NotifyMDM
Mobile Device Management

Integrating Cisco ISE with NotifyMDM Quick Start

Table of Contents

Overview

Notify Technology Corporation is a leading provider of MDM software used to establish and enforce policies on hand-held endpoints. This could include corporate-owned or employee-owned phones and tablets. Devices manufactured by all the major equipment providers are supported at some level. Apple iOS and Android devices are the primary focus, but NotifyMDM also supports Blackberry and Windows Phone.

Mobile Device Management is being widely deployed in enterprise environments and is in a constant state of expansion.

Features can be grouped into several categories:

- Device Restrictions – There are two common types of restrictions. Either some feature of the device is disabled, such as the camera, or there are additional requirements for basic usage, such as a PIN lock or storage encryption. When a restriction is in place, the user is not offered the choice of non-compliance. Restrictions are used to reduce security risks to the enterprise.
- Device Compliance – This may also be referred to as posture enforcement. The MDM server will check the attributes of the device against a list of acceptable operational conditions. Compliance checks can be enforced based on their severity. For example, NotifyMDM can automatically restrict device access if the device has been compromised. A compliance check is different from a restriction because user actions can take the device out of compliance. Compliance can be used to increase security or reduce operational costs.
- Notifications – Administrators can send a message to a large population of devices. This could be a push message to the device notification page. For example, “The fire drill is complete, you may return to the building” could be sent to all devices on a particular campus. Notifications are used to increase productivity.
- Content Distribution – Documents can be made available to users on demand. Content distribution is used to increase productivity.
- Application Distribution – The MDM solution can offer a company catalog of available applications or install required applications. The applications can come from public repositories or can be corporate-developed applications. Application distribution has both security and productivity gains. Security is enhanced because any application distributed by the MDM, including local storage associated to the application, is removed as part of a corporate wipe.
- Corporate Resource Assignments – Corporate Resources are a collection of servers, networks, and other resources that MDM can make available to users. Using a user’s profile, MDM can manage apps, associate a device with servers or networks in the enterprise system, and configure user account settings to push out to the device. MDM can also push out resources such as Provisioning Profiles, Subscribed Calendars, Web Clips, and an Access Point Name, CalDav and CardDAV servers, Exchange Server, LDAP Servers, Mail Servers, Managed Apps, SCEP server, VPN, and Wi-Fi networks

The NotifyMDM solution has three main components:

- Policy server
- Device OS API
- Device client application

Beyond these, there are additional components for enterprise integration and, email. NotifyMDM requires the client application to detect some conditions, such as jail-broken (or the term Apple prefers, *Compromised OS*) or rooted devices.

Purpose and Description

Cisco Identity Services Engine (ISE) provides the enterprise with a method to screen any device trying to gain network access via Wi-Fi.

- The Wi-Fi access point forwards all traffic to a Wireless LAN Controller (WLC).
- Mobile devices are discovered by Cisco ISE as they attempt to access the network.
- Using the device MAC address, ISE queries NotifyMDM for the device's posture information.
- Based on information returned from the MDM server, ISE determines whether or not the device is permitted access and gives the WLC information it needs to determine which Access Control List (ACL) to apply to the device. The ACL details what resources are permitted or denied for the device. For example, an ACL can deny access to internal networks, but may allow Internet access.

Rules determining what ACL the Wireless LAN Controller should apply to the device are configured by the administrator in ISE. Criteria such as registered, not registered, compliant, not compliant, etc. determine which ACL is assigned.

Cisco ISE assigns network access level based on enrollment and posture results. ISE redirects unenrolled devices to a page from which the NotifyMDM app can be downloaded (Android) or to a web enrollment page (iOS).

Integration Steps

1. Import the primary root NotifyMDM site certificate to ISE
2. Grant ISE access to the NotifyMDM API
3. Add the NotifyMDM server to ISE

Getting NotifyMDM Ready for ISE

ISE Requirements

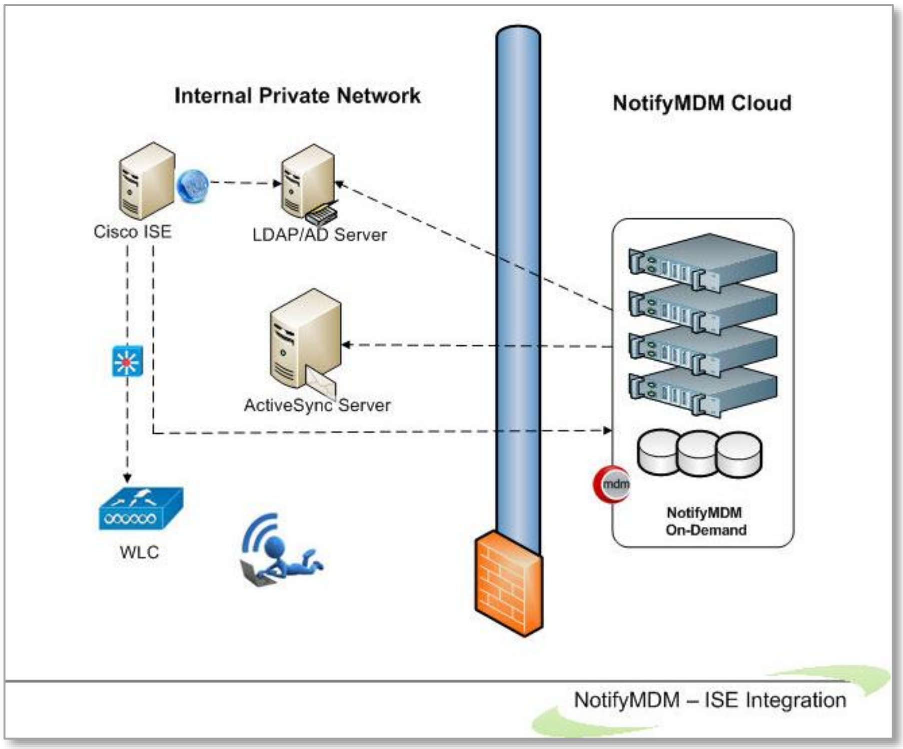
- The ISE console v1.3 requires Windows Internet Explorer (10.x - 11.x) or Mozilla Firefox (24.x - 30.x)
- The ISE console v1.2 requires Windows Internet Explorer (10.x – 11.x); It does not work on Chrome or Firefox.

