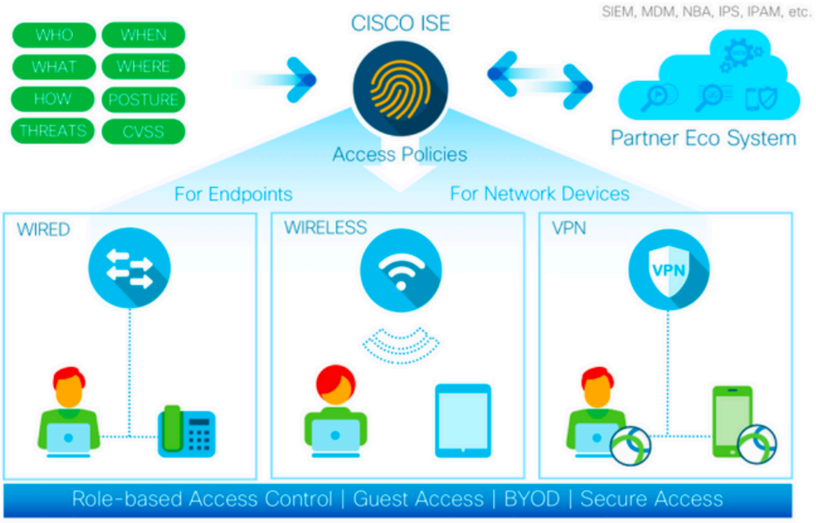
**Jay Tiwari, Security Consulting Engineer**
**Cisco Systems, Inc.**

## Table of Contents

## Introduction

Cisco ISE is a leading, identity-based network access control and policy enforcement system. It is a common policy engine for controlling, endpoint access and network device administration for enterprises. ISE allows an administrator to centrally control access policies for wired, wireless, and VPN endpoints in a network.

***Figure 1: Cisco Identity Services Engine***



ISE builds context about the endpoints that include users and groups (Who), device type (What), access time (When), access location (Where), access type (Wired/Wireless/VPN) (How), threats, and vulnerabilities. By sharing vital contextual data with technology partner integrations and the implementation of the Cisco TrustSec® policy for software-defined segmentation, ISE transforms a network from a conduit for data into a security enforcer that accelerates the time-to-detection and time-to-resolution of network threats.

## About This Document

This document provides technical guidance to design, deploy and operate Cisco Identity Services Engine (ISE) with JAMF MDM Server. This document focuses on integration of ISE with JAMF server so that ISE can retrieve compliance information from JAMF server and leverage the information to control network access to the user's APPLE device.

