

AirWatch - Cisco ISE Integration

Enhancing Corporate Wi-Fi Security Cisco ISE and AirWatch

© 2014 VMware, Inc. All rights reserved.

This document, as well as the software described in it, is furnished under license. The information in this manual may only be used in accordance with the terms of the license. This document should not be reproduced, stored or transmitted in any form, except as permitted by the license or by the express permission of AirWatch, LLC.

All other marks and names mentioned herein may be trademarks or trade names of their respective companies.

Contents

Introduction.....	3
Use Case	3
Process	4
Who Can Benefit from AirWatch - Cisco ISE Integration?.....	4
Enterprises Not Utilizing Mobile Device Network Security Policies	4
Enterprises Not Allowing Mobile Devices on Network.....	4
Enterprises Currently Using Cisco ISE without AirWatch	4
Requirements	5

Introduction

The Cisco Identity Services Engine (ISE) is a Network Access Control (NAC) appliance designed to enhance network security by forcing devices to comply with policies before they are allowed to access a corporate network. AirWatch customers who are interested in using Cisco networking components and have advanced security requirements can benefit from AirWatch's integration with Cisco ISE functionality to give them a more complete network security solution.

Use Case

As a stand-alone solution, the Cisco ISE ensures mobile devices connected to your corporate Wi-Fi network are compliant with limited policies based on device type and user. When AirWatch and Cisco ISE are integrated, the ISE makes much more accurate and specific compliance decisions on a more granular level by using the wealth of mobile device data AirWatch provides.

Conversely, the ISE takes AirWatch's ability to enable or disable Wi-Fi functionality a step further by restricting access to whitelisted websites while a device is connected to the corporate Wi-Fi network. The following table depicts which data elements AirWatch and Cisco can manage individually and demonstrates the power of this integrated solution.

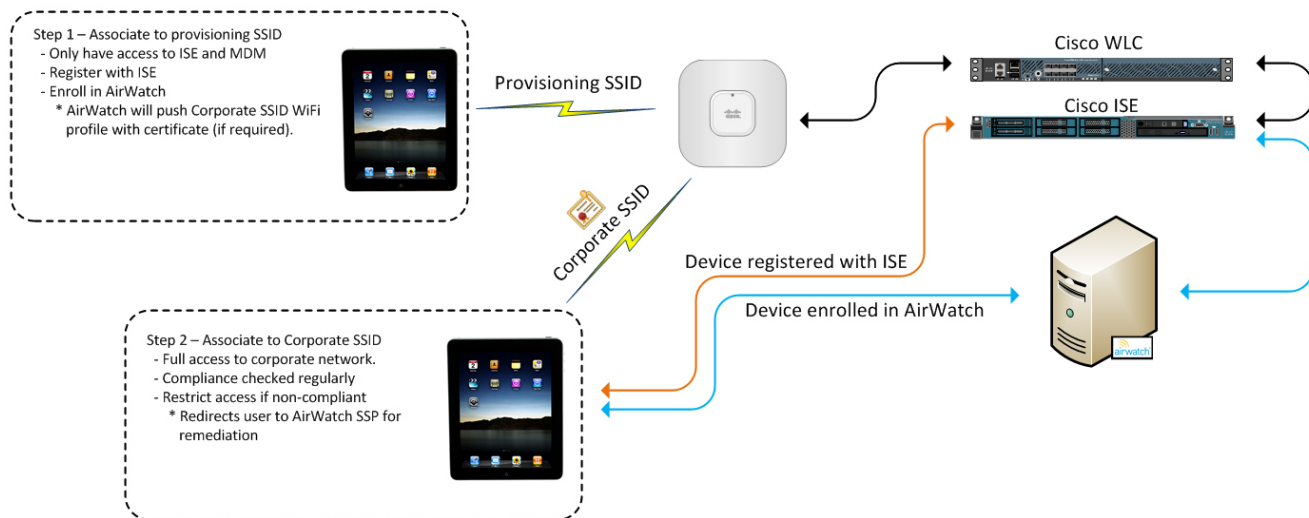
	AirWatch	Cisco
Device Type	✓	✓
Device User	✓	✓
Device Details	✓	✗
Device Compromised	✓	✗
Device Compliance	✓	✗
Disable WiFi	✓	✓
Restrict WiFi*	✗	✓

*Selectively restrict access to whitelisted websites only.

Process

The AirWatch-Cisco ISE integrated solution creates a secure method of access for anyone attempting to join your internal corporate Wi-Fi network. This requires registration with the ISE and enrollment into your AirWatch environment. When an end-user attempts to connect their mobile device, they initially access a Service Set Identifier (SSID) which prompts them to register with the ISE and enroll in AirWatch.

Once enrolled, AirWatch deploys the internal corporate Wi-Fi profile along with any other applicable restrictions. When the device connects to the internal SSID, it has full access to the corporate network. While the device connected, compliance is checked against assigned policies at regular intervals. Additionally, if a device violates an active compliance policy, access is immediately restricted and the user is redirected to the AirWatch Self Service Portal (SSP) for remediation.