Establishing Connectivity Between ISE and NotifyMDM

The first requirement is to establish basic connectivity between the Cisco ISE server and the NotifyMDM server.

For those using NotifyMDM on-demand service, a firewall is typically located between ISE and the NotifyMDM cloud. The firewall should be configured to allow an HTTPS session from ISE located in the data center to the NotifyMDM server located in the public Internet. The session is established outbound from ISE towards the MDM where ISE takes the client role. This is a common direction for web traffic over corporate firewalls.

Figure 1 Typical Cloud Deployment Model

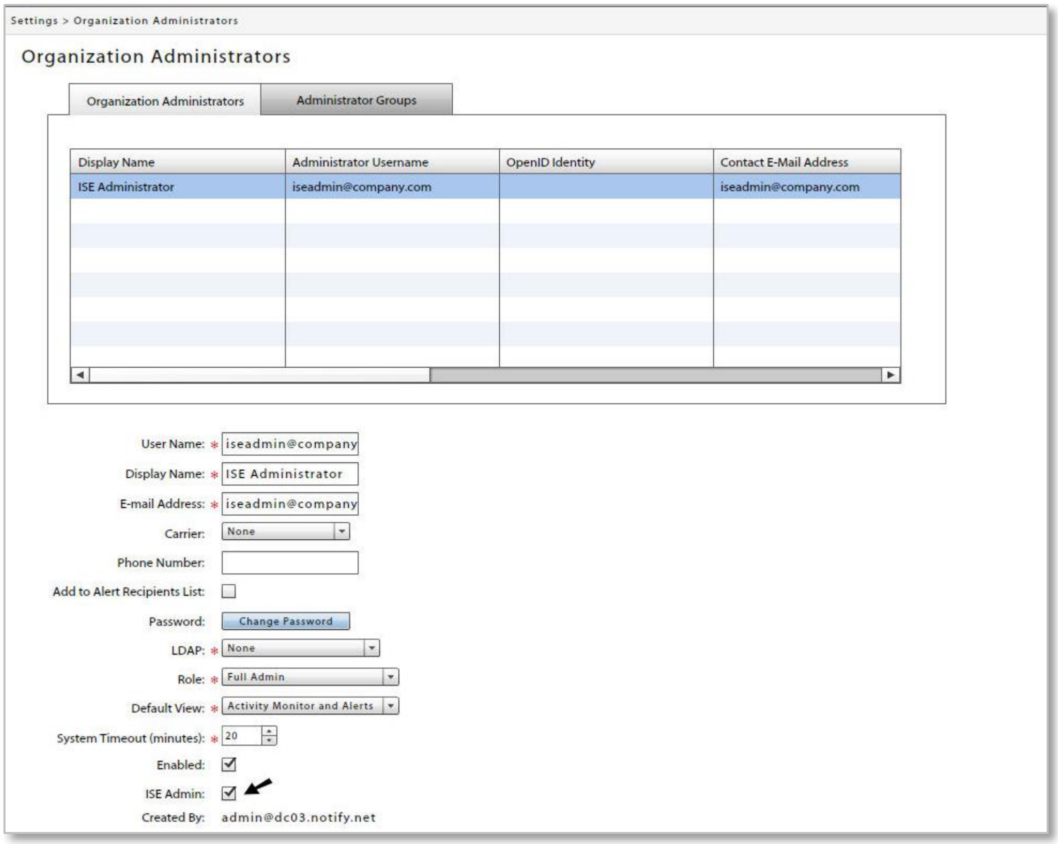


Grant ISE Access to the NotifyMDM API

The NotifyMDM API is protected by HTTPS and requires an Organization Administrator account that has been granted permission to the API. Ideally a specific account would be configured for ISE with a very strong password.

From the NotifyMDM dashboard, navigate to **System Management** > **Organization Administrators** and click **Add Administrator** to create an Organization Administrator account to be designated as the ISE administrator. Once it is created, select it from the grid and mark it as the **ISE Admin**.