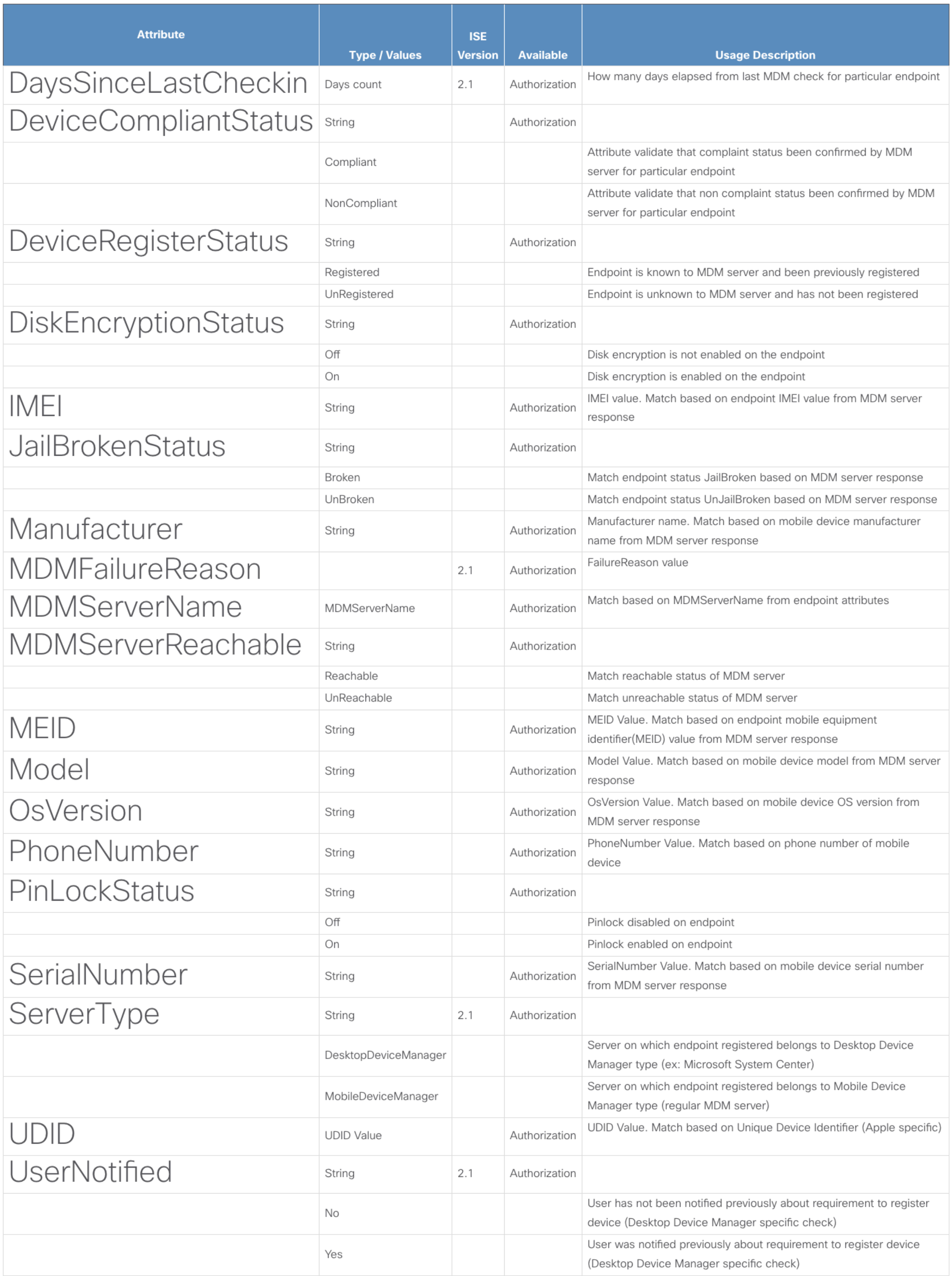
The first half of the document focuses on the planning and design activities, the other half covers specifics of configurations and operations. There are three major sections in this document. The initial, define part talks about defining the problem area, planning for deployment, and other considerations. Next, in the design section, you will see how to configure JAMF server to communicate with Cisco ISE to make policy decision based on the compliance information. Lastly, in the operate section, you will learn how troubleshoot and monitor.

## Definition

ISE supports JAMF as a partner MDM server for managing Windows computers. JAMF server allows users to manage a large number of APPLE computers. With JAMF, IT Technicians proactively manage the entire lifecycle of all Apple devices. This includes deploying and maintaining software, responding to security threats, distributing settings, and analysing inventory data.

# Use Cases of ISE with JAMF

After you add the MDM server definition in Cisco ISE, the MDM dictionary attributes are available in Cisco ISE that you can use in authorization policies. You can view the dictionary attributes that are available for use in authorization policies.

