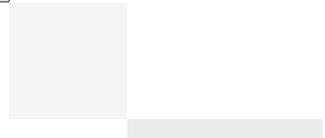
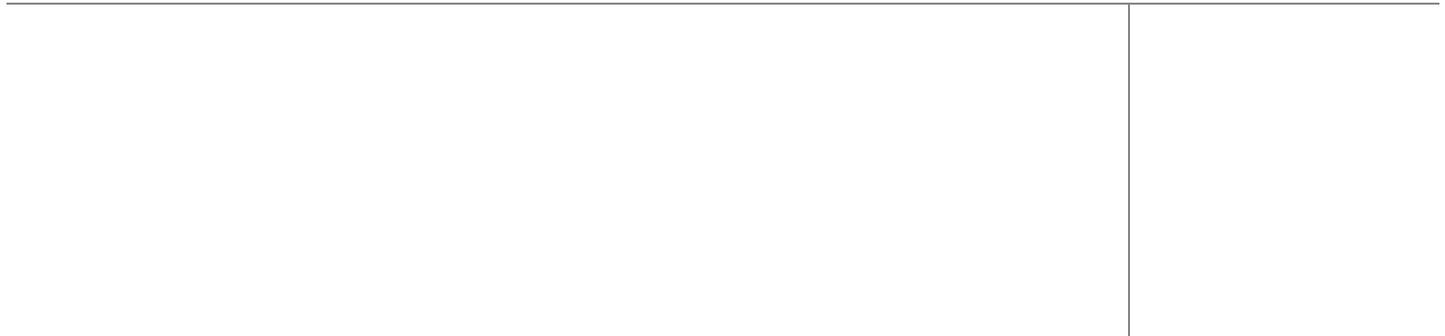




Integrating AirWatch with Cisco Identity Services Engine

Revised: August 6, 2013



ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at <http://www.cisco.com/go/trademarks>. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Integrating AirWatch with Cisco Identity Services Engine

© 2013 Cisco Systems, Inc. All rights reserved.



Integrating AirWatch with Cisco Identity Services Engine

This document supplements the Cisco Bring Your Own Device (BYOD) CVD (http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide.html) and provides mobile device management (MDM) partner-specific information as needed to integrate with Cisco ISE. In an effort to maintain readability, some of the information presented in the CVD is repeated here. However this document is not intended to provide standalone BYOD guidance. Furthermore, only a subset of the AirWatch MDM functionality is discussed. Features not required to extend ISE's capabilities may be mentioned, but not in the detail required for a comprehensive understanding. The reader should be familiar with the AirWatch Administrator's guide.

This document is targeted at existing AirWatch customers. Information necessary to select an MDM partner is not offered in this document. The features discussed are considered to be core functionality present in all MDM software and are required to be compatible with the ISE API.

Overview

AirWatch is a leading provider of MDM software used to establish and enforce device policy on hand-held endpoints. This could include corporate- 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 AirWatch also supports Blackberry, Win8, and Apple's Mountain Lion software (OSX 10.8).

Mobile Device management is a relatively new phenomenon 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 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, an email could be sent to the user when they have exceeded 80% of their data plan or AirWatch can automatically issue a corporate wipe if the device



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2013 Cisco Systems, Inc. All rights reserved.

has been compromised. A compliance check is different from a restriction because the user 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**—Bookmarks, documents, and other content can be pushed to devices in the background without user intervention or made available on demand. This data is then stored in a corporate container. Content distribution is used to increase productivity.
- **Application Distribution**—The MDM can offer a company catalog of available software or install required software. The software can come from public repositories or can be corporate-developed applications. Application distribution has both security and productivity gains. Security is enhanced because any software distributed by the MDM, including local storage associated to the software, is removed as part of a corporate wipe. This is not true if the user installs the same software from Apple’s App Store or Google Play.

AirWatch’s MDM solution has three main components:

- Policy server
- Device OS API
- Device client software

Beyond these, there are additional components for enterprise integration, email, secure Web, and data loss prevention. The majority of the base functionality is available through the MDM API built into the mobile device operating system. AirWatch requires the client software to detect some conditions, such as jail-broken¹ or rooted devices. Because ISE tests for these conditions, the AirWatch server is configured to treat the client software as a required application and will install the software during the on-boarding process.

Deployment Models

AirWatch offers both an on-premise model and cloud service model. The two models are functionally equivalent. The CVD explores the advantages and disadvantages of each of the models. An obvious difference is the topology. An on-premise model is defined when the MDM server is located in the enterprise DMZ and managed directly by the enterprise. A cloud model places the MDM server in the cloud and is offered as a software subscription. Both models support integration with corporate services, such as corporate directories, Microsoft Exchange, or a Blackberry Enterprise Server. The cloud model provides this functionality with AirWatch’s Enterprise Integration Server. The discussion below, including the illustrations, is based on a cloud model.



Note

Starting with AirWatch version 6.4, the Enterprise Integration Server is replaced with the AirWatch Cloud Connector (AWCC) and the Mobile Access Gateway (MAG). AWCC offers integration with local systems, such as user directory integration, while the MAG provides enhanced data loss prevention (DLP).

1. Apple prefers the term “Compromised OS” when referring to devices where the user has gained elevated privileges to the operating system.

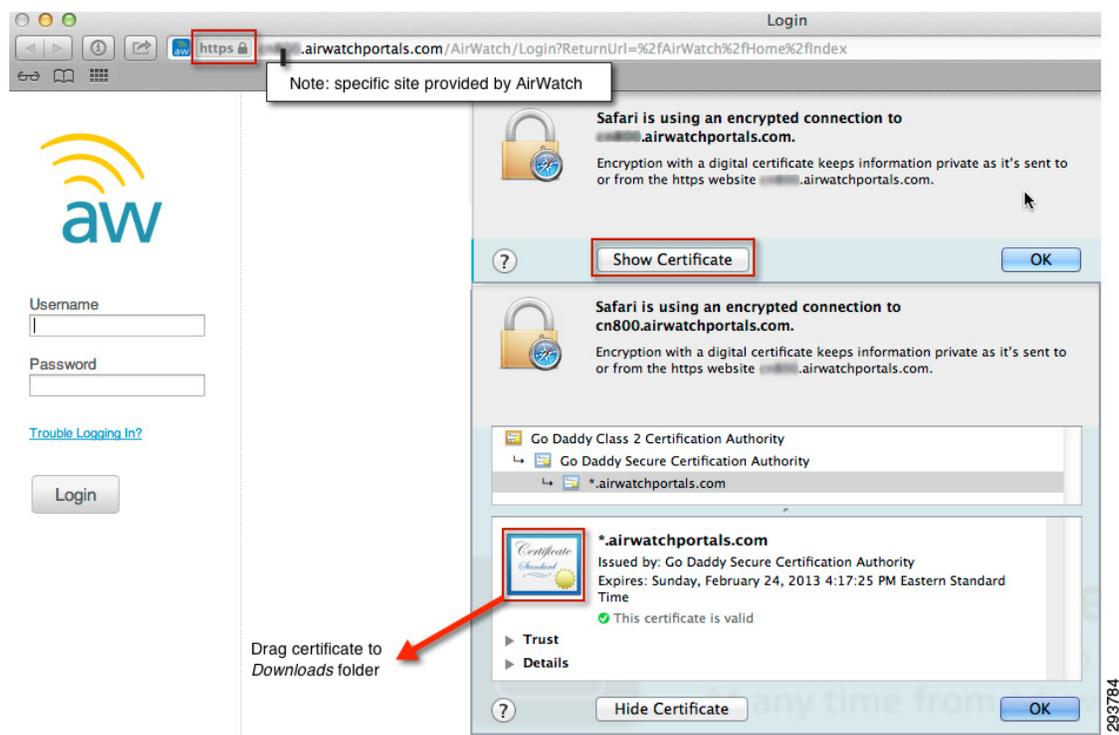
Getting AirWatch ready for ISE

The first requirement is to establish basic connectivity between the Cisco ISE server and the AirWatch MDM server. In both the on-premise and the cloud model, a firewall is typically located between these two components. The firewall should be configured to allow an HTTPS session from ISE located in the data center to the MDM server located in either the corporate DMZ or 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.

Import API Portal Certificate to ISE

The AirWatch MDM 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. ISE must establish trust with this website. Even though the cloud website is authenticated with a publicly signed certificate, ISE does not maintain a list of trusted root CAs. Therefore, the administrator must establish the trust relationship. The simplest approach is to export the MDM site certificate, then import the certificate into local cert store in ISE. Most browsers allow this. Safari is shown in [Figure 1](#) with a cloud-based MDM deployment.

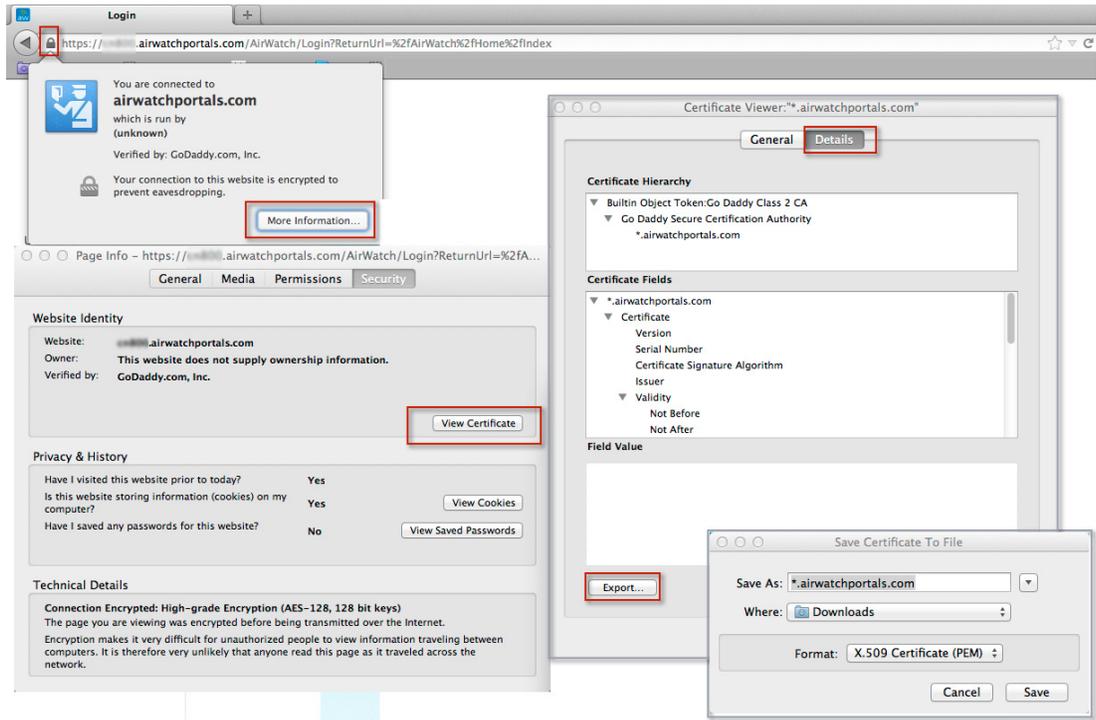
Figure 1 Exporting the MDM Site Certificate with Safari



AirWatch utilizes a wildcard certificate that is valid for all portal websites belonging to the airwatchportals.com domain.

Exporting a certificate from Firefox is covered in the CVD and repeated in [Figure 2](#).

