
- A full list of apps installed

Configure Ivanti MDM Integration

Ivanti vulnerability scans can be configured within the “Mobile Device Scan” category within Tenable Vulnerability Management. Here are the step-by-step instructions for configuring a scan.

To configure Ivanti MDM integration:

1. Log in to your Tenable user interface.
2. In the upper-left corner, click the **Menu** button.

   The left navigation plane appears.
3. In the left navigation plane, click **Scans**.

   The **Scans** page appears.
4. In the upper-right corner of the page, click the **Create a Scan** button.

   The **Select a Scan Template** page appears.
5. Select the Mobile Device scan template.

   The **scan configuration** page appears.
6. In the **Name** box, type a name for the scan.
7. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
8. (Optional) Add a description, folder location, scanner location, and specify target groups.

   The credentials options appear.
9. Click the **Credentials** tab.

   The **Credentials** pane appears.
10. In the **Select a Credential** menu, select **Ivanti**.

11. Configure each option.

Option	Description	Default Value	Required
VSP Admin Portal URL	The server URL Tenable uses to authenticate to the Ivanti administrator portal.	-	yes
VSP Admin Portal Port	The port Tenable uses to authenticate to the Ivanti administrator portal.	443	no
Port	The port Tenable uses to authenticate to Ivanti.	443	yes
Username	The username for the account you want Tenable to use to authenticate to Ivanti.	-	yes
Password	The password for the account you want Tenable to use to authenticate to Ivanti.	-	yes
HTTPS	When enabled, Tenable uses an encrypted connection to authenticate to Ivanti.	Enabled	no
Verify SSL Certificate	When enabled, Tenable verifies that the SSL Certificate on the server is signed by a trusted CA.	Enabled	no

12. Click **Save**.

Ivanti and VM Scan Results Review

This section contains help for you to interpret the results of your scans.

Plugin Families and Plugins

The following plugins are useful for verifying whether a scan within the integration was successful:

- Integration Status
    - Plugin ID 204872
    - This plugin provides the integration Status Report and number of devices found.
- MDM Mobile Device Reporting
    - Plugin ID 60035
    - This plugin gathers the information provided from mobile device management systems around the network and reports the devices, information, and where they are managed.
- Debugging Log Report
    - Plugin ID 84239
    - Logs generated by other plugins are reported by this plugin.

Debug Log Reporting

The debugging log, identified by plugin ID 84239, is located within the vulnerabilities section subsequent to a scan's completion. It comprises log files generated by various other plugins. For this plugin to execute, debugging must be enabled within the policy. The ivanti_collect.log is particularly valuable for diagnosing potential issues pertaining to the Ivanti integration.

Tenable Nessus for Ivanti MDM

Ivanti is a mobile device management platform that secures, manages, and supports the full lifecycle of mobile devices across an enterprise, prioritizing security and productivity. Ivanti also provides MDM solutions to manage and secure mobile devices, ensuring they comply with organizational policies.

Tenable primarily supports two main products: Ivanti Endpoint Manager Mobile (formerly MobileIron Core) and Ivanti Neurons (formerly MobileIron Cloud).

Tenable offers integration capabilities with Ivanti, enabling the utilization of scan data and the execution of patch audits on systems for which direct credential access may be limited. This leads to enhanced device management and a clearer understanding of cyber exposure.

What information does the Ivanti integration collect?

The Ivanti integration primarily collects information that focuses on device status, configuration and security posture.

Here is a high level overview of some key categories of the information collected:

- Device and user identity Data: Device ID, MAC address, IMEI, logged-in username, user group/role
- Hardware and Operating System Data: Manufacturer, model name, OS version, patch level, build number
- App config settings: App settings, App Type, Device Count
- Policy Metadata: Policy Name & ID, Policy Type, Compliance Actions, Policy Rules

What the Ivanti integration does not collect

- Information regarding users who are not currently logged in
- A full list of apps installed

Configure Ivanti MDM Integration

Ivanti vulnerability scans can be configured within the “Mobile Device Scan” category within Tenable Nessus. Here are the step-by-step instructions for configuring a scan.

To configure Ivanti MDM integration:

1. Log in to your Tenable user interface.
2. In the upper-left corner, click the **Menu** button.

   The left navigation plane appears.
3. In the left navigation plane, click **Scans**.

   The **Scans** page appears.
4. In the upper-right corner of the page, click the **Create a Scan** button.

   The **Select a Scan Template** page appears.
5. Select the Mobile Device scan template.

   The **scan configuration** page appears.
6. In the **Name** box, type a name for the scan.
7. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
8. (Optional) Add a description, folder location, scanner location, and specify target groups.

   The credentials options appear.
9. Click the **Credentials** tab.

   The **Credentials** pane appears.
10. In the **Select a Credential** menu, select **Ivanti**.

11. Configure each option.

Option	Description	Default Value	Required
VSP Admin Portal URL	The server URL Tenable uses to authenticate to the Ivanti administrator portal.	-	yes
VSP Admin Portal Port	The port Tenable uses to authenticate to the Ivanti administrator portal.	443	no
Port	The port Tenable uses to authenticate to Ivanti.	443	yes
Username	The username for the account you want Tenable to use to authenticate to Ivanti.	-	yes
Password	The password for the account you want Tenable to use to authenticate to Ivanti.	-	yes
HTTPS	When enabled, Tenable uses an encrypted connection to authenticate to Ivanti.	Enabled	no
Verify SSL Certificate	When enabled, Tenable verifies that the SSL Certificate on the server is signed by a trusted CA.	Enabled	no

12. Click **Save**.

Ivanti and Nessus Scan Results Review

This section contains help for you to interpret the results of your scans.

Plugin Families and Plugins

The following plugins are useful for verifying whether a scan within the integration was successful:

- Integration Status
    - Plugin ID 204872
    - This plugin provides the integration Status Report and number of devices found.
- MDM Mobile Device Reporting
    - Plugin ID 60035
    - This plugin gathers the information provided from mobile device management systems around the network and reports the devices, information, and where they are managed.
- Debugging Log Report
    - Plugin ID 84239
    - Logs generated by other plugins are reported by this plugin.

Debug Log Reporting

The debugging log, identified by plugin ID 84239, is located within the vulnerabilities section subsequent to a scan's completion. It comprises log files generated by various other plugins. For this plugin to execute, debugging must be enabled within the policy. The `ivanti_collect.log` is particularly valuable for diagnosing potential issues pertaining to the Ivanti integration.