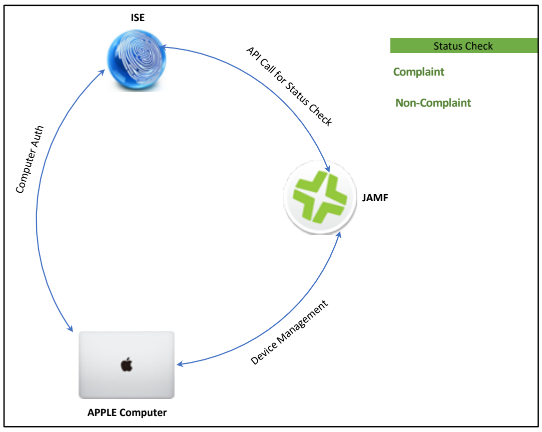


| Attribute | Type / Values | ISE Version | Available | Usage Description |
|---|---|---|---|---|
| DaysSinceLastCheckin | Days count | 2.1 | Authorization | How many days elapsed from last MDM check for particular endpoint |
| DeviceCompliantStatus | String | | Authorization | |
| | Compliant | | | Attribute validate that complaint status been confirmed by MDM server for particular endpoint |
| | NonCompliant | | | Attribute validate that non complaint status been confirmed by MDM server for particular endpoint |
| DeviceRegisterStatus | String | | Authorization | |
| | Registered | | | Endpoint is known to MDM server and been previously registered |
| | UnRegistered | | | Endpoint is unknown to MDM server and has not been registered |
| DiskEncryptionStatus | String | | Authorization | |
| | Off | | | Disk encryption is not enabled on the endpoint |
| | On | | | Disk encryption is enabled on the endpoint |
| IMEI | String | | Authorization | IMEI value. Match based on endpoint IMEI value from MDM server response |
| JailBrokenStatus | String | | Authorization | |
| | Broken | | | Match endpoint status JailBroken based on MDM server response |
| | UnBroken | | | Match endpoint status UnJailBroken based on MDM server response |
| Manufacturer | String | | Authorization | Manufacturer name. Match based on mobile device manufacturer name from MDM server response |
| MDMFailureReason | | 2.1 | Authorization | FailureReason value |
| MDMServerName | MDMServerName | | Authorization | Match based on MDMServerName from endpoint attributes |
| MDMServerReachable | String | | Authorization | |
| | Reachable | | | Match reachable status of MDM server |
| | UnReachable | | | Match unreachable status of MDM server |
| MEID | String | | Authorization | MEID Value. Match based on endpoint mobile equipment identifier(MEID) value from MDM server response |
| Model | String | | Authorization | Model Value. Match based on mobile device model from MDM server response |
| OsVersion | String | | Authorization | OsVersion Value. Match based on mobile device OS version from MDM server response |
| PhoneNumber | String | | Authorization | PhoneNumber Value. Match based on phone number of mobile device |
| PinLockStatus | String | | Authorization | |
| | Off | | | Pinlock disabled on endpoint |
| | On | | | Pinlock enabled on endpoint |
| SerialNumber | String | | Authorization | SerialNumber Value. Match based on mobile device serial number from MDM server response |
| ServerType | String | 2.1 | Authorization | |
| | DesktopDeviceManager | | | Server on which endpoint registered belongs to Desktop Device Manager type (ex: Microsoft System Center) |
| | MobileDeviceManager | | | Server on which endpoint registered belongs to Mobile Device Manager type (regular MDM server) |
| UDID | UDID Value | | Authorization | UDID Value. Match based on Unique Device Identifier (Apple specific) |
| UserNotified | String | 2.1 | Authorization | |
| | No | | | User has not been notified previously about requirement to register device (Desktop Device Manager specific check) |
| | Yes | | | User was notified previously about requirement to register device (Desktop Device Manager specific check) |

In this document following use case is considered:
During authorisation process ISE is checking JAMF server for APPLE computer compliance status;

1. if computer is complaint give required access
2. If non-complaint redirect computer to JAMF MDM server for remediation.