Figure 2 Exporting the MDM Site Certificate with Firefox

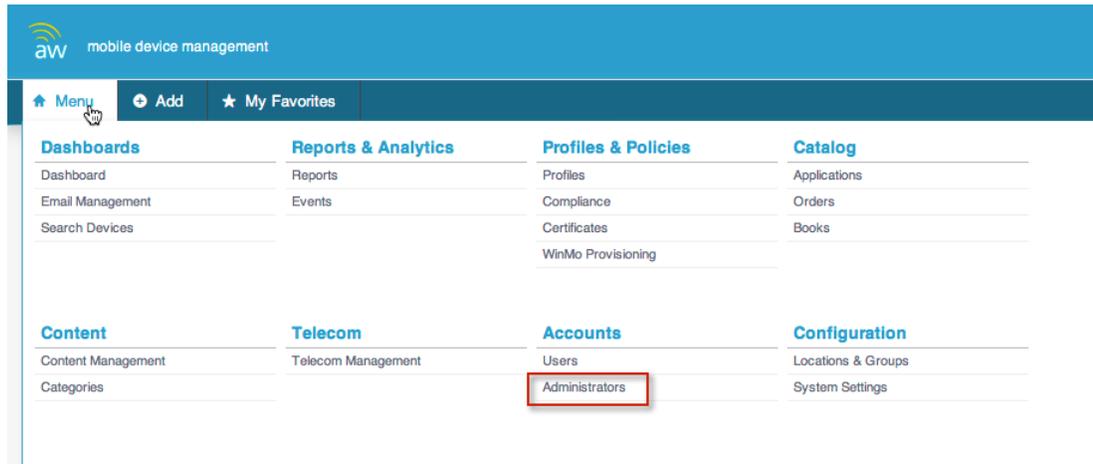


Grant ISE Access to the AirWatch API

The AirWatch API is protected by HTTPS and requires an administrator account that has been granted permission to the API. Ideally a specific account would be configured for ISE with a very strong password. In addition to this account, only a limited number of administrator accounts should be granted the ability to create new administrators or assign administrator roles.

Before the user is created, an API role should be created for ISE. This role will then be tied to an administrator account assigned to ISE along with an organization group for the account. AirWatch uses organization groups to logically partition the service. Administrators can manage the system settings at their level or create additional child organization groups below their group level, but have no access to the system settings above their organization group. The highest-level organization group is known as global. Organization groups and their implications for multi-domain ISE environments are out of scope. The administrator should configure the API role at the highest level organization group available to them and assign the ISE API account to the same group. Additional details concerning organization groups are available in the AirWatch documentation and introduced later in this document. A local administrator account is required for the REST MDM API roles to function properly.

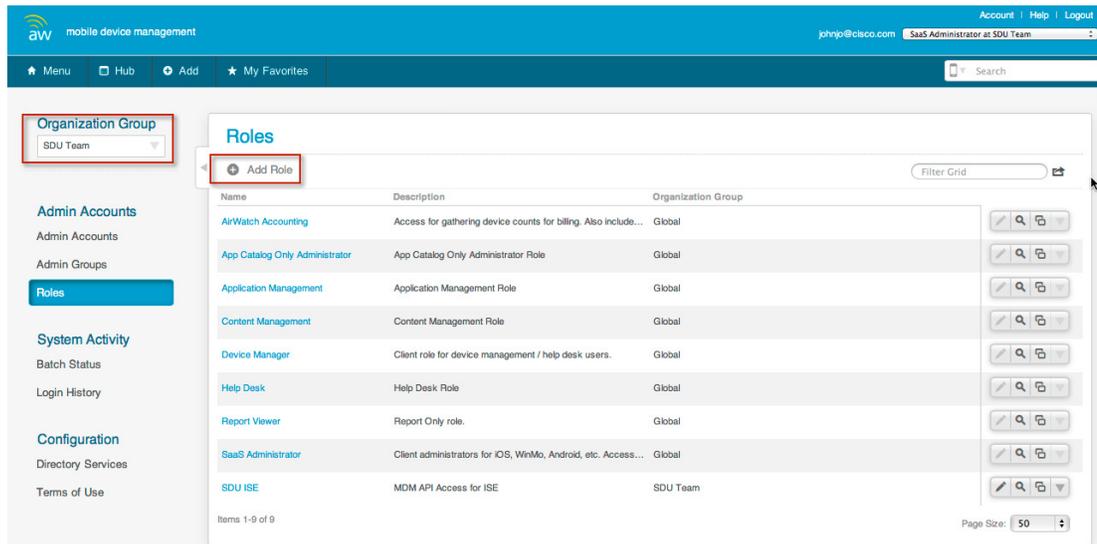
Figure 3 *Select Administrator Account*



293786

Each account type can be assigned roles entitling that user to specific features of the system. AirWatch provides default roles for the most common types of administrators and users. The majority of administrator roles do have access to the MDM API. As shown in [Figure 4](#), a role can be created that will include only the API service. This role will then be assigned to the ISE user account.

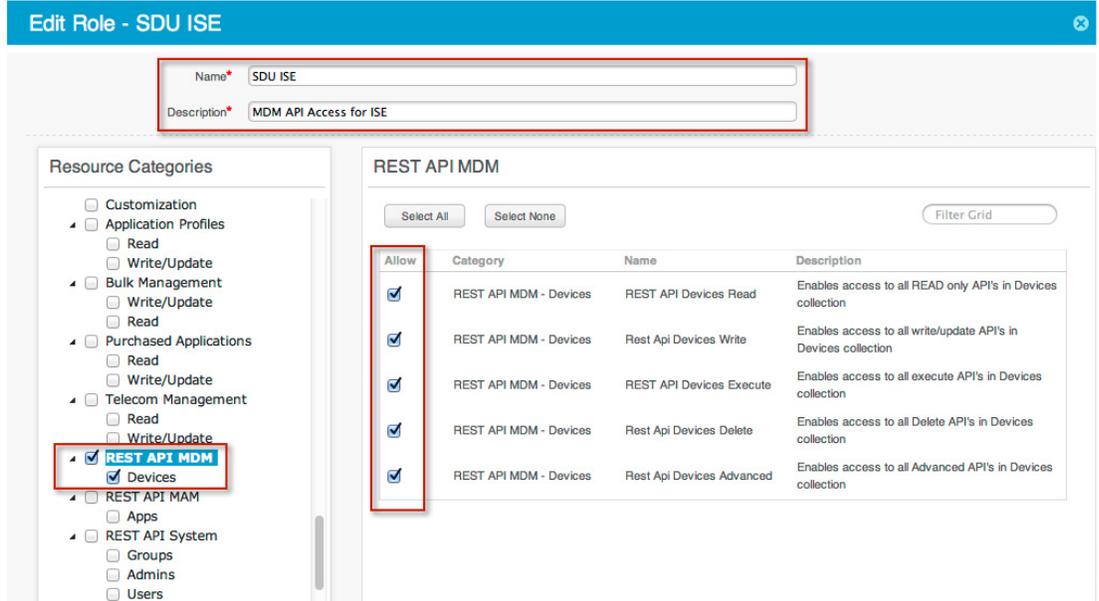
Figure 4 *Add Role Template to be Used by ISE*



293787

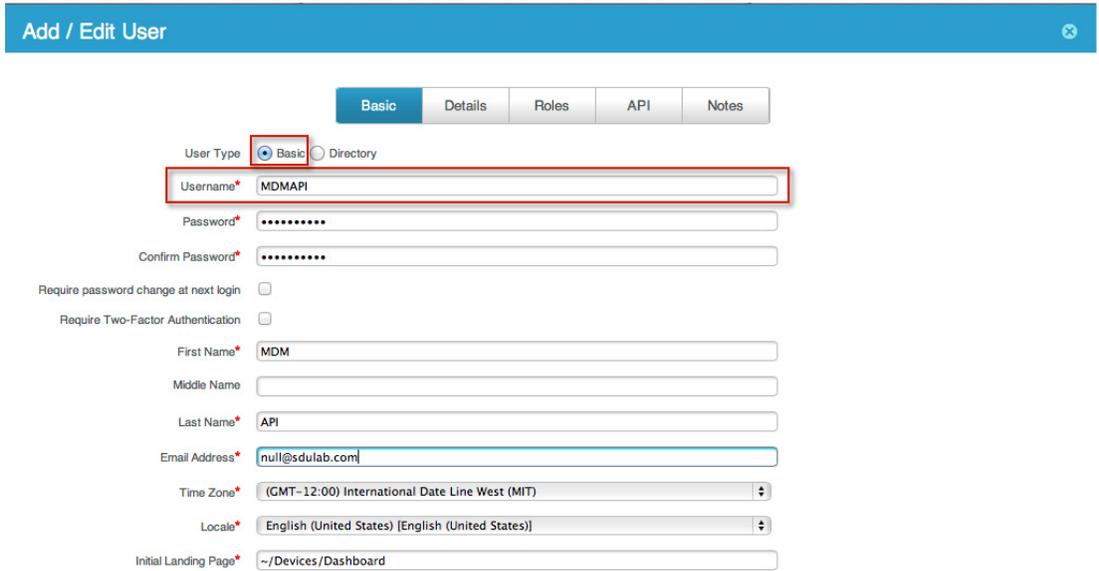
The MDM role created for ISE requires the REST API features. The resource categories on the left can be used to select REST API MDM and de-select all of the other categories. The specific items belonging to each category are listed on the right, along with a brief description.

Figure 5 Assign REST API to Role



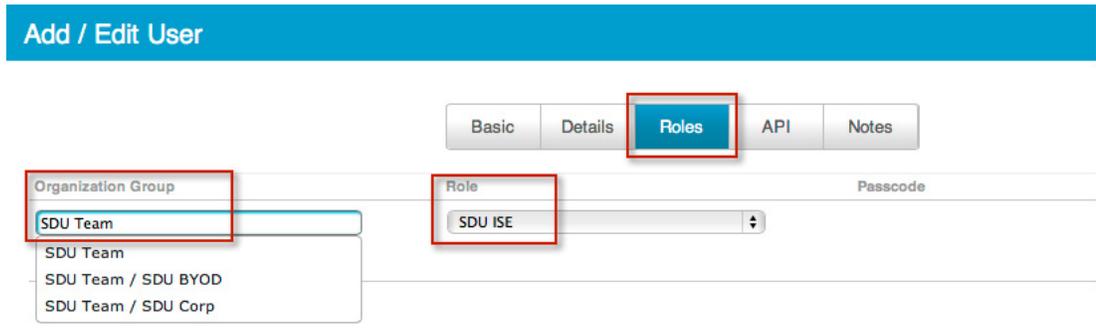
Once the role as been added, an admin account can be created for ISE. The basic information required for all accounts includes a username, password, and email address. The email address can be fictitious as shown here, or could be the ISE administrator’s email. The MDM will not send email to this address.

Figure 6 Create User Account for ISE



Finally the account created for ISE is assigned the previously created role.