Who Can Benefit from AirWatch - Cisco ISE Integration?

Enterprises Not Utilizing Mobile Device Network Security Policies

If your company does not enforce security policies on mobile devices when accessing the internal corporate Wi-Fi network, your infrastructure is potentially exposed to security risks and attacks from the mobile device. Incorporating the Cisco ISE and AirWatch allows mobile devices to connect to the corporate Wi-Fi in a safe and secure manner.

Enterprises Not Allowing Mobile Devices on Network

If your company does not currently allow mobile devices on your internal corporate network, incorporating the Cisco ISE along with AirWatch could allow devices on to the corporate Wi-Fi, because both products work together to minimize or remove risks associated with allowing mobile devices on to the Wi-Fi network.

Enterprises Currently Using Cisco ISE without AirWatch

If you already have a Cisco ISE solution, adding AirWatch to the architecture enhances the functionality of the ISE by adding more detail to the mobile device status. When used with your existing Cisco Wireless Networking components and AirWatch, you can confirm mobile devices accessing your wireless network are compliant with your security policies.

Requirements

If you would like to take advantage of the enhanced mobile device security provided by the AirWatch-Cisco ISE integrated solution, ensure you have the following resources available:

- AirWatch version 6.1 SP1 or higher with the AirWatch Cisco ISE API installed
- Cisco ISE version 1.2 or higher
- Cisco Wireless LAN Controller (WLC) version 7.3 or higher

To ensure your environment is compatible with the Cisco ISE APIs and that you have the latest version of the Cisco APIs installed, launch a web browser and navigate to the following URL: `https://{apiurl}/ciscoise/mdminfo`. The {apiurl} value for the actual URL can be found in the AirWatch Admin Console. From the main menu, navigate to **Groups & Settings ► All Settings ► System ► Advanced ► Site URLs**. For SaaS environments, the format is `asXX.airwatchportals.com` (e.g., the URL for cn22 would be `as22.airwatchportals.com`). If you are prompted for a username/password, installation was successful. If a '404 not found' error is displayed, installation was not completed. Contact your Cisco representative as well as AirWatch Support for assistance or if you have any additional questions about Cisco ISE integration.

AirWatch Configuration

The Cisco ISE API must be installed on the AirWatch API Server. Beginning with AirWatch v6.4, the API is installed automatically. For AirWatch users running versions older than v6.4, the Cisco ISE API must be installed using a separate installer.

To check if the API is installed:

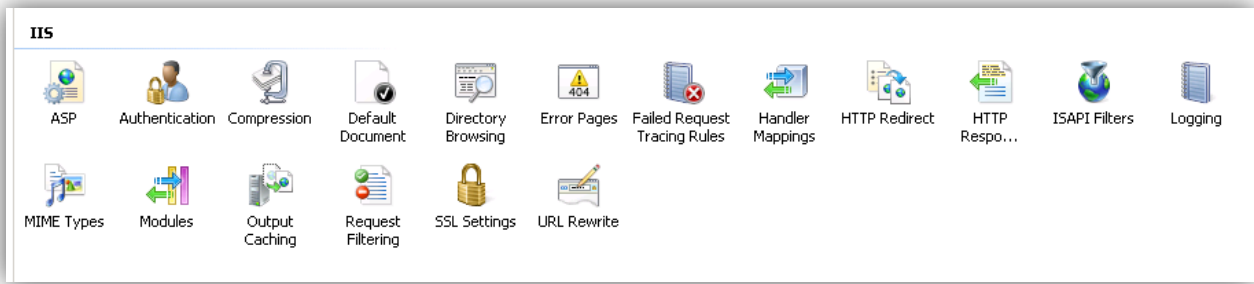
1. Open an Internet browser and navigate to the URL <https://{apiurl}/ciscoise/mdminfo>. The {apiurl} value for the actual URL can be found in the AirWatch Admin Console. Navigate to **Groups & Settings ► All Settings ► System ► Advanced ► Site URLs**. For SaaS environments, the format is `asXX.airwatchportals.com` (e.g., the URL for cn22 would be `as22.airwatchportals.com`).
2. Enter a basic administrator's username and password when prompted for credentials. An XML file with site specific information should be displayed.

Note: If you are not prompted to enter credentials, the Cisco ISE API is not installed.

If the XML file is not displayed, the Cisco ISE API is not installed correctly. The most likely cause is the URL Rewrite is configured incorrectly or at the wrong location.

To check the URL Rewrite configuration:

3. Launch IIS on the API Server and navigate to the Default Web Site.
4. Ensure the rewrite rule is configured at this location and not the **ciscoise** level.
5. Confirm the **URL Rewrite** IIS plugin is installed and configured with a rule to redirect any traffic from `/ciscoise/mdminfo` to `/ciscoise/v1/ciscoise/registration/mdminfo` as shown below.