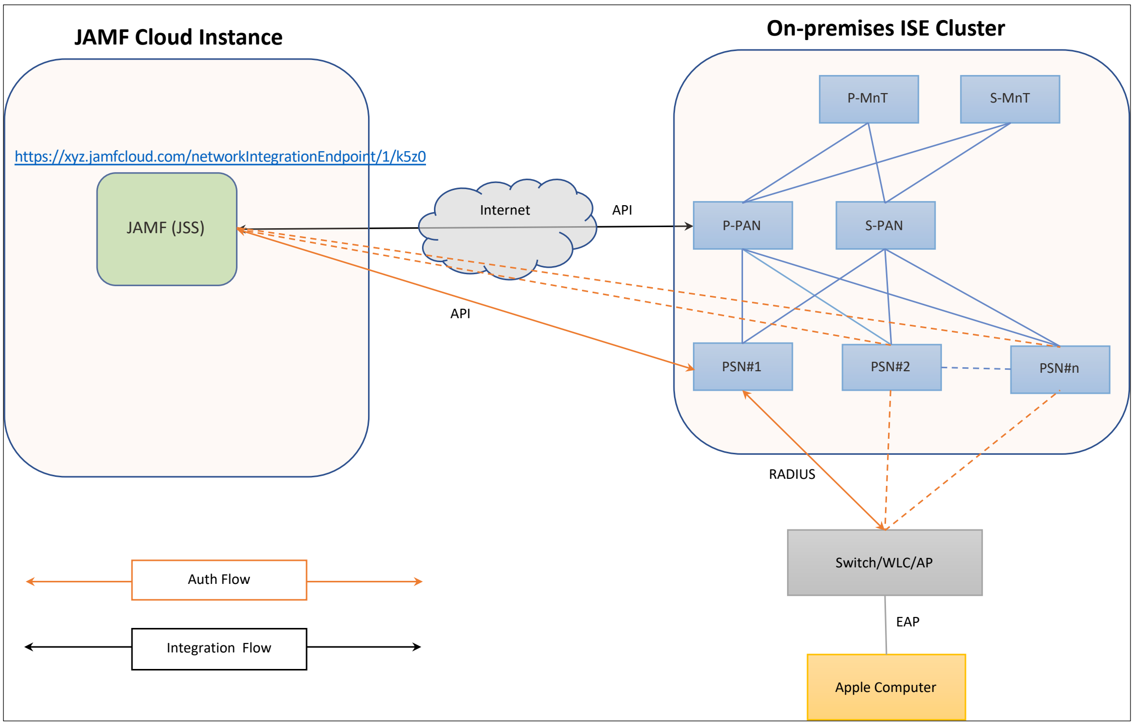
*Figure 2: MDM Flow with ISE*



# Deploy

## Deployment Architecture

*Figure 3: ISE & JAMF Integration & Flow*



As shown in figure JAMF is cloud instance and ISE cluster is in on-premises. ISE cluster integration with JAMF happens with ISE PAN and after successful integration, during authentication/authorisation, PSN directly reaches to JAMF to check MDM attribute/s status for authorisation policy enforcement.

**Note:** Make sure that firewall port is opened and API communication is allowed between ISE cluster ( PAN & PSN) and JAMF cloud instance.

## JAMF Configuration

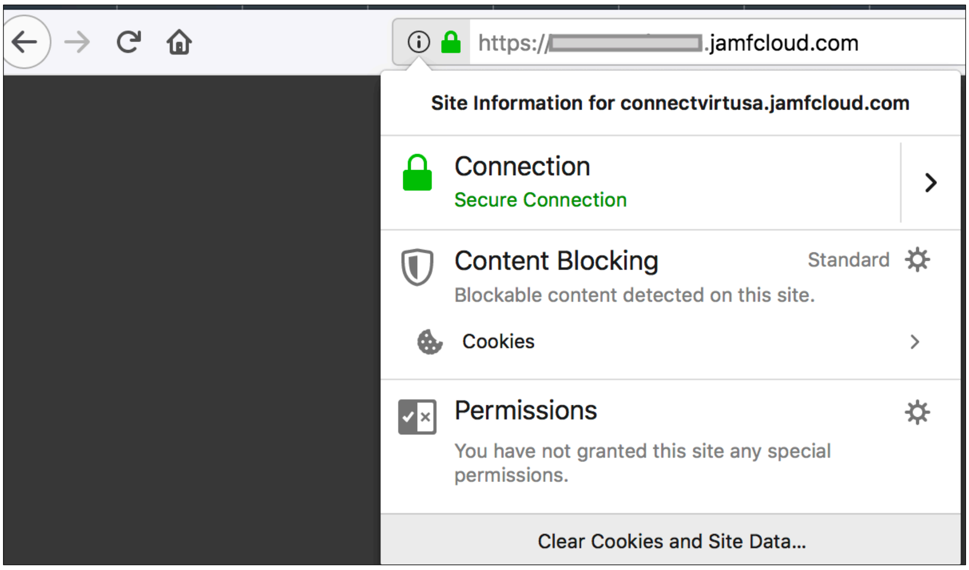
In order to integrate JAMF to ISE, first of all configure JAMF/JSS to create integration URL or Instance ID. For configuration, following steps are required:

- Log in to the JSS with a web browser.
- In the top-right corner of the page, click Settings.
- Click Network Organization.
- Click Network Integration.
- Click New. Note: Only one network integration instance can be added per site in the JSS.
- Configure the network integration instance using the settings on the pane, including the site, the advanced computer search and advanced mobile device search to be used for compliance verification, compliance messaging to be displayed to users, and the remote lock and wipe passcode setting for computers. Note: If you select the “Create Random Passcode” option for the passcode assignment method for computers, to identify the passcode used for a remote lock or wipe on a specific computer, you will need to view the management history for the computer in the JSS.
- Click Save.
- After saving the network integration instance, a unique network integration URL appears at the bottom of the pane. This URL will be used by the network access management service to communicate with the specific JSS network integration instance. In this context, URL generated for ISE integration is **https://xyz.jamfcloud.com/networkIntegrationEndpoint/1/k5z0** where xyz.jamfcloud.com is FQDN of JAMF instance and networkIntegrationEndpoint/1/k5z0 is instance name.

## Certificate Export from JAMF

If https connection is required to integrate JAMF to ISE, export JAMF certificate. In order to export JAMF certificate go to web browser and open JAMF URL, as shown in figure below (Firefox is used in sample figure):

***Figure 4:Expoort JAMF Certificate***



https://[redacted].jamfcloud.com

Site Information for connectvirtusa.jamfcloud.com

Connection

Secure Connection

Content Blocking — Standard

Blockable content detected on this site.

Cookies

Permissions

You have not granted this site any special permissions.

Clear Cookies and Site Data...

Now click on “Connection” → “More Information”→ “View Certificate”→ “Details” and export certificate to local machine where bowser is opened.

## Certificate Import to ISE Trusted Store

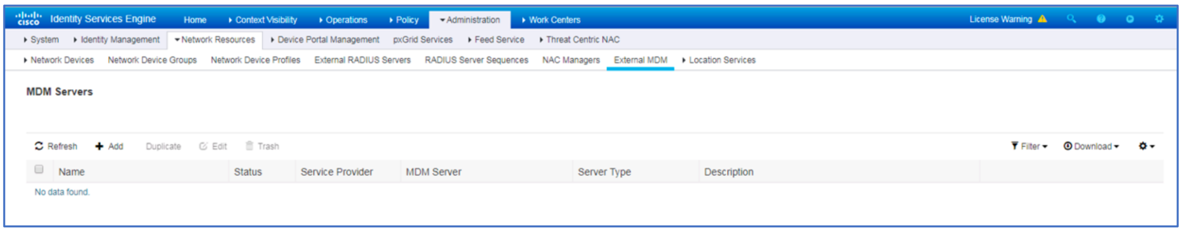
In order to complete the https integration with JAMF, JAMF certificate must be in ISE Certificate Trusted Store. To import certificate to ISE Certificate Trusted Store go to ISE Admin GUI and navigate to Administration → System → Certificates → Trusted Certificates and import JAMF certificate.

## ISE Configuration for JAMF Integration

Now, configure ISE to connect to the JAMF server, test the connection, and add the JAMF server as an available MDM server in the ISE system.