Figure 5 Designate an Organization Administrator as the ISE Admin



Settings > Organization Administrators
Organization Administrators
Organization Administrators
Administrator Groups

Display Name	Administrator Username	OpenID Identity	Contact E-Mail Address
ISE Administrator	iseadmin@company.com		iseadmin@company.com

User Name: * iseadmin@company

Display Name: * ISE Administrator

E-mail Address: * iseadmin@company

Carrier: None

Phone Number:

Add to Alert Recipients List: □

Password: Change Password

LDAP: * None

Role: * Full Admin

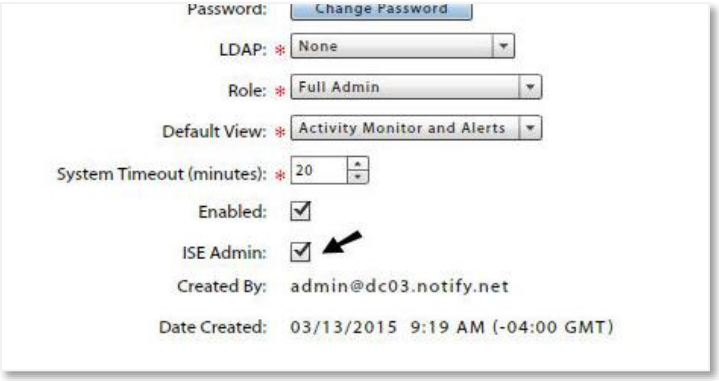
Default View: * Activity Monitor and Alerts

System Timeout (minutes): * 20

Enabled: ☑

ISE Admin: ☑

Created By: admin@dc03.notify.net



Password: Change Password

LDAP: * None

Role: * Full Admin

Default View: * Activity Monitor and Alerts

System Timeout (minutes): * 20

Enabled: ☑

ISE Admin: ☑

Created By: admin@dc03.notify.net

Date Created: 03/13/2015 9:19 AM (-04:00 GMT)

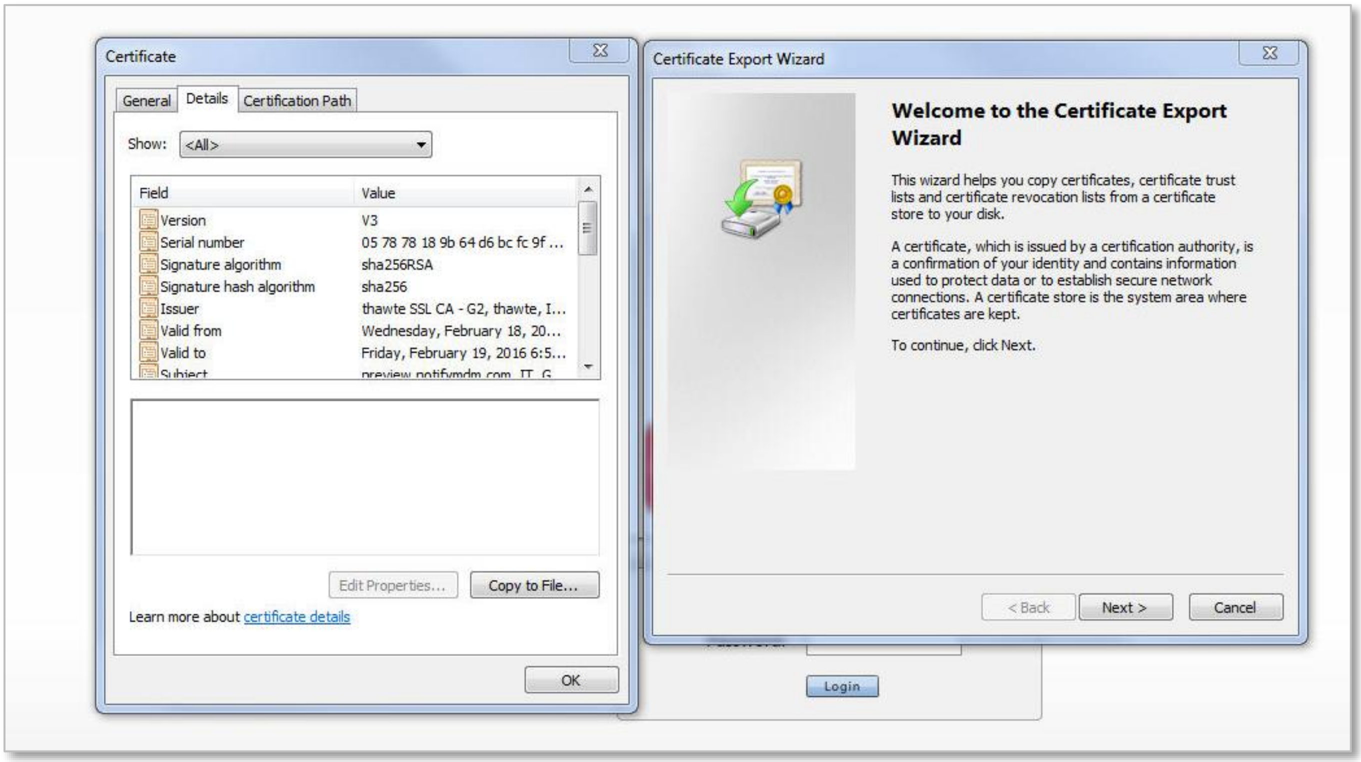
Import MDM Certificate to ISE

The NotifyMDM server incorporates an HTTPS portal to support the various users of the system. In the case of a cloud service, this website will be provided to the enterprise and ISE must establish trust with this website. Therefore the administrator must establish the trust relationship.