Figure 7 Bind Account to Organization Group and Role

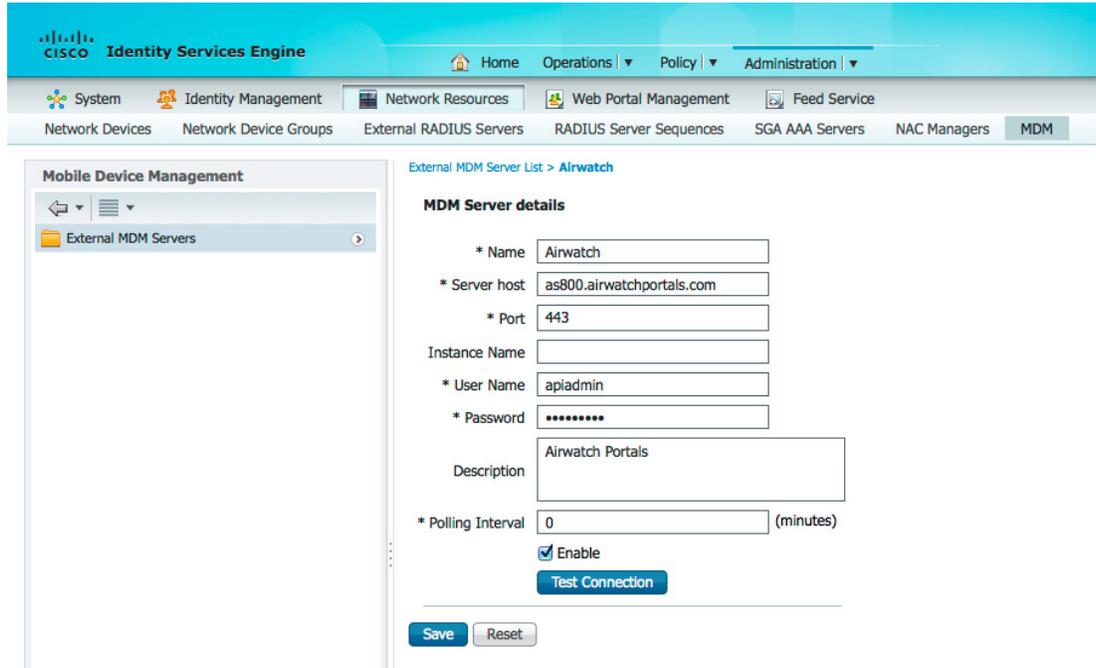


Add MDM Server to ISE

Once the account has been defined on the AirWatch MDM server with the proper roles, ISE can be configured to use this account when querying the MDM for device information. ISE will contact the MDM 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 MDM server.

As shown in [Figure 8](#), the URL for the AirWatch server is the same as the admin page and used earlier to export the certificate. The directory path is handled automatically by the system and is not specified as part of the configuration. The Instance Name field is used in multi-tenant deployments more commonly found when subscribing to a cloud service. The field should be left blank unless the cloud provider has instructed otherwise. The port should be configured for HTTPS (TCP port 443). The MDM cannot be configured to listen on a specific port for API users and any change will also impact both the admin and user portal pages.

Figure 8 Configure the MDM API on ISE



293791

The polling interval specifies how often ISE will query the MDM for changes to device posture. Polling can be disabled by setting the value to 0 minutes. Polling can be used to periodically check the MDM compliance posture of an end station. If the device is found to be out of MDM compliance and the device is associated to the network, then ISE will issue a Change or Authorization (CoA) forcing the device to re-authenticate. Likely the device will need to remediate with the MDM although this will depend on how the ISE policy is configured. Note that MDM compliance requirements are configured on the MDM and are independent of the 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.

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 window, 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 overage charges. In this case, blocking network access based solely on this attribute would aggravate the MDM compliance condition and run counter the device administrator's intentions. In addition, the CoA will interrupt the user WiFi 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 attained. If the polling interval is set, then it should match the device check-in period defined on the MDM. 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 no less than half this value. Oversampling the device posture will create unnecessary loads on the MDM server and reduced battery life on the mobile devices. There are other considerations with respect to scan intervals. Changing MDM timers should be done only after consulting with AirWatch's best practices.

The **Test Connection** button will attempt to log in to the API 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 MDM will not be active.

Verify Connectivity to MDM

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 AirWatch. The last message shown confirms a successful connection.

Table 1 Connection Messages

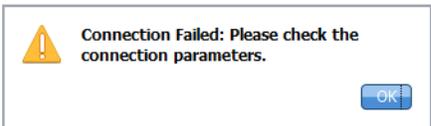
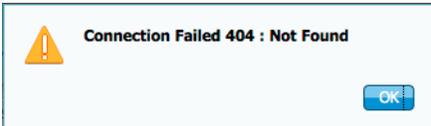
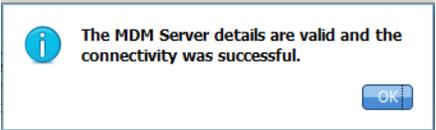
Message	Explanation
	A routing or firewall problem exists between the ISE located in the data center and the MDM located in either the DMZ or Cloud. The firewall's configuration should be checked to confirm HTTPS is allowed in this direction.
	The most likely cause of an HTML 404 error code is that an instance was configured when it was not required or that the wrong instance has been configured.
	The user account setup on the AirWatch 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.
	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 AirWatch server returning an HTML code 401 to ISE.

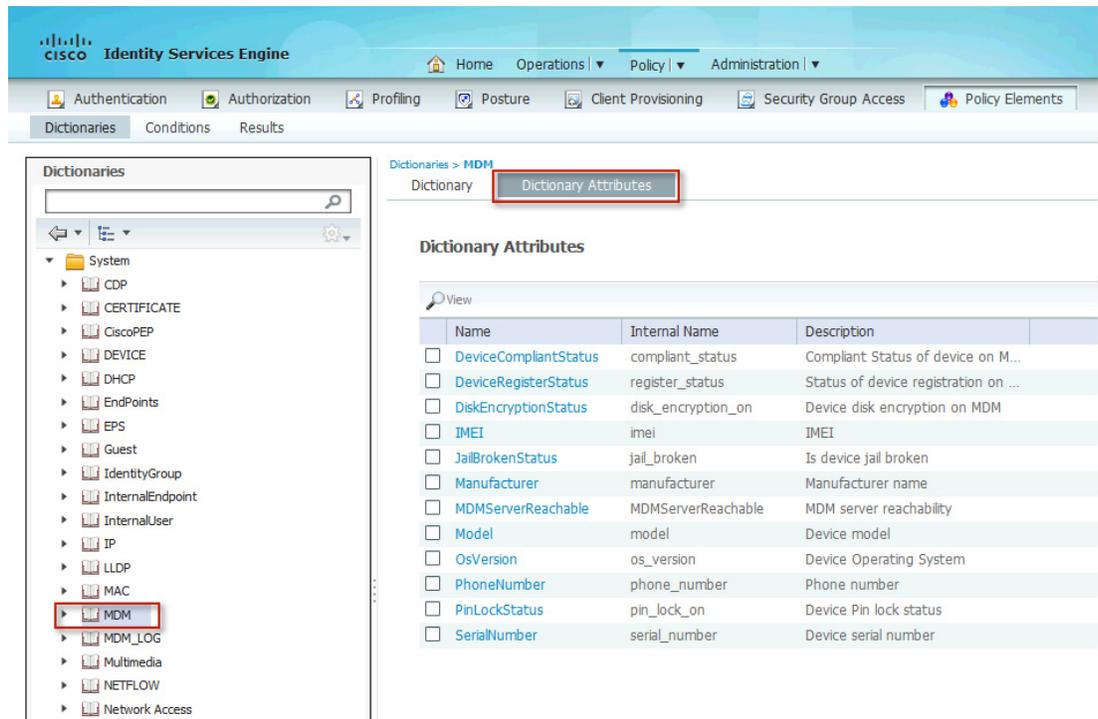
Table 1 Connection Messages

Message	Explanation
	ISE does not trust the certificate presented by the AirWatch 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 connection has successfully been tested. The administrator should also verify the MDM dictionary has been populated with attributes.

Review MDM Dictionaries

When the AirWatch MDM becomes active, ISE will retrieve a list of the supported dictionary attributes from the MDM. Currently AirWatch supports all of the attributes that ISE can query. The dictionary attributes are shown in [Figure 9](#).

Figure 9 Dictionary Attributes



293798

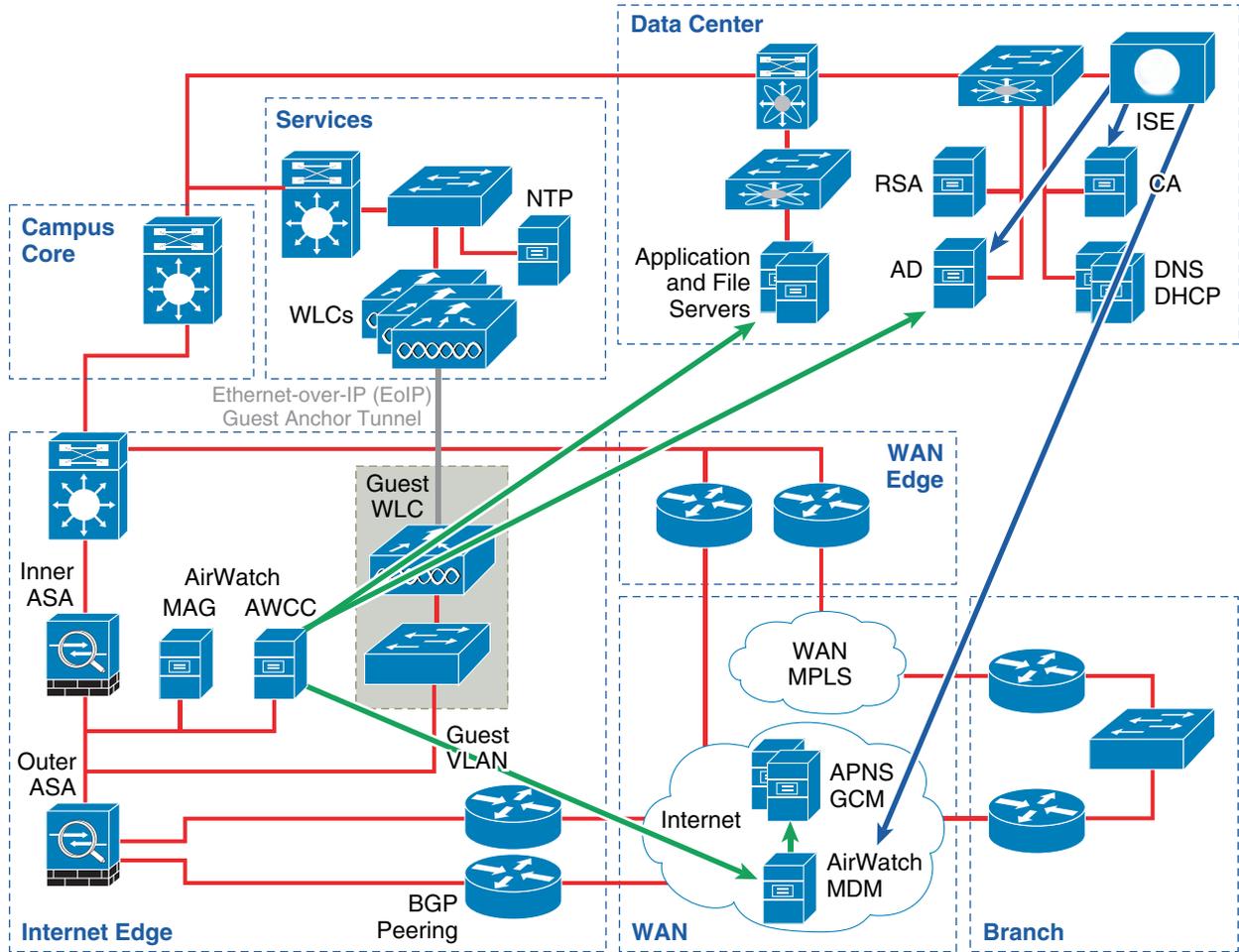
Enterprise Integration

Both ISE and MDM must be integrated into a common enterprise environment. At the basic level, this involves sharing the same directory structure. A common directory simplifies the operational aspects of the overall system, but also allows a consistent policy structure around AD group membership. For example, if a user is a member of the FULL_ACCESS group, that membership should result in a policy from both ISE and MDM that is consistent with the group and cognizant of the other component. For example, if the MDM installs an application on a device, then ISE should allow the application on the network for members of that AD group.