1. Login to the ISE Primary Admin node web interface
2. Select **Administration -> Network Resources -> External MDM**

***Figure 5: JAMF Instance Creation***



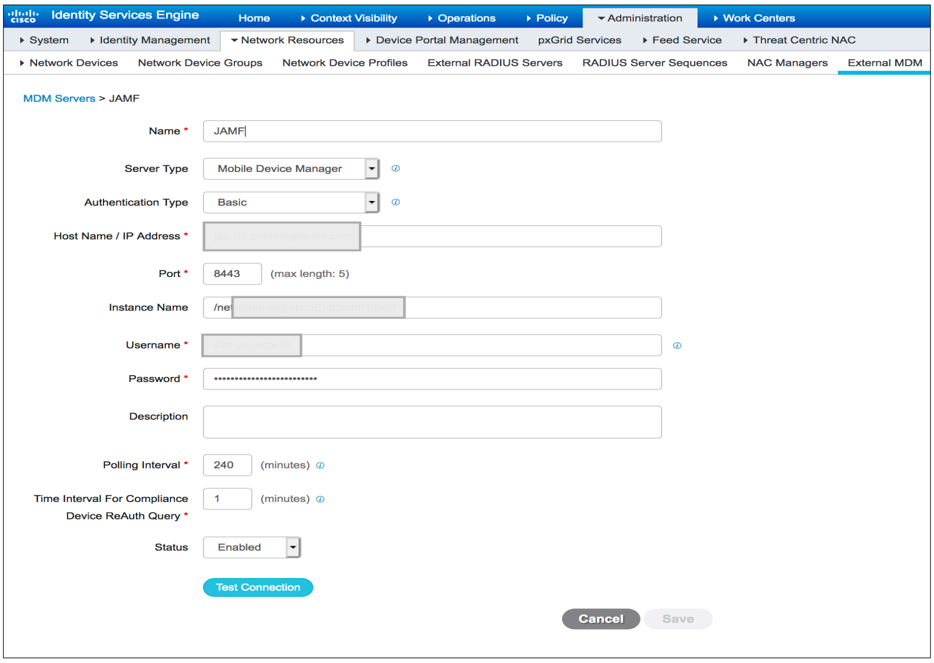
MDM Servers

| Name | Status | Service Provider | MDM Server | Server Type | Description |
|---|---|---|---|---|---|

No data found.

3. Click on the “Add” button to add a new MDM server.

***Figure 6: JAMF Instance Integration Configuration***



MDM Servers > JAMF

Name * JAMF

Server Type Mobile Device Manager

Authentication Type Basic

Host Name / IP Address * [redacted]

Port * 8443 (max length: 5)

Instance Name /ne[redacted]

Username * [redacted]

Password * ••••••••••••••••••••••••

Description

Polling Interval * 240 (minutes)

Time Interval For Compliance Device ReAuth Query * 1 (minutes)

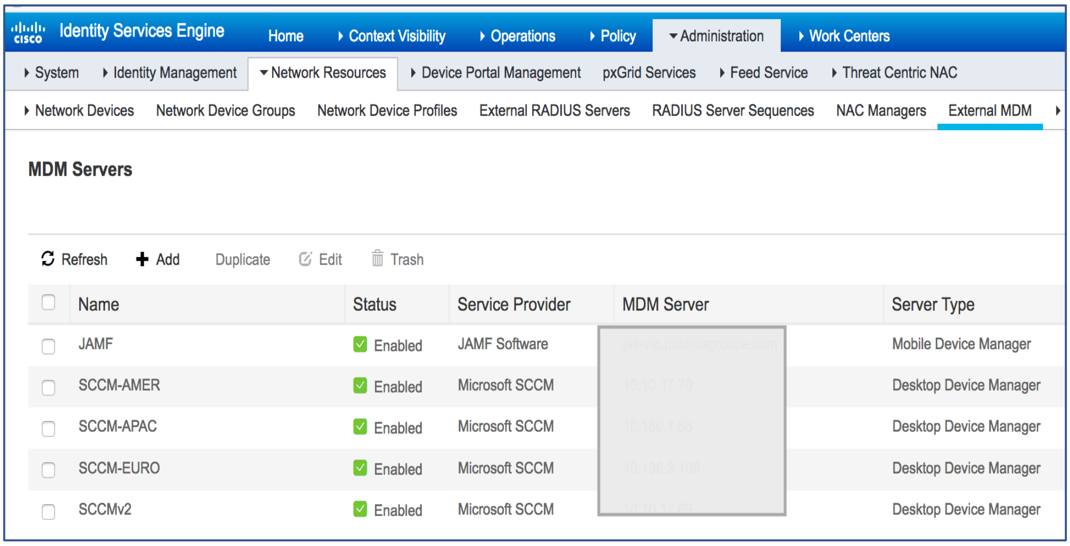
Status Enabled

4. The “Name” field can be any name you want to reference the MDM as when creating policies within ISE. The name cannot contain. any spaces. In this example, we are using “JAMF”.
5. The “Server Type” must be set to “Mobile Device Manager” for JAMF.
6. Enter the Fully Qualified Domain Name (FQDN) of the JAMF server or the IP address that is reachable from the ISE Admin node. JAMF server FQDN is: **xyz.jamfcloud.com**
7. Port is TCP port number on which JAMF server is listening. In this document, JAMF instance is listening on TCP **443**

8. For the “Site or Instance Name”, please use the JAMF Site Name. JAMF instance name is: **networkIntegrationEndpoint/1/k5z0**
9. The username will be the user account that was created for JAMF in order to integrate ISE. iseadmin service account is created to integrate ISE with JAMF.
10. Enter the password for the service account.
11. Select the “Test Connection” button at the bottom to test the connection to the JAMF server. If the connection is successful, you should see a dialog box stating it was successful
12. Click the “OK” button on the success dialog.
13. Change the “Status” to “Enabled”.
14. Click “Submit” to add the new JAMF server to ISE as an MDM.
15. Verify that you can see the JAMF server added to the MDM servers Page.