Export the MDM Site Certificate

The simplest approach is to export the primary root MDM site certificate, then import the certificate into a local cert store in ISE. Most browsers allow this. Internet explorer and Firefox are shown in Figures 2 & 3 with a cloud-based MDM deployment.

Figure 2 Exporting the MDM Site Certificate with Internet Explorer



Field	Value
Version	V3
Serial number	05 78 78 18 9b 64 d6 bc fc 9f ...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	thawte SSL CA - G2, thawte, I...
Valid from	Wednesday, February 18, 20...
Valid to	Friday, February 19, 2016 6:5...
Subject	preview.notifymdm.com, IT, G

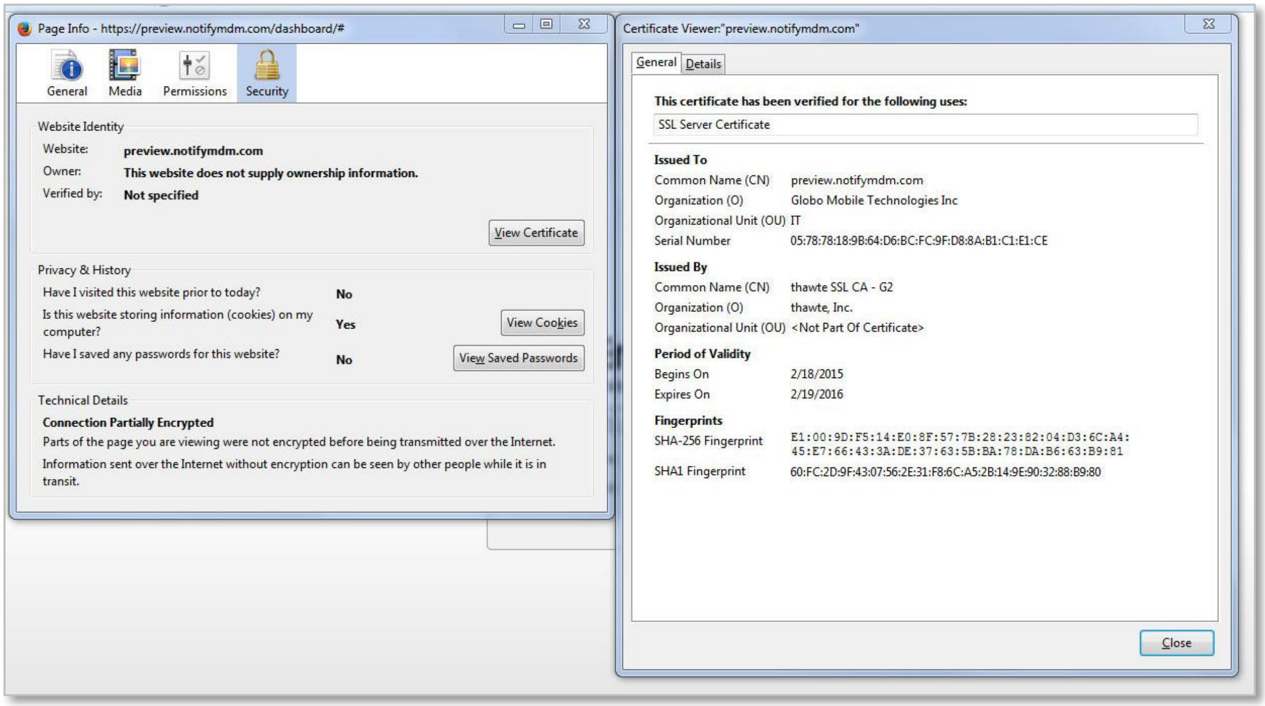
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Figure 3 Exporting the MDM Site Certificate with Firefox



Page Info - https://preview.notifymdm.com/dashboard/#

Website Identity

Website:	**preview.notifymdm.com**
Owner:	**This website does not supply ownership information.**
Verified by:	**Not specified**

Privacy & History

Have I visited this website prior to today?	**No**
Is this website storing information (cookies) on my computer?	**Yes**
Have I saved any passwords for this website?	**No**

Technical Details

Connection Partially Encrypted

Parts of the page you are viewing were not encrypted before being transmitted over the Internet.

Information sent over the Internet without encryption can be seen by other people while it is in transit.