AirWatch offers an Enterprise Integration Service (EIS) in version 6.3 and below, or the AirWatch Cloud Connector (AWCC) and Mobile Access Gateway (MAG) in version 6.4 and above, to easily integrate the AirWatch solution with existing enterprise systems. This is ideally suited for the cloud model, but could also be used in on-premise scenarios where the AirWatch server resides in the DMZ, but does not have access to all enterprise services, such as the directory or Microsoft Exchange.

For the remainder of this section, a cloud model is assumed. The AWCC runs on top of a Microsoft IIS deployment typically dedicated for this purpose. Unlike the EIS service that accepts inbound HTTPS connections from the cloud, the AWCC initiates outbound sessions. In both cases, requests are processed locally and the results are returned to the server. Once set up properly, the admin can then configure select services in the cloud as if the MDM server was located on-premise, including the use of locally significant domain names. AirWatch AWCC can be deployed in a DMZ-Relay model as discussed here and shown in [Figure 10](#) or in a reverse-Proxy model. The AirWatch documentation explains both models.

Figure 10 Typical Cloud Deployment Model



Socket Requirements

There are several flows that need to be allowed between the various components. The full list is available from Airwatch. [Table 2](#) summarizes the required sessions.

Table 2 Common Socket Requirements

Source	Destination	TCP Port	Purpose	Comment
MDM	APNS	2195	Apple Push Notification	Cert Required
MDM	APNS	2196	Apple Push Feedback Service	APNs Message Status
MDM	GCN	5228	Google Cloud Messaging	
MDM	LDAP (sLDAP)	389 (636)	Directory	
Mobile Device	ISE	8443	Captive Portal	On-Boarding, Remediation

Table 2 **Common Socket Requirements**

Source	Destination	TCP Port	Purpose	Comment
Mobile Android Device	GCM	5228	Google Cloud Messaging	
Mobile iOS Device	APNS	5223	Apple Push Notification	

The installation is straightforward and fully documented by AirWatch. All of the information needed, including code, can be found on the EIS or Cloud Connector system settings page, as shown in [Figure 11](#). The administrator has the flexibility of selecting which services are off-loaded to the ISE and which are not. Airwatch does provide a migration path to customers running earlier code that will allow EIS settings to be transferred to the Cloud Connector.

Figure 11 EIS Configuration

Organization Group
SDU Team

System / Enterprise Integration

Enterprise Integration functionality has been upgraded.

Cloud Connector will now be used to provide integration services and Mobile Access Gateway will provide a secure communication channel for devices to access corporate resources. You can continue to use Enterprise Integration Services (EIS), or you can transfer your current EIS settings to Cloud Connector. Transferring your settings will automatically disable EIS. Any services relying on EIS will be unavailable until Cloud Connector is installed on servers previously hosting EIS or until EIS is re-enabled.

Transfer Settings

Current Setting Inherit Override

To enable this feature:
1. Download and install the [AirWatch EIS Installer](#) to a server attached to your network.
2. For help with configuring, refer to the [Enterprise Integration Installation Guide](#)

Enable Enterprise Integration Service

EIS URL* **Verify**

Ignore SSL Errors

Authentication Certificate AirWatch Cert & HTTP Auth

Enterprise Services

Select which Enterprise services you want to enable through EIS

- SMTP (Email Relay)
- Directory Services (LDAP / AD)
- Microsoft Certificate Services
- Simple Certificate Enrollment Protocol (SCEP)
- Exchange Powershell
- BES
- OpenTrust CMS Mobile
- Entrust PKI
- Symantec MPKI
- Syslog

AirWatch Services

Select which AirWatch components should use EIS

- Device Services
- Device Management (Enrollment, App Catalog)
- Self-Service Portal
- All Other Components

EIS Certificate **DC659B538DAE702E597A1273B35DE813EB2EEB87**

AirWatch Certificate **35F39605FED49327F01A2A9C05C5629BD9072930**

Clear Certificates

[Export settings for the Enterprise Integration Server](#)

Child Permission* Inherit only Override only Inherit or Override

On-premise deployment models do not require an AWCC. Instead, the AirWatch MDM server is located in the DMZ rather than the EIS server shown above. The server will still need to reach the Apple Push Notification Service (APNS) and Google Cloud Messaging (GCM) services over the

293800

public Internet. It is possible to leverage the AWCC if the enterprise security policy does not allow LDAP or Secure-LDAP from the DMZ. In this case, the AWCC is located in the DC and establishes a session to the MDM server in the DMZ. The AirWatch Administrator’s guide provides additional information, including other deployment models better suited to specific environments. Finally, the firewall policies must allow the MDM access to both APNS and GCM servers and is also detailed in the AirWatch admin guide.

Active Directory/LDAP Integration

With either an on-premise or cloud model, integrating ISE and the MDM to a common directory is important for the overall operations. One benefit is the ability to set a requirement that a user periodically change their directory password. If the MDM were using a local directory, it would be nearly impossible to keep the accounts synchronized. But with a centralized directory structure, password management can be simplified. The main advantage is the ability to establish complementary network and device policy base on group membership. The CVD provides examples of how groups can be used to establish a user’s entitlement to network resources. Likewise, the same group membership can be used to differentiate access to device resources and mobile applications.

AD Group Memberships

Three possible AD groups are presented in the CVD to illustrate their usage—Domain Users, BYOD_Partial_Access, and BYOD_Full_Access. ISE establishes the device’s network access based on the associated user’s membership.

Figure 12 shows the policies presented in the CVD.

Figure 12 CVD Use Policies

Policy	AD Group	Compliant		Permission	
		ISE	MDM		
Personal_Full Access	BYOD_Full_Access	YES	YES	Full	
Personal_Partial Access	BYOD_Partial_Access	YES	YES	Partial	
Personal_Internet Only	Domain Users	YES	YES	Internet Only	
Corporate Devices		YES	YES	Full	

These groups can be extended to the MDM such that members are issued profiles that complement their level of network access. As an example, Table 3 shows some arbitrary policies that can be established and enforced based on the CVD use cases.

Table 3 Policies Based on CVD Cases

Ownership	User Group	Restrictions
-----------	------------	--------------

Table 3 Policies Based on CVD Cases

Employee-Owned Device	Domain Users	Internet Only, personal devices are not required to on-board with the MDM.
	BYOD_Partial_Access	Fairly restrictive policy that isolates corporate data into containers. Restrictions prevent users from disabling the policy.
	BYOD_Full_Access	Trusted users are offered a slightly less restrictive policy. Corporate data is still isolated in containers.
Corporate-Owned Device	All Users classes	Very restrictive device policy disabling non-essential business functions such as the game center.

Domain Users is the default AD group. By definition, every user defined in the directory is a domain user. While it is possible to create the reciprocal group on the MDM, it is not needed. The CVD treats non-domain members as temporary guests. These guests are unlikely to need MDM management. More important, if a user is not a domain member, then the MDM administrator will need to define a local user account. This is likely a very small set of users that are handled as an exception, such as distinguished guests. Domain Users are essentially everyone with an account on the MDM, including members of BYOD_Partial_Access and BYOD_Full_Access.

MDM profiles and ISE AuthZ rules are fundamentally different with respect to AD Groups. ISE policy may include the AD group match as a condition for establishing a specific and single policy. MDM profiles are not a singular result. Most devices will be provisioned with multiple profiles based on various attributes. Members of the BYOD_Full_Access and Domain Users groups can each be configured for a specific profile. But if a user happens to have membership in both BYOD_Partial_Access and BYOD_Full_Access, then that user's device is provisioned with both profiles. In addition, everyone will be provisioned with basic security restrictions. ISE will check the device to ensure these restrictions are met before granting network access. These restrictions establish ISE compliance and are defined here as required PIN lock, encrypted storage, and non-jail broken or rooted devices.

MDM Profiles

Apple and Android differ in how device management is implemented.

Apple defines profiles that are an important concept of mobile device management. They are a foundational component of Apple's mobile device management protocol that is implemented by the operating system. This concept can be extended to application profiles, but as discussed here, they are found under the settings of the device. Each profile can contain one or more payloads. A payload has all the attributes needed to provision some aspect of built-in system functions, such as PIN lock. One special payload is the MDM payload that defines the MDM server as the device administrator. There can only be one MDM payload installed on any device. In iOS 5 and earlier, the profile containing the MDM payload cannot be locked and the user is free to delete it at any time. When this occurs, all other profiles installed by the MDM are also removed, essentially resulting in a corporate wipe. The MDM may lock any profile that it installed to prevent the user from removing them individually. The MDM is allowed to inspect other profiles such as the WiFi profile installed by ISE, but is not allowed to remove any profile that it did not install, including the WiFi as detailed in the BYOD CVD. Because multiple profiles can be installed on a device, and profiles have payloads, it is possible to have a payload collision. Devices with multiple security payloads will install all the payloads by aggregating the most secure settings from each.

In most other cases the first payload is installed and subsequent payloads are ignored or multiple payloads are accepted. For example, the device can have multiple VPNs provisioned but only one can be named XYZ.



Note

Starting in iOS6, Apple does allow the MDM payload to be locked if the user has not set a PIN lock.

Android devices generally implement device management functions through a specific set of APIs, most of which are manufacture or model specific. For example, Samsung uses their SAFE API, while HTC uses its One APIs.

MDM profiles can be applied to devices associated to users that belong to a user group. Configuring this with AirWatch first requires the creation of the user group. Afterwards, a profile can be restricted to that user group. This is shown in [Figure 13](#).