Edit Inbound Rule

Name: Cisco mdminfo

Match URL

Requested URL: Matches the Pattern Using: Regular Expressions

Pattern: [Test pattern...](#)

Ignore case

Conditions

Server Variables

Action

Action type: Rewrite

Action Properties

Rewrite URL:

Append query string

Log rewritten URL


Stop processing of subsequent rules

Cisco ISE Configuration


Import the AirWatch Server SSL Certificate into the ISE

6. Obtain the SSL Certificate of the AirWatch site using the following Internet browser-specific procedures:


a. Chrome

- i. Launch Chrome and access the URL for the AirWatch environment.
- ii. Click the  icon to the left of the environment URL and select the **Connections** tab within the menu that appears.
- iii. Click the **Certificate information** hyperlink to launch the Certificates dialog.
- iv. Select the **Details** tab and click **Copy to File...** to launch the Certificate Export Wizard.
- v. Click **Next**.
- vi. Ensure the desired export format (.CER) is selected and click **Next**.
- vii. Enter a file name for the certificate and click **Next**.
- viii. Click **Finish**.

b. Firefox

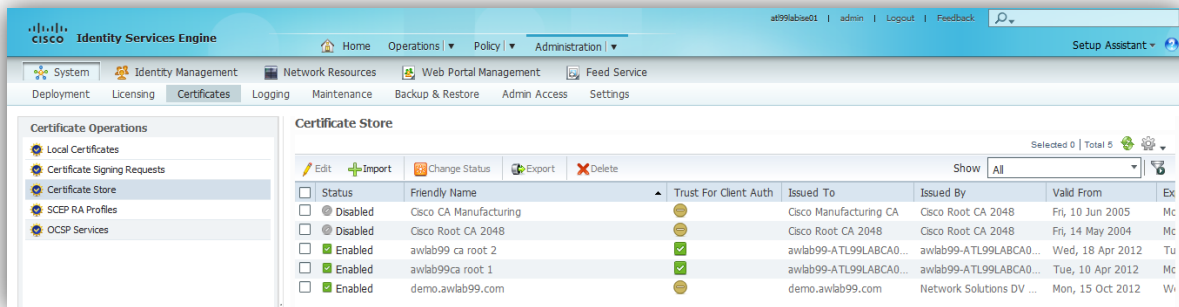
- i. Launch Firefox and access the URL for the AirWatch environment.
- ii. Click the  icon to the left of the environment URL and then click **More Information...** to launch the Page Info dialog.
- iii. Click **View Certificate** to launch the Certificate Viewer dialog.
- iv. Select the **Details** tab and click **Export**.
- v. Enter a file name for the certificate and ensure the desired network location and file type (.CER) are correct.
- vi. Click **Save**.

c. Internet Explorer

- i. Launch Internet Explorer and access the URL for the AirWatch environment.
- ii. Click the  icon to the right of the environment URL and then click **View certificates** to launch the Certificate dialog.
- iii. Select the **Details** tab and click **Copy to File...** to launch the Certificate Export Wizard.
- iv. Click **Next**.
- v. Ensure the desired export format (.CER) is selected and click **Next**.
- vi. Enter a file name for the certificate and click **Next**.
- vii. Click **Finish**.

d. Safari

- i. Launch Safari and access the URL for the AirWatch environment.
 - ii. Click the **https** icon to the left of the environment URL and then click **Show Certificate** to launch the Certificate dialog.
 - iii. Note the name of the certificate and then click **OK** to close the dialog.
 - iv. Launch Finder and navigate to **Applications ► Utilities**.
 - v. Launch **Keychain Access**.
 - vi. Select the **Certificates** category at left and click the applicable certificate.
 - vii. From the device's main menu, select **File ► Export Items....**
 - viii. Enter a file name for the certificate, specify a destination location, and select **. CER** as the file type.
 - ix. Click **Save**.
7. On the ISE, navigate to **Administration ► Certificates ► Certificate Store**.
 8. Select **Import** and then select the certificate obtained in the previous step.



Configure AirWatch as the MDM Server

9. Navigate to **Administration ► MDM**.
10. Click **Add** to create a new record.
11. Enter the required information about the AirWatch server.
12. Click **Verify**.
13. If everything appears correct, click **OK**.
14. Ensure the **Active** checkbox is selected and then click **Save**.

Cisco Identity Services Engine at99labise01

Home | Operations | Policy | Administration

System | Identity Management | Network Resources | Web Portal Management | Feed Service

Network Devices | Network Device Groups | External RADIUS Servers | RADIUS Server Sequences | SGA AAA Servers | NAC Managers | **MDM**

Mobile Device Management

External MDM Servers

External MDM Server List > **AirWatch_AWLAB99**

MDM Server details

* Name:

* Server host:

* Port:

Instance Name:

* User Name:

* Password:

Description:

* Polling Interval: (minutes)

Enable