Certificate Viewer:"preview.notifymdm.com"

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN)	preview.notifymdm.com
Organization (O)	Globo Mobile Technologies Inc
Organizational Unit (OU)	IT
Serial Number	05:78:78:18:9B:64:D6:BC:FC:9F:D8:8A:B1:C1:E1:CE

Issued By

Common Name (CN)	thawte SSL CA - G2
Organization (O)	thawte, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>

Period of Validity

Begins On	2/18/2015
Expires On	2/19/2016

Fingerprints

SHA-256 Fingerprint	E1:00:9D:F5:14:E0:8F:57:7B:28:23:82:04:D3:6C:A4: 45:E7:66:43:3A:DE:37:63:5B:BA:78:DA:B6:63:B9:81
SHA1 Fingerprint	60:FC:2D:9F:43:07:56:2E:31:F8:6C:A5:2B:14:9E:90:32:88:B9:80

Import the Certificate to ISE

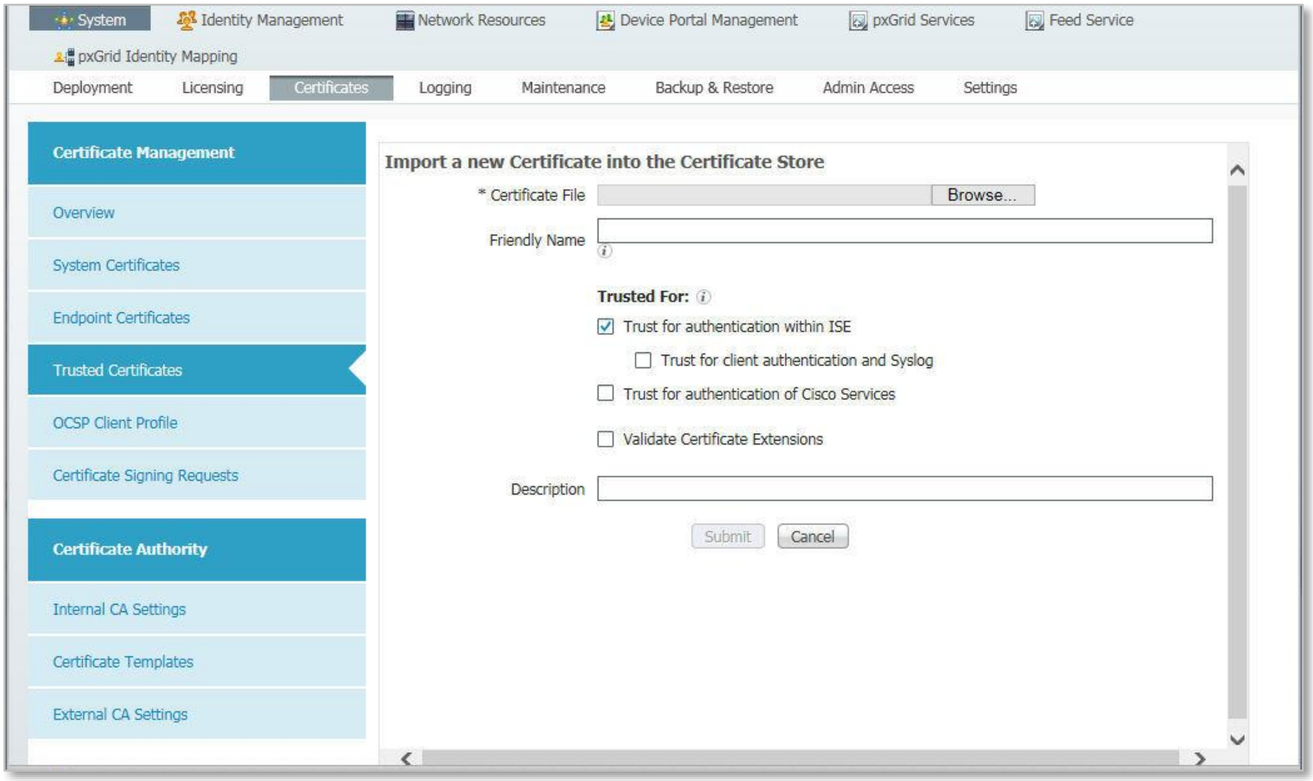
ISE has a certificate store to which you can import the MDM certificate.

From the ISE console, select the **Administration** tab and choose **Certificates**.
Select **Trusted Certificates** from the left panel.

At the **Certificate File** field browse to locate the certificate file and add it.

Verify that the checkbox next to, *Trust for authentication within ISE* is marked.

Figure 4 Importing the Certificate to ISE Certificate Store



Import a new Certificate into the Certificate Store

* Certificate File

Friendly Name

Trusted For:

☑ Trust for authentication within ISE

☐ Trust for client authentication and Syslog

☐ Trust for authentication of Cisco Services

☐ Validate Certificate Extensions

Description

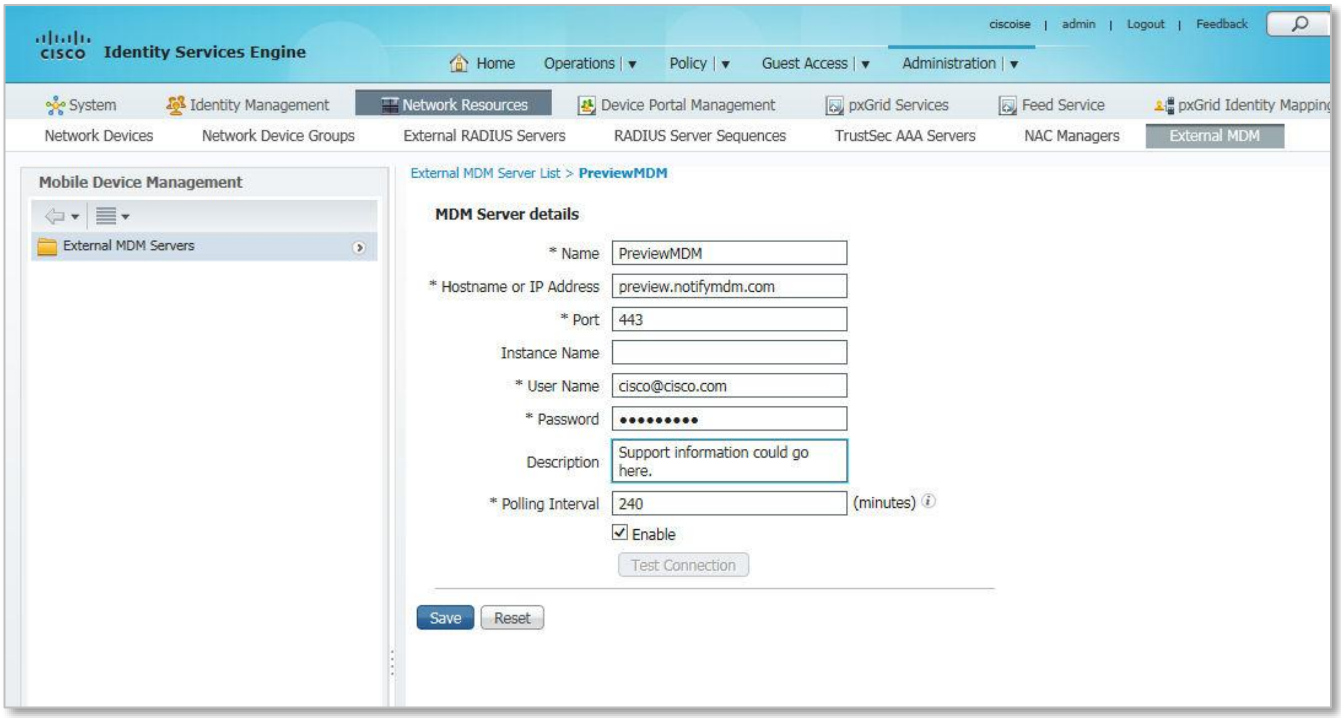
Add the NotifyMDM Server to ISE

Once the administrator account has been defined on the NotifyMDM server with the proper role, ISE can be configured to use this account when querying the NotifyMDM server for device information. ISE will contact the NotifyMDM server to gather posture information about devices or to issue device commands, such as corporate wipe or lock. The session is initiated from ISE towards the NotifyMDM server.

From the Cisco ISE console, navigate to **Administration** > **Network Resources** > **External MDM** to configure the NotifyMDM server.

Enter the **Name**, **IP Address**, and (external) **Port** of the NotifyMDM server.
In the **User Name** / **Password** fields, enter the MDM Organization Administrator credentials you have designated as the ISE Admin for NotifyMDM.

Figure 6 Configure the MDM API on ISE



MDM Server details

* Name	PreviewMDM
* Hostname or IP Address	preview.notifymdm.com
* Port	443
Instance Name	
* User Name	cisco@cisco.com
* Password	•••••••••
Description	Support information could go here.
* Polling Interval	240 (minutes)
	☑ Enable

Polling Interval. The polling interval specifies how often ISE will query the MDM for changes to device posture. ISE queries the NotifyMDM server for a list of the devices that are out of compliance. If a device associated to the network is found to be out of MDM compliance the compliance remediation action is to restrict network access. ISE will then issue a Change of Authorization (CoA), forcing the device to re-authenticate. Likely the device will need to remediate with the MDM to return to compliance. Note that MDM compliance requirements are configured on the MDM server and are independent of ant policy configured on ISE. It is possible, although not practical, to set the polling interval even if the ISE policy does not consider the MDM Compliant dictionary attribute.

- Polling can be disabled by setting the value to 0 minutes, however, the advantage of polling is that if a user takes the device out of MDM compliance, they will be forced to reauthorize that device. The shorter the polling interval, the quicker ISE will discover the condition.

There are some considerations to be aware of before setting this value. The MDM compliance posture could include a wide range of conditions not specific to network access. For example, the device administrator may want to know when an employee on a corporate device has exceeded 80% of the data plan to avoid any over usage charges. In this case, blocking network access based solely on this attribute would aggravate the MDM compliance condition and run counter to the device administrator's intentions. In addition, the CoA will interrupt the user Wi-Fi session, possibly terminating real-time applications such as VoIP calls.

The polling interval is a global setting and cannot be set for specific users or asset classes. The recommendation is to leave the polling interval at 0 until a full understanding of the MDM's configuration is complete. If the polling interval is set, then it should match the device check-in period defined on the MDM server. For example, if the MDM is configured such that devices will report their status every four hours, then ISE should be set to the same value and not less than half this value. Oversampling the device posture will create unnecessary loads on the MDM server.

Updates do not happen in real time. Keep the following in mind when deciding upon a polling interval:

- Compliance changes on the device may not be reported to the MDM server until the device's next scheduled check-in time.
- After the MDM server receives the changes from a device, compliance changes will not take effect until ISE requests a compliance update from the MDM server; MDM will not push.
- When ISE polls, it only asks for devices out of compliance.
- ISE only checks a specific device when the device creates a new session.
- ISE only reports updates which are criteria for compliance. For example: A user adds a pin lock, but pin lock is not a compliance criteria. ISE will not report that the user added a pin lock.