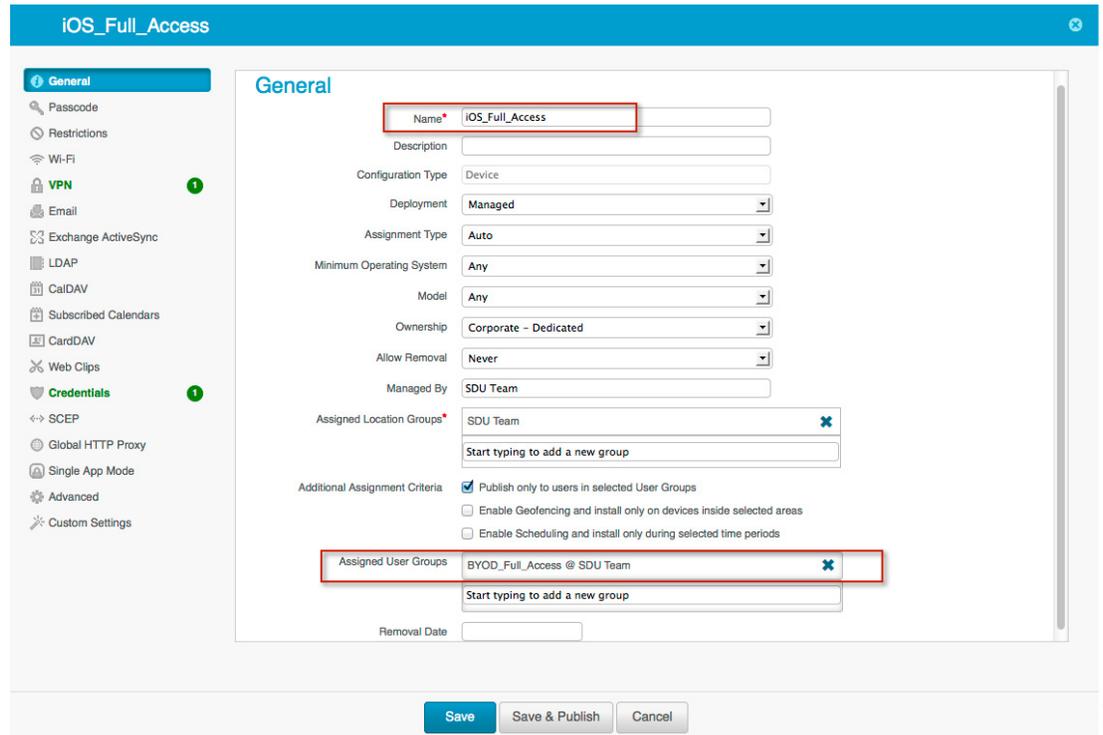
Figure 13 *Configure AD User Groups*

The screenshot shows the 'Add User Group' configuration page. At the top, there's a blue header with the text 'Add User Group'. Below it, there are several input fields and a search button. The 'Type' dropdown is set to 'Directory'. The 'External type' dropdown is set to 'Group'. The 'Search Text' field contains 'BYOD' and is highlighted with a red box. To the right of this field is a 'Search Again' button. Below the search field, there are three text input fields: 'Directory Name' with the value 'dc-addc-1.sdulab.com', 'Group Base DN' with the value 'DC=sdulab,DC=com', and 'Group Name' which has a list of options: 'BYOD_Advanced', 'BYOD_Full_Access' (highlighted in blue), 'BYOD_Partial_Access', and 'TESTBYODFULL'. Below these fields is the 'Distinguished Name' field with the value 'CN=BYOD_Full_Access,CN=Users,DC=sdulab,DC=com'. At the bottom, there are two sections: 'Location Group Assignment' with a checkbox 'Enable automatic Location Group assignment for users in this User Group' which is unchecked, and 'New User Group Settings' with two radio buttons: 'Apply default settings' (selected) and 'Use custom settings for this user group' (unchecked).

With the group created, the profile can be bound to the group, as shown in [Figure 14](#).

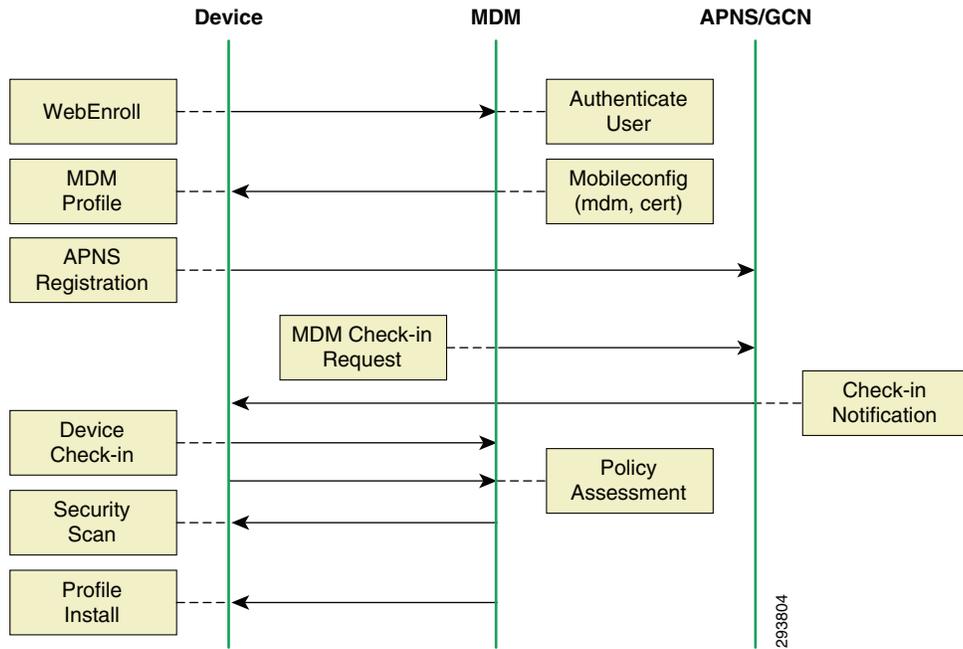
293802

Figure 14 Binding Profiles to User Groups



With the example configuration shown above, users that belong to BYOD_Full_Access will see either four or five profiles installed on their devices. Two profiles installed by ISE and two or three from the MDM. The MDM server will install the MDM payload during the on-boarding process. After that profile has been installed, the device will be issued a check-in request via APNS or GCM. When the device responds to the push notice, it will connect to the MDM where any additional profiles are installed. In our case, this includes at least the base restriction profile. If the user belongs to either BYOD_Full_Access or BYOD_Partial_Access, then an additional profile will be installed specific to that user group. [Figure 15](#) shows the steps required of a device to enroll with the MDM.

Figure 15 Enrollment Network Flows



SCEP

The AirWatch MDM can provision certificates onto the device via SCEP. This allows profiles to contain a payload that provisions a service that requires authentication via a certificate and another payload contains the associated certificate. One such example is VPN payload for either AnyConnect or Cisco IPsec. This is discussed in more detail as part of the applications section. Cisco ISE also uses SCEP to install user certificates for the WiFi profile.

Mobile Client Application

With Apple devices, the majority of MDM features are implemented directly through the operating system and do not require a mobile device client application. However some of the advanced functionality does require a client running on the endpoint. In particular, jailbreak and rooted detection requires the MDM client. Because ISE depends on these features for policy enforcement, corporate devices and personal devices with partial or full access should include a profile that specifies the AirWatch client as a mandatory application. By default, the user is not required to install any applications on the device. AirWatch client software is required to provide location information that can be used in geo-fence policies and push based notifications to the device.

With Android devices, the client application is required to enroll with the server. Starting in release 6.4, users will be re-directed to Google Play during the enrollment process so that the AirWatch client application can be installed. With Apple devices, the client application can be installed by the user directly and used to on-board the device. Or the mobile client can be pushed to the device as a mandatory application during on-boarding.

In addition to providing specific device information, the client application offers the end users some useful information concerning the status of their devices. Users can determine if the device is successfully communicating with the server, whether the device is compliant, and among other things, the IP address of the WiFi interface. The mobile client also has activity logs that the user can view.

One useful feature of the client application is the ability to manually refresh the device's posture to the server. The need arises when the device has been placed in MDM quarantine due to a compliance violation. For example, the device may not have a PIN lock when one is required. When the user configures the device with a PIN lock, the phone's OS will not trigger an update to the MDM agent. The agent will detect the change during the next security scan interval. Only then will the server discover this the next time the device is polled. This could result in ISE continuing to place the device in quarantine ever after the user has corrected the issue. Rather than waiting for the MDM to poll the device for an update, the user could use the mobile application to send the current data to the server. [Figure 24](#) shows the send data button on the mobile client.

In addition to the mobile device client application, AirWatch also offers a Secure Content Locker application that can receive push messages from the MDM server. The majority of administrators will deploy both the mobile client application and the secure content locker.

Device Ownership

One of the key components of BYOD is the mix of personal devices and corporate devices on the network and the ability to establish policy based on this attribute. Both the ISE and the MDM have the concept of asset classes. This allows corporate devices to be distinguished from all other devices in the system. Ownership is an important aspect of BYOD. For example, AirWatch recommends that support staff should not be allowed to issue a Full_Wipe of personal devices or track the location of a personal device. However, corporate devices may get full wipes as a matter of normal operation and may be used to track location, especially if travel is a key component of the job. Having the ability to handle the information gathered from personal and corporate devices differently is important.

In this first release of the MDM dictionary, there is not a tight integration between assets classes defined on ISE and those defined on the MDM. The API does not support such a device attribute. Complicating matters somewhat is the key index used to identify a device: ISE uses the device's MAC address, which is unique across the network, while AirWatch uses the device's UDID, which is globally unique.

ISE determines corporate devices through an identity group referred to as the Whitelist, which contains the MAC addresses of corporate assets. Discovering the MAC address of Android and Apple devices is typically a manual process. Apple lists the MAC on the Settings > General > About page. AirWatch does allow devices to be bulk-imported into the system using a device UDID. An enterprise may need to create a list of corporate MAC addresses and the associated UDIDs to pre-provision them as corporate devices on both systems. Apart from bulk imports, another option for daily operations is device staging. This allows an administrator the ability to on-board devices on behalf of users during which time the device can be declared as a corporate asset in both systems.

Organization Groups

The AirWatch MDM is built around a concept of inheritance. Child groups inherit attributes from the parent group, providing a powerful way to manage assets. The concept is a familiar organizational structure and can be used to establish both user and device policies. A full

understanding of how inheritance is applied to policy is required before configuring the MDM and is beyond the scope of this document. However, the basic concepts are introduced here to advance the CVD use cases presented earlier.



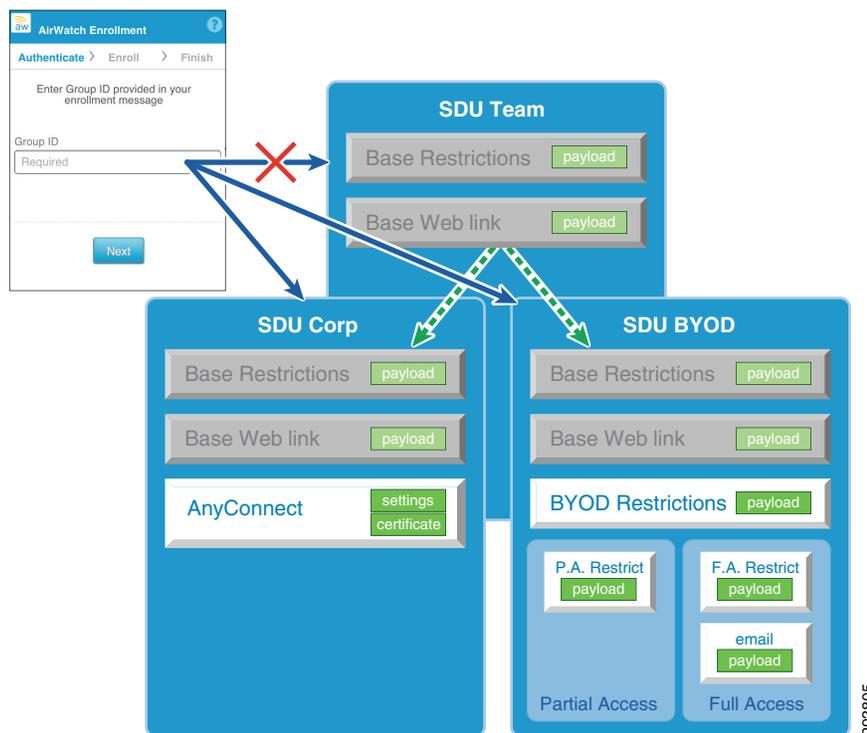
Note

This example is presented here to illustrate how locations groups could be used to build policy structure. There are many choices and this approach may not be appropriate in every production environment.

