Integrate UEM and MDM Servers With Cisco ISE

- Overview of Unified Endpoint Management in Cisco ISE, on page 1
- MAC Address for VPN-Connected Endpoints, on page 3
- Additional references, on page 3
- Communications, services, and additional information, on page 3

Overview of Unified Endpoint Management in Cisco ISE

If you use Unified Endpoint Management (UEM) or Mobile Device Management (MDM) servers to secure, monitor, manage, and support the endpoints that are deployed in your network, you can configure Cisco ISE to interoperate with these servers. Integrate your Cisco ISE and your endpoint management servers to access device attribute information from these servers through APIs. You can then use the device attributes to create Access Control Lists (ACLs) and authorization policies to enable network access control.

Cisco ISE PSNs also send APIs to fetch lists of noncompliant devices from connected UEM or MDM servers at set polling intervals. Any noncompliant endpoints with active sessions at the time of polling are quarantined and CoAs are issued in Cisco ISE based on the fetched information.

This document details the configurations that you must perform in your endpoint management servers to integrate these servers with Cisco ISE. This document currently details the required configurations for the following MDM or UEM vendors:

- Cisco Meraki Systems Manager
- Ivanti (previously MobileIron UEM) core and cloud UEM services
- Microsoft Endpoint Manager Intune

Cisco ISE also supports the following endpoint management servers:

- 42Gears
- Absolute
- Blackberry - BES
- Blackberry - Good Secure EMM
- Citrix XenMobile 10.x (On-prem)
- Globo

- IBM MaaS360
- JAMF Casper Suite
- Microsoft Endpoint Configuration Manager
- Mosyle
- SAP Afaria
- Sophos
- SOTI MobiControl
- Symantec
- Tangoe
- Omnissa (previously AirWatch)

Note Cisco ISE 3.0 or earlier releases cannot be integrated with Jamf Pro 10.42.0 or later.

After you carry out the necessary configurations in the MDM or UEM servers that you want to connect to Cisco ISE, you must join the servers to your Cisco ISE. See "Configure Mobile Device Management Servers in Cisco ISE" in the Chapter "Secure Access" in the *Cisco ISE Administrator Guide* for your release.

Cisco ISE MDM API Version 3 for GUID

Cisco ISE Release 3.1 introduces the capability to handle random and changing MAC addresses of endpoints. You can use Cisco ISE MDM API Version 3 to receive a unique endpoint identifier that is named GUID from the connected MDM and UEM servers. Then, Cisco ISE uses the GUID to identify an endpoint instead of its MAC address. See "Handle Random and Changing MAC Addresses With Mobile Device Management Servers" in the Chapter "Secure Access" in the *Cisco ISE Administrator Guide* for your release.

To receive GUID from a UEM or MDM server, the following conditions must be met:

- The UEM or MDM server supports Cisco ISE MDM API Version 3.
- In the UEM or MDM, the certificates for Cisco ISE usage are configured so that the Subject Alternative Name field, or the Common Name field, or both, push the GUID to Cisco ISE.

The following UEM or MDM servers currently support Cisco ISE MDM API Version 3:

- Cisco Meraki Systems Manager
- Ivanti (previously MobileIron UEM) core and cloud UEM services
- Microsoft Endpoint Manager Intune
- JAMF Casper Suite
- Omnissa (previously AirWatch)

Note For information on Omnissa configuration, see Omnissa Product Documentation.

MAC Address for VPN-Connected Endpoints

Cisco ISE uses the MAC addresses of endpoints to save and manage endpoint data in its databases, display context visibility information, and enable authorization workflows.

In case of VPN-connected endpoints, the VPN headend typically receives an endpoint's MAC address or Unique Device Identifier (UDID), or both, from Cisco Secure Client (formerly known as Cisco AnyConnect) and then sends the information to Cisco ISE over RADIUS communication.

When you integrate Cisco ISE with an MDM server, Cisco ISE uses either the MAC address or the UDID of an endpoint to query the MDM server for the endpoint's registration and compliance statuses, and other MDM attribute values.

If Cisco ISE queries an MDM server using an endpoint's UDID, the compliance response from the MDM server usually includes the endpoint's MAC address. Receiving an endpoint's MAC address from either the Cisco Secure Client or the MDM server is critical for Cisco ISE. Cisco ISE uses the MAC address to save and manage the endpoint data in its databases.

Additional references

See Cisco ISE End-User Resources for additional resources that you can use when working with Cisco ISE.

Communications, services, and additional information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.