Many MDM instances can be integrated into ISE. After integration JAMF MDM server page will look like below figure:

*Figure 7: ISE MDM Server Page*



MDM Servers

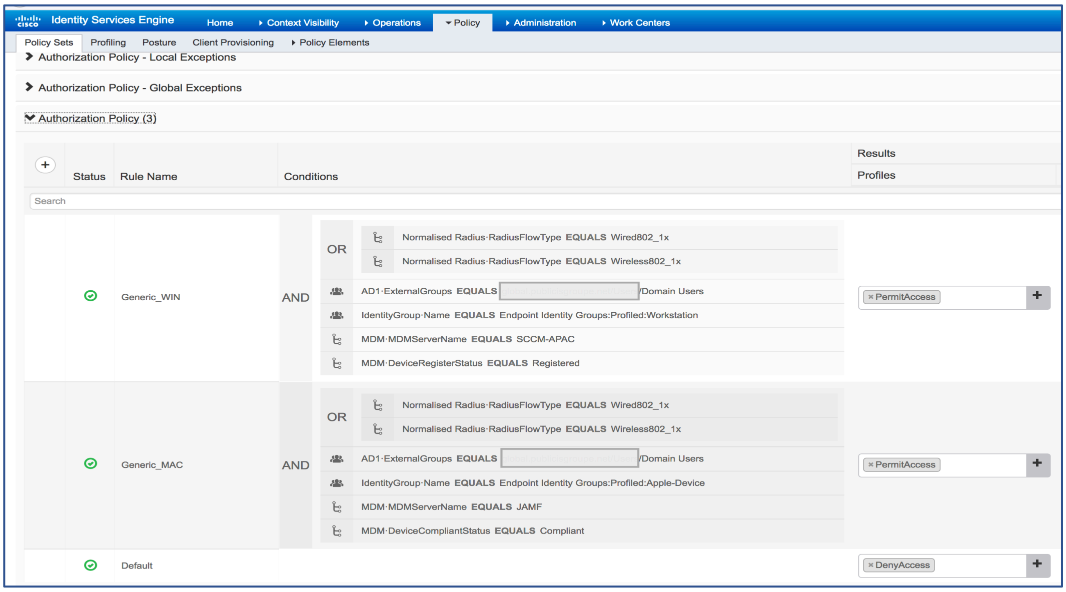
| □ | Name | Status | Service Provider | MDM Server | Server Type |
|---|---|---|---|---|---|
| □ | JAMF | ☑ Enabled | JAMF Software | [redacted] | Mobile Device Manager |
| □ | SCCM-AMER | ☑ Enabled | Microsoft SCCM | [redacted] | Desktop Device Manager |
| □ | SCCM-APAC | ☑ Enabled | Microsoft SCCM | [redacted] | Desktop Device Manager |
| □ | SCCM-EURO | ☑ Enabled | Microsoft SCCM | [redacted] | Desktop Device Manager |
| □ | SCCMv2 | ☑ Enabled | Microsoft SCCM | [redacted] | Desktop Device Manager |

## Authorisation Policy Configuration

Now MDM integration instance can be called in authorization policy as condition to define required access to APPLE computer.

In order to create authorisation policy with complaint status check with JAMF MDM server, navigate to Policy → Policy Set → “Policy_Set_Name” → Authorization Policy and create a policy with MDM complaint and non-complaint attribute.