By default, all deployments start with a global organization group that has a set of attributes that define the system. This includes attributes like the APNS certificates and possibly the EIS component. Below that, [Figure 16](#) shows two child organization groups defined as containers: SDU Corp and SDU BYOD containing corporate devices and personal devices respectively.

Policy is now defined at two levels: at the highest level, global restrictions are defined. Both corporate and personal devices inherit these policies. Below that, specific policies for corporate and personal devices are defined with the respective organization group. At this level, the policies are further associated to user groups defined in AD. Devices in SDU BYOD associated to a user with membership to BYOD_Partial_Access will have policy specific to that user on that device. The same user in the same AD group may also register a corporate device that will be provisioned with different profiles that reflect both the user group and device ownership. [Figure 16](#) shows how inheritance is being used to implement the use cases presented in the CVD for the fictitious company SDULAB. In addition, the illustration shows that devices will enroll either with the SDU Corp group or the SDU BYOD group, but should not enroll in the parent group SDU Team.

Figure 16 Organization Group Structure



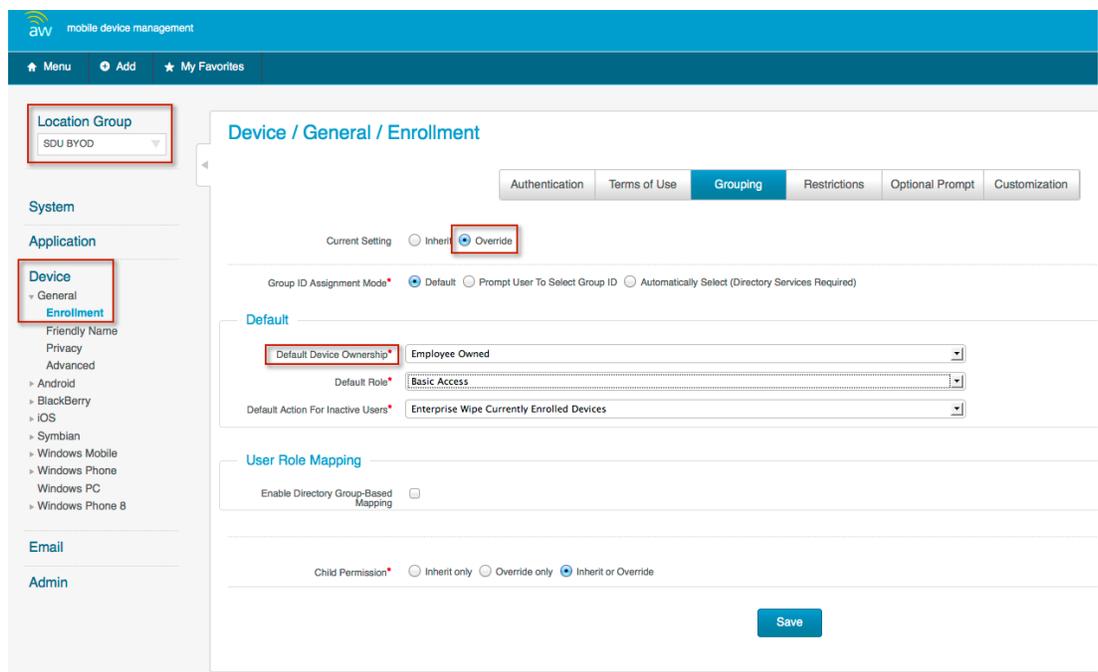
A key component is the configured default ownership of the group used by employees to enroll a device. Devices enrolled in the SDU Corp group will be marked as corporate devices, while devices enrolled in the SDU BYOD group are marked as personal devices. The group ID is provided to the user. Each

organization group can be protected by a one-time token to help ensure users are adhering to the intended purpose. Setting up organization groups will require additional guidance from the AirWatch support team. Only those components that are relevant to the use cases are shown within this guide.

Configuring the organization group with a default ownership allows employees the ability to on-board both corporate and personal devices. This minimizes the involvement of IT and associated support costs, yet still provides a MDM policy that distinguishes between ownership and users. IT will still need to populate the ISE whitelist with corporate MAC addresses.

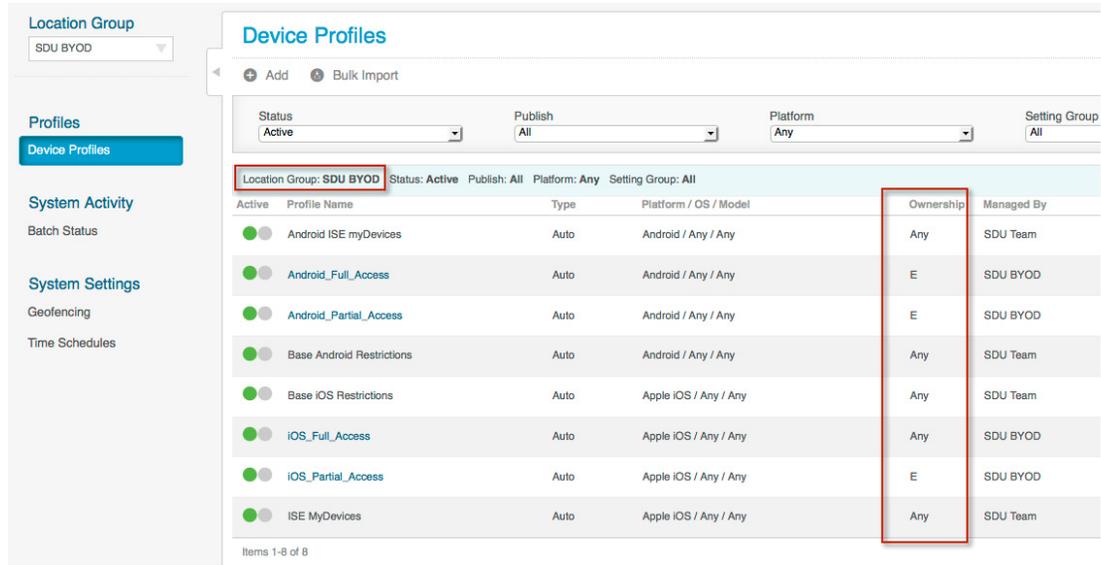
Default ownership is configured as part of the device general enrollment settings. These are found under the system settings page. [Figure 17](#) shows the SDU BYOD organization group being configured such that any device enrolled to this group will have a default ownership set to Employee Owned.

Figure 17 Default Ownership Associated to an Organization Group



A similar group is setup for corporate devices, except that the default ownership is set to corporate. Once these groups are in place, the administrator is free to establish profiles at the appropriate levels. Profiles can now be associated to users of an AD group, such as the default group Domain Users, and the two specific groups, Partial_Access and Full_Access. [Figure 18](#) shows profiles being applied in the SDU BYOD organization group. Profiles applied at this level are specific to employee owned devices. Note that some profiles are managed at the parent level, SDU Team, and are applied to all devices regardless of ownership.

Figure 18 Device Profiles Applied by Ownership



At each level in the hierarchy, there maybe a profile that contains a restrictions payload. For example, a member of SDU BYOD with an AD membership of BYOD_Partial_Access will get a restrictions payload from that group that prevents devices from syncing documents with the iCloud. They will also inherit a restrictions payload from the parent group SDU Team that will set the ISE compliance restrictions, e.g., PIN lock, device encryption, and not compromised. When multiple restriction payloads are installed on a device, the device will aggregate the settings by keeping the more restrictive attributes. Since the enterprise-wide policy is for a PIN lock, the child organization groups are not required to repeat the PIN lock requirement and can focus on what makes that profile unique for that particular set of devices.

Table 4 Device Policies at the BYOD Subgroup Level for Personal Devices

Profile	PIN Lock	Encryption	No iCloud Sync	Restriction A	Restriction B	Restriction C
SDU Team	X	X		X		
SDU BYOD			X	X		X
Result	X	X	X	X		X

User Experience

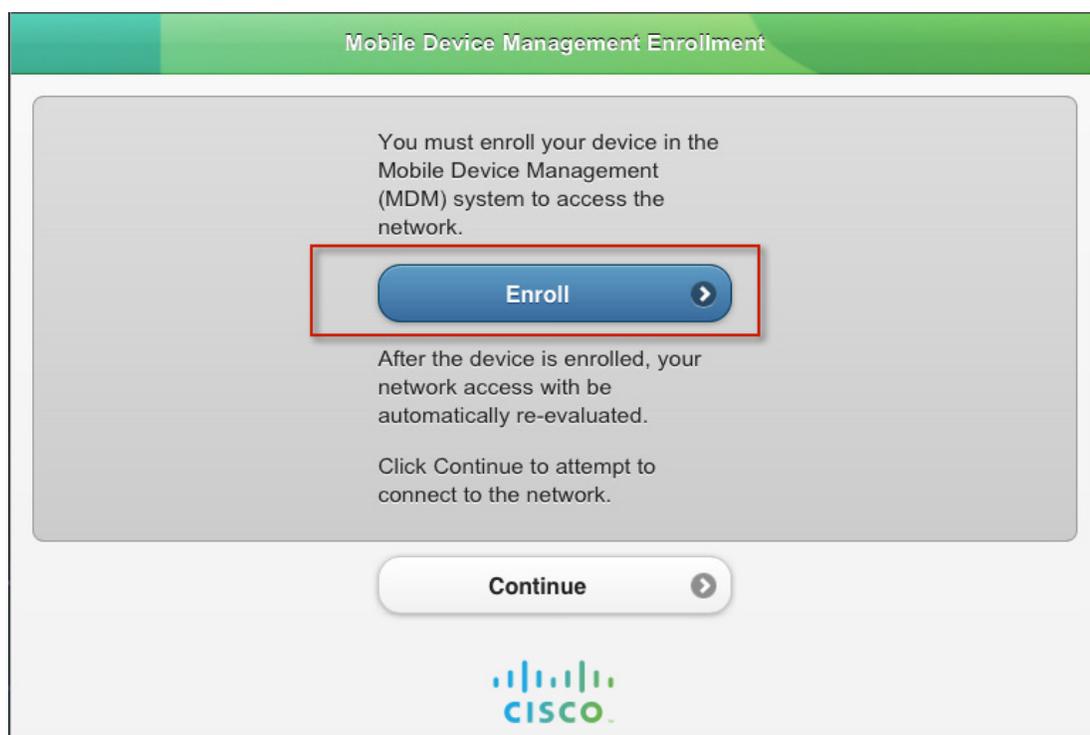
For the most part, the fact that a device is under management is seamless to the user. If they are running the mobile client application, as recommended for ISE compliance checks, then the user will have some additional information about their device that will be useful for troubleshooting with ISE. The initial user experience revolves around self-enrollment also known as on-boarding.

MDM Enrollment

The workflow that users must complete to on-board their device is set by the ISE policy. As presented in the CVD, the user will first on-board with ISE. When the user first joins the BYOD_Employee SSID, ISE will check the device’s MDM registration status through the MDM API. If the device is not registered, then a captive ACL is activated. This ACL will allow Internet access, but will capture any

attempts to access corporate resources. A full explanation is provided in the CVD. The device requires Internet access to complete the MDM on-boarding process, including downloading the client application from either the Google Play Store or Apple's App Store. When the device is captured the user will be presented with a screen that includes two buttons. The first will redirect the client to the MDM registration page. The second button issues a CoA to force a re-evaluation of the AuthZ policy after MDM enrollment completes.