Test Connection. The Test Connection button will attempt to use the API to access the MDM server and is required prior to saving the settings with the MDM set to *Enable*. If the test does not complete successfully, the settings can still be saved, but the Enable box will be deselected and the connection to the MDM server will not be active.

Some problems can occur when testing the connection to the MDM server. Table 1 shows some common messages generated when testing the connection between ISE and NotifyMDM. The last message shown below confirms a successful connection.

Table 1: Connection Messages

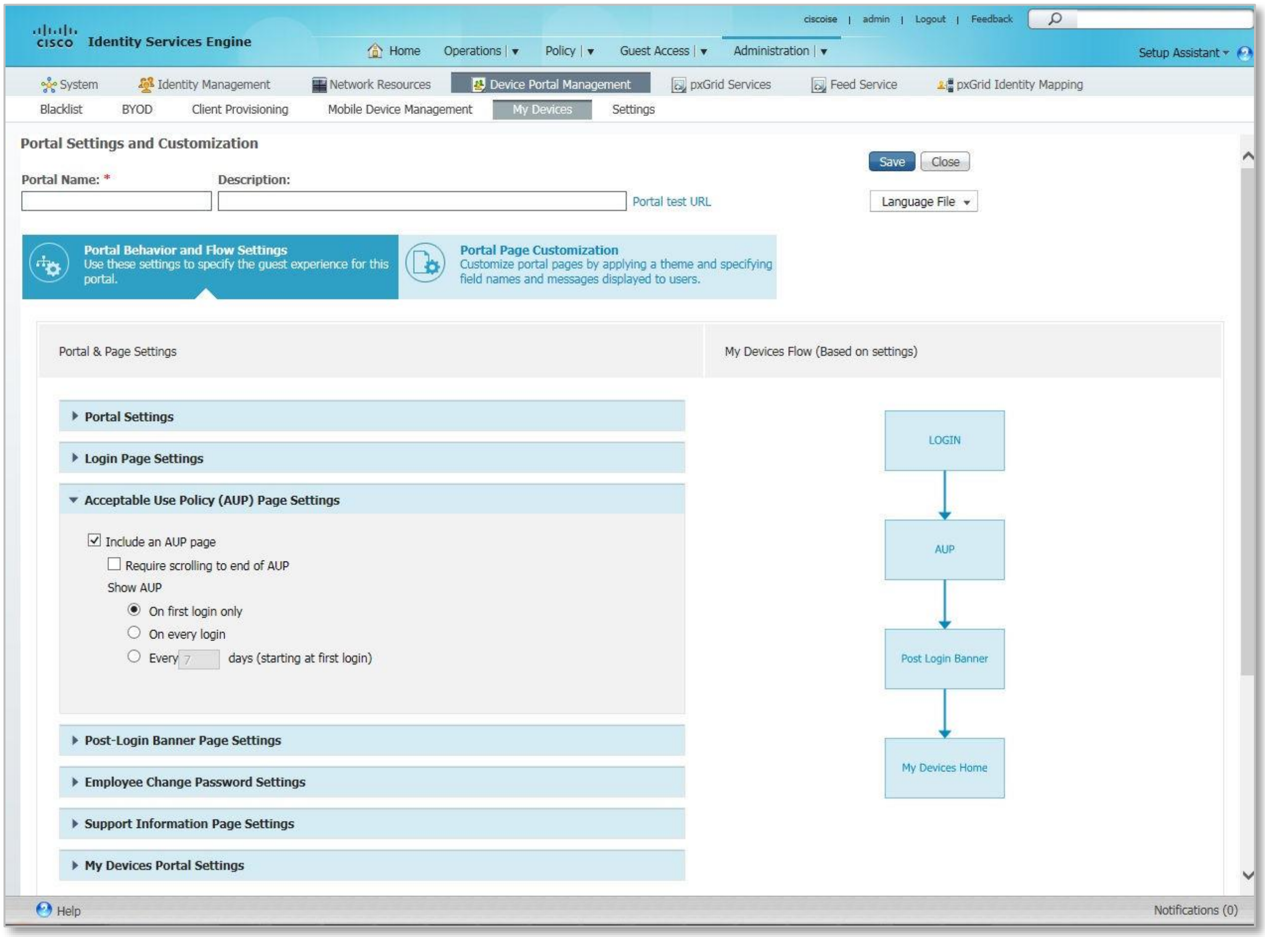
Message	**Explanation**
Connection failed: Please check connection parameters	A routing or firewall problem exists between the ISE located in the data center and the MDM located in either the DMZ or Cloud. The firewall's configuration should be checked to confirm HTTPS is allowed in this direction.
Connection Failed 404: Not Found	The most likely cause of an HTML 404 error code is that an instance was configured when it was not required or that the wrong instance has been configured.
Connection Failed 403: Forbidden	The user account setup on the NotifyMDM server does not have the proper roles associated to it. Validate that the account being used by ISE is assigned the REST API MDM roles as shown above.
Connection Failed 401: Unauthorized	The user name or password is not correct for the account being used by ISE. Another less likely scenario is that the URL entered is a valid MDM site, but not the same site used to configure the MDM account above. Either of these could result in the NotifyMDM server returning an HTML code 401 to ISE.
Connection Failed: There is a problem with the server Certificate or ISE trust store.	ISE does not trust the certificate presented by the NotifyMDM website. This indicates the certificate was not imported to the ISE certificate store as described above or the certificate has expired since it was imported.
The MDM Server details are valid and the connectivity was successful.	The connection has successfully been tested. The administrator should also verify the MDM AUTHZ dictionary has been populated with attributes.

