Integrate UEM and MDM Servers with Cisco ISE

Unified endpoint management in Cisco ISE

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

Cisco ISE PSNs also use APIs to fetch lists of noncompliant devices from connected UEM or MDM servers at set polling intervals. Cisco ISE quarantines any noncompliant endpoints with active sessions at the time of polling and issues CoAs based on the fetched information.

You can configure your endpoint management servers to integrate them with Cisco ISE. Use the required configurations for your MDM or UEM vendor, such as

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

Cisco ISE also supports these endpoint management servers:

- 42Gears
- Absolute
- Blackberry - BES
- Blackberry - Good Secure EMM
- Citrix XenMobile 10.x (On-prem)
- Globo
- IBM MaaS360

- Jamf Casper Suite
- Jamf Pro 10.42.0 or later
- Microsoft Endpoint Configuration Manager
- Mosyle
- SAP Afaria
- Sophos
- SOTI MobiControl
- Symantec
- Tangoe
- Omnissa (previously AirWatch)

After you configure the MDM or UEM servers to connect to Cisco ISE, join these servers to your Cisco ISE deployment. 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

From Cisco ISE release 3.1, you can handle random and changing MAC addresses of endpoints. You can use Cisco ISE MDM API version 3 to receive a unique endpoint identifier, called GUID, from connected MDM and UEM servers. Cisco ISE then 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, these conditions must be met:

- The UEM or MDM server supports Cisco ISE MDM API version 3.
- Configure the certificates for Cisco ISE usage in your UEM or MDM so that the **Subject Alternative Name** field, the **Common Name** field, or both, push the GUID to Cisco ISE.

These 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)

For information on Omnissa configuration, refer to Omnissa Product Documentation.

MAC address for VPN-connected endpoints

Cisco ISE uses endpoint MAC addresses to save and manage data, display context visibility information, and enable authorization workflows.

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

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

When Cisco ISE queries an MDM server with endpoint's UDID, the MDM server usually responds with 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

Refer to Cisco ISE collection pages 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.