Figure 19 **MDM Enrollment**

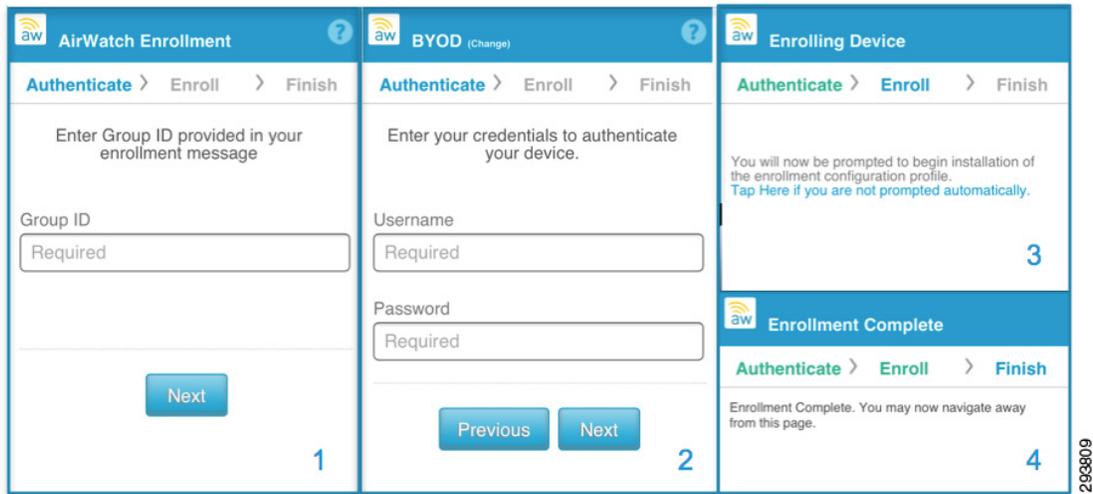


In version 6.3 Android users must load the AirWatch client application on their device prior to enrolling the device with the MDM server. This can be done from either the provisioning network or the employee network. However, it is not automatic. The enterprise will need to educate Android users of this restriction. Starting with AirWatch 6.4, Android users will be redirected to Google Play during the enrollment process to download the AirWatch client software. After installation, the user will configure the agent to point at the AirWatch server. When using a cloud deployment model, the server URL will typically start with DS (Device Service).

When the user lands on the AirWatch registration page, they will be asked for the Group ID, as shown in Figure 20. This is the tag that is bound to the organization group. Based on the discussion above, corporate and personal devices should on-board into distinct groups. Once a group has been selected, the user will move forward to authenticate to this group. The authentication method is group-specific. This can be used to ensure the user does not abuse the device ownership by on-boarding a personal device in the corporate group or vice-versa as discussed previously. If the user successfully authenticates, a profile including the MDM payload and associated certificate is installed on the device and the user is notified that the on-boarding process is complete.

The user is returned to the redirect where the “continue” button is used to re-evaluate the device’s MDM enrollment status, which should now be set to “enrolled”.

Figure 20 MDM Enrollment



After the device has enrolled, the server will request a check-in. During the initial check-in, additional profiles, applications, or Web Clips will be provisioned on the device. Web Clips are HTML bookmarks that are displayed as application icons on an Apple mobile device. Android devices simply call these bookmarks.

Pass Code Complexity

The user may be required to configure a PIN lock on their device during the on-boarding process if the device is not already configured with one. When this occurs, the user will need to launch the client app and send data. This is explained in more detail in [Device Compliance/Restrictions](#). The MDM administrator can choose the minimum password length and complexity. The natural tendency is to require very strong passwords, however there may be unintended consequences. The PIN lock will need to be entered any time the employee wants to use their phone. While texting and driving is illegal in many locations, the PIN lock is also required to make phone calls. If the user is required to navigate through several keyboards to enter the PIN lock, the administrator may be creating an environment of risk taking. There may be legal implications outside the scope of this document that should be considered. The more likely scenario is that the user will opt-out of the BYOD network for their personal devices. Devices not managed could have no PIN lock at all and yet still contain corporate data that the employee improperly put on the device. A practical approach is to require a simple 4 digit PIN on personal mobile phones. Corporate tablets can still be profiled with complex passcodes including special characters. This provides a balanced approach and will not discourage participation. Four digit PINs or the last four digits of a SSN are used fairly often to provide some level of security.

Application Stores

The AirWatch MDM server can install public applications from either the App Store or the Play store or private applications that are uploaded to the catalog. Applications developed with the AirWatch SDK may allow a provisioning profile. Cisco AnyConnect can be provisioned directly in the VPN payload as shown in the last section of this document. This is a two payload profile that is deployed along with the application. One payload is the AnyConnect settings, account information, group, etc. The second payload is the user certificate to authenticate with the ASA. Public applications can be part of a Volume Purchasing Program (VPP) where the enterprise can purchase licenses in bulk.

Corporate Data

AirWatch and ISE can work closely together to create a fairly comprehensive approach to managing corporate data. This is generally known as data loss prevention (DLP). Data comes in two forms, data at-rest and data in-flight. Data at-rest is stored directly the mobile device and data in-flight is the movement of data. This can be extended to include moving data between two storage containers on the same device.

Data at-Rest

Android and Apple handle stored data differently. Android has an open file structure that allows content to be shared between applications. Security is provided through file permissions, which creates a tight and integrated environment. Many Android devices also support external and removable storage in the form of SD Cards. Apple iOS creates a storage environment for each application. When an application is deleted, the partition holding that application's data is also removed. AirWatch has implemented a Secure Content Locker (SCL) that is effectively a client application that can store corporate data in that application's storage structure. The data is encrypted. What sets the SCL apart is the ability to centrally manage and distribute content from a central location. The MDM server can place sensitive corporate data into this locker. This has the intended effect of negating the need for the employee to use email attachments to move corporate data to and from the mobile device. Once there, the data cannot be shared with other applications. The locker is equipped with a reader for most common file types. When combined with an email gateway, email attachments can be removed from the email, encrypted, and placed in the users SCL. The attachment, along with all files in the locker, can only be decrypted by SCL and therefore is not viewable outside of the locker.

Data in-Flight

Sharing data between applications is fairly common. Built-in system applications like Contacts can share their information. With Apple devices, the data is passed through the owning application. Apple iOS now provides privacy settings to control access to system data stores. The common thread with both Android and Apple is tight application integration. This functionality presents challenges when trying to contain data. The AirWatch Secure Locker prevents data sharing.

Certainly moving corporate data to and from the device is also concern. The most common tool is email attachments, although cloud storage services such as Dropbox and Skydrive are also a concern. AirWatch can blacklist these types of applications. This is most appropriate on corporate devices. ISE can deploy per-user ACLs through the Wireless LAN Controller to enforce this policy at the network level for both corporate and personal devices.

AirWatch has several approaches to email management. The most comprehensive is an email gateway. Other options include establishing a PowerShell administrator role when using a Microsoft Exchange environment. Finally there are tools available to secure Gmail and Google docs. These are detailed in the AirWatch configuration guides. In each case, network policy can be established with ISE to reinforce the device's application policy.

One final component of data security is the Web browser. AirWatch offers a browser that can be installed on the device. In conjunction, the system browsers can be disabled so that users cannot access them. The AirWatch browser operates in a restricted mode or a kiosk mode. In kiosk mode, the browser is restricted to a single home page such as the company WebEx Connect site. ISE can apply network policy to support the single Web destination approach. Restrictive mode does allow devices to navigate to other sites, but functionality such as copy and print can be restricted.

Mobile Content management is evolving. AirWatch has recently released additional features to support DLP in the latest version 6.4, including application tunnels to the mobile access gateway (MAG), Web client tunneling via the MAG, and secure collaboration via SCL to allow secure sharing between team members. Future releases of this document may explore this area in more depth. Further information regarding these features is available from AirWatch.

Corporate Wipe

Both ISE and AirWatch can remove corporate data from personal devices. AirWatch calls this an Enterprise wipe, while ISE refers to it as a Corporate Wipe. Other common terms used are selective wipe, or partial wipe. When ISE issues this command, it is forwarded to AirWatch via an API call. The MDM can then remove corporate applications using privileges granted to the MDM Profile. When these complete, the MDM profile is removed, which will remove all the associated sub-profiles. While it is also possible to leave some applications behind, all MDM profiles will be removed. Profiles not installed by the MDM are not deleted. This includes two profiles that were installed by ISE, one containing the CA certificate and the other containing the WiFi profile and user certificate. When an application is deleted, the associated data is also removed. This is especially effective when the Secure Content Locker has been deployed because it is a centralized location that holds sensitive corporate data. If a built-in application was disabled by the MDM, it will be restored.

The relationship between the MDM profile, sub-profiles, and applications is important to understand. [Figure 21](#) shows this relationship. The top two profiles were installed by ISE and will remain on the device after a corporate wipe has been issued. The remaining four profiles will be removed. The profile labeled MDM Profile/V_1 contains the MDM payload and the certificate used to sign the sub-profiles. This profile is used to remove applications and sub-profiles. Removing any application, such as the AirWatch SCL, will also remove the data associated with the application. The MDM Profile/V_1 is not associated to any specific organization group and is required to place the device under management. The profiles Base iOS Restrictions/V_10 and ISE MyDevices/V_1 were inherited from the SDU Team organization group. The profile iOS_Full_Access/V_3 was installed on this device from the SDU_BYOD organization group to a user belonging to the AD Group Full_Access.

Figure 21 *AirWatch Enterprise Wipe*



The mobile client application can be removed. However there may be cases where the administrator would like to leave the AirWatch client application on the device to allow an authenticated user to re-enroll the device. Corporate wipes by themselves do not blacklist the device from either the MDM or ISE. An ISE administrator, the MDM administrator, or the user from either the ISE My Devices Portal or the AirWatch myDevices page may issue a selective wipe. If a selective wipe is being issued as a result of an employee's termination, then additional steps must be undertaken, such as blacklisting the device with ISE and removing the user AD group memberships. This will prevent the user from re-enrolling the device. Optionally, the user certificate can be revoked on the CA server.

The final action is to force the user to re-authorize against ISE by disassociating them from the network. ISE release 1.2 now supports this directly from the Operations page, as shown in [Figure 22](#). The device may immediately try to re-associate, but will match the blacklist thereby denying the device network access. The user will not be able to self-enroll this particular device until IT has removed the MAC address from the blacklist.

Figure 22 Forced CoA from ISE

Initiated	Updated	Session Status	CoA Action	Endpoint ID	Identity	IP Address
2013-02-24 20:17:08.328	2013-02-24 20:17:14.127	Started	⚙️	68:96:7B:01:2E:11	user2	10.31.1.122
2013-02-24 20:14:09.368	2013-02-24 20:14:15.868	Started			user2	10.31.1.125
2013-02-24 19:58:52.596	2013-02-24 19:58:52.596	Authenticated			johnjo	
2013-02-22 14:10:25.803	2013-02-22 14:10:30.227	Started			D8:30:62:8E:AD:	10.31.1.130
2013-02-22 12:37:29.888	2013-02-22 12:37:34.848	Started		18:E2:C2:82:43:7F	18:E2:C2:82:43:7F	10.31.1.127

293811

MyDevices Portal

AirWatch offers a MyDevices portal that allows the user to manage their devices. User Roles are defined to provide various level of functionality, such as Find Device, Enterprise Wipe, or Device Wipe. These roles are typically applied to a user group. Web Clips are used to provide the user with a desktop shortcut. The Web Clip should point at <http://<AirWatchEnvironment>/mydevice/>. A sample page with all the roles enabled is shown in Figure 23. The AirWatch Administrator’s guide has additional information in the Device Management chapter listed under End User Self-Service.