*Figure 8:Authorization Policy with MDM Attribute*



Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (3)

| Status | Rule Name | Conditions | Results<br>Profiles |
|---|---|---|---|
| ✓ | Generic_WIN | AND<br>OR: Normalised Radius·RadiusFlowType EQUALS Wired802_1x<br>Normalised Radius·RadiusFlowType EQUALS Wireless802_1x<br>AD1·ExternalGroups EQUALS /Domain Users<br>IdentityGroup·Name EQUALS Endpoint Identity Groups:Profiled:Workstation<br>MDM·MDMServerName EQUALS SCCM-APAC<br>MDM·DeviceRegisterStatus EQUALS Registered | PermitAccess |
| ✓ | Generic_MAC | AND<br>OR: Normalised Radius·RadiusFlowType EQUALS Wired802_1x<br>Normalised Radius·RadiusFlowType EQUALS Wireless802_1x<br>AD1·ExternalGroups EQUALS /Domain Users<br>IdentityGroup·Name EQUALS Endpoint Identity Groups:Profiled:Apple-Device<br>MDM·MDMServerName EQUALS JAMF<br>MDM·DeviceCompliantStatus EQUALS Compliant | PermitAccess |
| ✓ | Default | | DenyAccess |

Similar way authorisation policy for non-complaint APPLE computer can be created where computer will be redirected to MDM page for remediation.

## Testing

Bring a two APPLE computer, one which is complaint and one which is non-complaint and test network authentication and access control. Complaint computer should be getting required access however non-complaint computer should be redirected to MDM server.

## Troubleshooting

Common issues during MDM integration are:

1. Connectivity issue between PAN & MDM Server
2. Connectivity issue between PSN & MDM Server
3. Permission issue in MDM Server

In order to troubleshoot, follow steps below:

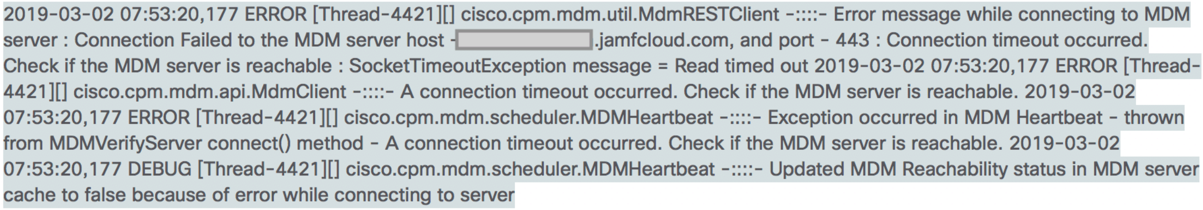
**Step-1:** Enable packet capture. In order to enable packet capture in ISE, navigate to Operations → Troubleshoot → Diagnostic Tools → TCP Dump and create capture. Once capture is taken, download it and analyse the log.

**Step-2:** To get visibility into communication between ISE and MDM server, enable TRACE in ISE. Logging level can be changed by navigating to Administration > System > Logging > Debug Log Configuration. To download log go to Operations → Troubleshoot → Download Logs.

During the node selection, choose Primary PAN node if you need to troubleshoot initial connection. When issues are seen with actual authentications, logging level needs to be changed on the PSN where endpoints are authenticated.

External-MDM component writes logs into the ise-psc.log, all logs related to the MDM operation can be easily filtered by the 'cpm.mdm'.

Example log taken from PSN:



```
2019-03-02 07:53:20,177 ERROR [Thread-4421][] cisco.cpm.mdm.util.MdmRESTClient -::::- Error message while connecting to MDM
server : Connection Failed to the MDM server host -[redacted].jamfcloud.com, and port - 443 : Connection timeout occurred.
Check if the MDM server is reachable : SocketTimeoutException message = Read timed out 2019-03-02 07:53:20,177 ERROR [Thread-
4421][] cisco.cpm.mdm.api.MdmClient -::::- A connection timeout occurred. Check if the MDM server is reachable. 2019-03-02
07:53:20,177 ERROR [Thread-4421][] cisco.cpm.mdm.scheduler.MDMHeartbeat -::::- Exception occurred in MDM Heartbeat - thrown
from MDMVerifyServer connect() method - A connection timeout occurred. Check if the MDM server is reachable. 2019-03-02
07:53:20,177 DEBUG [Thread-4421][] cisco.cpm.mdm.scheduler.MDMHeartbeat -::::- Updated MDM Reachability status in MDM server
cache to false because of error while connecting to server
```