Device Portal Management

Cisco ISE version 1.3 allows the administrator to configure certain end user elements including, but not limited to Acceptable Use Policy Page Settings, Login Page Settings, and Portal Settings. These settings will determine how information appears on the device enrollment page. Instructions for the user can be made available through these settings as well.

From the ISE console, navigate to **Administration** > **Device Portal Management** > **My Devices**.

Figure 8 Device Portal Management



Portal Settings and Customization

Portal Name: *

Description:

Portal Behavior and Flow Settings
Use these settings to specify the guest experience for this portal.

Portal Page Customization
Customize portal pages by applying a theme and specifying field names and messages displayed to users.

Portal & Page Settings

- ▸ **Portal Settings**
- ▸ **Login Page Settings**
- ▾ **Acceptable Use Policy (AUP) Page Settings**

☑ Include an AUP page
□ Require scrolling to end of AUP
Show AUP
● On first login only
○ On every login
○ Every 7 days (starting at first login)

- ▸ **Post-Login Banner Page Settings**
- ▸ **Employee Change Password Settings**
- ▸ **Support Information Page Settings**
- ▸ **My Devices Portal Settings**

My Devices Flow (Based on settings)

LOGIN → AUP → Post Login Banner → My Devices Home

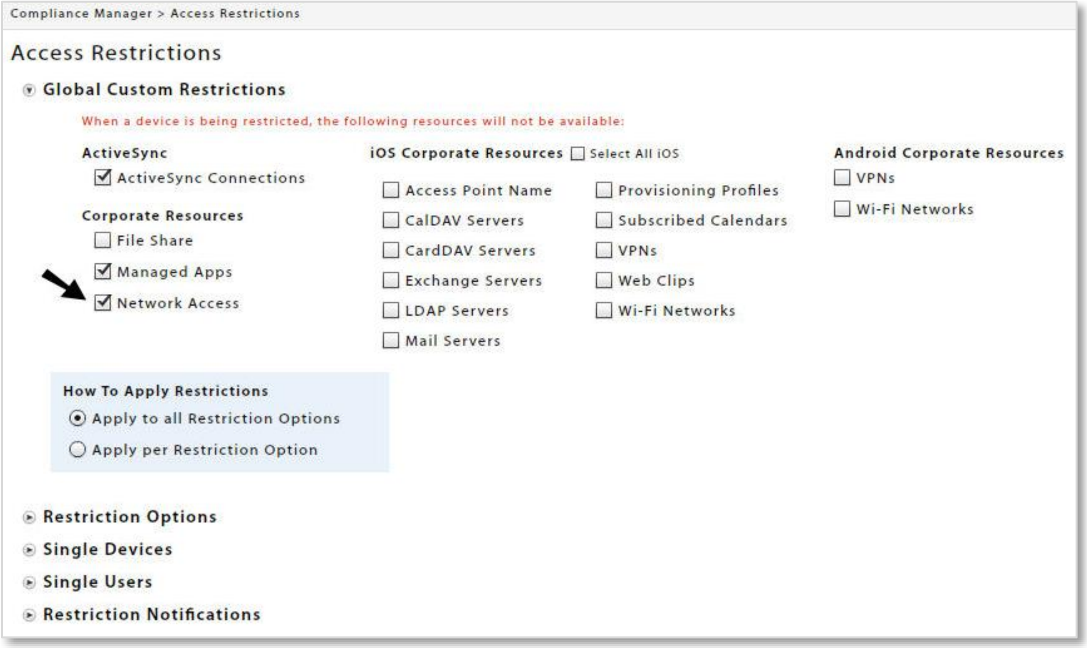
MDM Network Access Restriction

NotifyMDM should be configured to restrict network access when devices are non-compliant.

From the NotifyMDM dashboard, navigate to **Organization Management** > **Compliance Manager** > **Access Restrictions**.
Mark the box next to the **Network Access** option under Corporate Resources.

Network Access restriction can also be imposed for a particular device platform, a single user, or a single device.

Figure 9 MDM Network Access Restriction



Compliance Manager > Access Restrictions

Access Restrictions

Global Custom Restrictions

When a device is being restricted, the following resources will not be available:

ActiveSync
- ☑ ActiveSync Connections

Corporate Resources
- □ File Share
- ☑ Managed Apps
- ☑ Network Access

iOS Corporate Resources □ Select All iOS
- □ Access Point Name
- □ CalDAV Servers
- □ CardDAV Servers
- □ Exchange Servers
- □ LDAP Servers
- □ Mail Servers
- □ Provisioning Profiles
- □ Subscribed Calendars
- □ VPNs
- □ Web Clips
- □ Wi-Fi Networks

Android Corporate Resources
- □ VPNs
- □ Wi-Fi Networks

How To Apply Restrictions
- ● Apply to all Restriction Options
- ○ Apply per Restriction Option

Restriction Options

Single Devices

Single Users

Restriction Notifications