Figure 23 AirWatch MyDevice Portal for Users

293812

ISE also provides a My Devices Portal as detailed in previous chapters of the CVD. Currently the two sites are distinct and not cross-linked. Some of the functionality does overlap such as the MDM actions. But users will likely want a Web Clip to both locations.

Verify Device Compliance

ISE Compliance versus MDM Compliance

There are two compliance checks required of the device. The first is defined by a policy configured on the ISE and specific to network access control (NAC). The other is defined on the MDM and specific to Mobile Device Policy (MDP). The use of an MDM to determine NAC is a fairly new concept, first supported in ISE 1.2. Mobile device compliance policy is an essential component of MDM and has context outside of network access. This is similar to NAC compliance prior to the integration of the MDM. Integrating the components together does not negate the need for two distinct compliance policies with meaning only within their respective context. The network administrator has to be careful not to confuse ISE compliance with MDM compliance with respect to NAC.

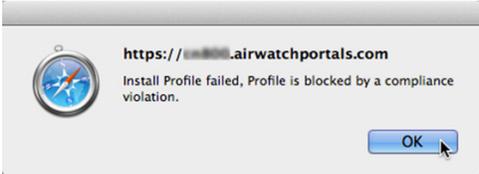
The attributes shown in [Table 1](#) should help clarify the difference between compliance policies.

Table 5 Compliance Attributes

ISE Compliance Attributes	AW Compliance Attributes
<input type="checkbox"/> DeviceCompliantStatus <input type="checkbox"/> DeviceRegisterStatus <input type="checkbox"/> DiskEncryptionStatus <input type="checkbox"/> IMEI <input type="checkbox"/> JailBrokenStatus <input type="checkbox"/> Manufacturer  <input type="checkbox"/> MDMServerReachable <input type="checkbox"/> Model <input type="checkbox"/> OsVersion <input type="checkbox"/> PhoneNumber <input type="checkbox"/> PinLockStatus <input type="checkbox"/> SerialNumber	<input checked="" type="checkbox"/> Application List Cell Data Usage Cell Message Usage Cell Voice Usage Compromised Status Encryption Interactive Profile Expiry Last Compromised Scan MDM Terms of Use Acceptance Model OS Version Passcode Roaming SIM Card Change

Before using the DeviceCompliantStatus attribute provided by the MDM, especially if the ISE administrator is not the MDM administrator, great care is needed to ensure network access is not restricted due to a non-related MDM compliance condition. The administrator must realize that MDM compliance is not specific to security concerns and that the MDM is responding to compliance conditions outside of the network domain. This is point is clarified in [Table 6](#) by looking at the available MDM responses to a non-compliant condition.

Table 6 MDM Responses

Action Type	Options
Profile 	<ul style="list-style-type: none"> ✓ Install Compliance Profile Block/Remove Profile Block/Remove Profile Type Block/Remove All Profiles
Notify	<ul style="list-style-type: none"> ✓ Send Email Send SMS Send Push Notification
Command	<ul style="list-style-type: none"> Request Device Check In ✓ Enterprise Wipe
Application	<ul style="list-style-type: none"> ✓ Block/Remove Managed App Block/Remove All Managed Apps

In addition, Airwatch’s compliance policy allows attributes to be logically combined. Finally, escalations are provided. AirWatch uses escalations to provide a measured response over time. For example, a typically MDM compliance policy might be:

If user approaches 80% of their text messaging plan, send an email. After one week, send another email, after one month send the manager an email, after three months, disable texting.

This compliance rule could be applied to specific users on specific devices.

During this time, the device will return an MDM non-compliant status to ISE over the API. Currently the MDM does not provide a method to mark compliance checks that are not reported to ISE. ISE cannot assert that network security issue caused a device to be MDM non-compliant.

Device Compliance/Restrictions

Restrictions and compliance are distinct but related concepts. A user is not offered the option of not adhering to a restriction. If a PIN lock is required, the device will be locked until the user selects a PIN that meets the established complexity. If the camera has been disabled, the icon is removed and the user has no way to launch the camera application. Restrictions are policy elements that are enforced without exception. Compliance is when a device is operating outside of the established policy. Non-restrictive

items that could cause compliance events are things such as the minimum OS version. The key point is that it is not possible to be non-compliant with a restriction. The exception is restrictions that include a grace period.

Device Scanning Intervals

The MDM client application can periodically scan the device. There are several different scans that run on different intervals. They are also available as device queries and are:

- **Device Information**—General information about the device includes serial numbers, UDID, phone number, operating system, model, battery status, etc.
- **Security**—Includes encryption status, device compromised, data roaming, and SIM card status and the number of profiles installed but not active.
- **Profiles**—The installed profiles on the device, including those not installed by AirWatch.
- **Apps**—A complete inventory of all the applications installed on the device.
- **Certificates**—A list of the installed certificates on the device.

Scan information is available in device details screen. When a device periodically checks in with the MDM server, it will notify the server of the current scan results.

PINLockStatus

The PINLockStatus is available to the API and can be used by ISE to set a minimum requirement for network access, as is shown in the CVD. Typically PIN lock is set as a restriction. But there are some cases where the MDM can set compliance check against a restriction, specific to PIN lock. It is possible to set a PIN lock with a grace period. During this time, the MDM can poll the device for the PIN lock status. When set, the triggered action could be the installation of additional profiles. By doing this, the device could be on-boarded with the MDM, but not granted full access until the user sets the password or the grace period expires.

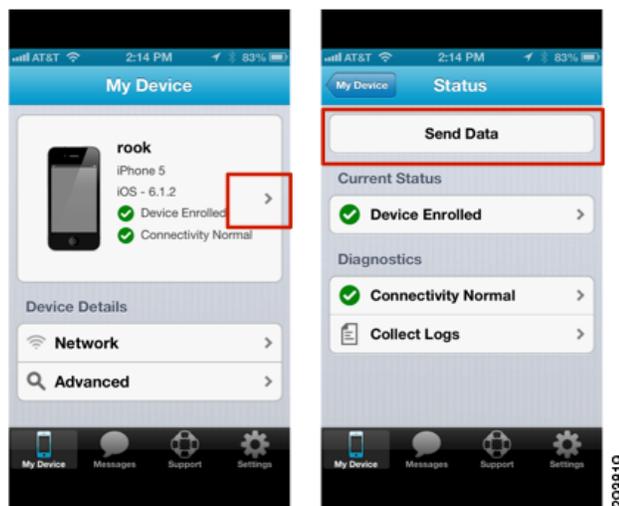
There are some caveats to be aware of with respect to ISE creating a PIN lock requirement for network access. These are not specific to AirWatch, however the work around is. When users are issued instructions explaining the on-boarding process, they should be asked to set a PIN lock on their device prior to starting the on-boarding process, rather than waiting for the forced PIN lock mid-way through the procedure. If the user does not follow this, they will likely end up in a quarantine state. There are two issues at play:

- First, the MDM server does not get a triggered update when a user creates a PIN lock. Because it is set as a restriction, the user is required to enter one, but it will be some time before the server will become aware of the PIN lock.
- Second, the MDM on-boards by installing the MDM profile and certificate first. This secures the communications between the server and device. After this profile is installed on the device, the server will send a check-in request to the device.

Because the MDM payload is required to respond to check-in messages, this confirms the device is fully under management. On the initial check-in, the device is loaded with the remaining profiles, including the one containing the PIN lock restriction. Before this completes, the user may have clicked the continue button on the MDM redirect page, resulting in a CoA. This will re-authorize the device before the user has been prompted to enter a PIN lock and the user will end up being quarantined. The work around it to open the AirWatch client and wait for any current scans to compete. The device should show in compliance, providing PIN lock has been included as a MDM compliance condition in addition to a

restriction. Once the client believes the device is compliant, the user should choose the “Send data” button as shown in Figure 24 to update the server of the new posture. Then the user can try the continue button again or bounce their wireless to force a re-authorization.

Figure 24 Manually Updating the MDM Server



Jailbroken or Rooted devices

These are devices where the user has gained direct access to the operating system, bypassing the control imposed on the device by the service provider. Devices in this state are generally considered compromised and there has been some recent legislative action to prohibit users defeating locks imposed on the device by the providers. The BYOD CVD offers a policy that does not allow jailbroken or rooted devices on the network. This is based on the MDM API. The MDM server will require a mobile client application installed on the device to determine the root status of the device. There are a few limitations to be aware of. Usually the process of rooting a device requires the user to reinstall the operating system. There is a good chance the user will uninstall the AirWatch mobile client at the same time. Without the software, the server cannot with certainty say the device is rooted, only that it has been compromised and is no longer under management. If the user also removes the MDM profile, then all of the child profiles are also removed with it, effectively resulting in a selective wipe. As a reminder, the MDM profile may not be locked. At this point, the user may attempt to on-board the device in a rooted or jailbroken state. The server will not be able to assess this condition until the mobile client is reinstalled on the device and has had a chance to complete at least one device scan. There is a time delay between when a device is first compromised and when the MDM server will be first aware of a problem. There is no requirement in the MDM protocol that a device should contact the MDM when the MDM payload is removed. The server is left to poll for the condition periodically. This delay can carry forth into ISE policy because ISE can only respond to the attributes as they are returned by the MDM.

RegisterStatus

When a device is being on-boarded, ISE will check the RegisterStatus attribute of the device via an API call to the MDM. If the device is not registered, the user is redirected to the AirWatch enrollment page. Obtaining a status of registered with the MDM means that the device is known to the MDM and that an

MDM payload and the associated certificate is on the device, and that the device has responded to at least one check-in request issued through APNS or GCM. A register status does not guarantee that all the profiles have been pushed to the device. Instead it indicates that the profile containing the MDM payload has been installed and that the device has responded to the initial check-in request. It is possible for profiles to be withheld until a posture assessment has been completed and reported back to the server. This could result in a registered device that is not equipped with the full set of intended restrictions.

Manage Lost/Stolen Devices

Corporate and personal devices require specific responses when reported lost or stolen. Personal devices reported as stolen should undergo an enterprise wipe to remove all corporate data. Lost personal devices may be handled in the same manner, although the user may attempt to locate the device from the myDevices page first, providing that service is allowed by the users role privileges and location services are enabled on the mobile device. The user or admin can also try to issue a “find device” if either the mobile client app or secure content locker is installed on the device. The device will emit a sound at period intervals to help the user locate the lost device. If the device remains lost after an attempt to locate it, then an enterprise wipe is prudent. The device can be restored if later found by the user. The admin may also choose to blacklist the device on the network depending on the situation, forcing the user to call support to regain access.

Corporate devices have some flexibility with respect to providing location information. If this information is available, then the administrator may have some options. They could choose to:

- Reassign the device to a secured organization group. This group effectively removes all corporate applications and data, provisions lock-down profiles, effectively rendering the device useless, and leaves the device under management such that forensic data is available in the event the enterprise would pursue legal options.
- Blacklist the device in ISE to prevent corporate access. Also issue an Enterprise Wipe command to the device to remove all corporate data. This also removes the MDM profile. The device will become unmanaged, lifting all operational restrictions on the device including the ability to locate the device.
- Blacklist the device in ISE to prevent corporate access. Also issue a Full Wipe to the device to remove all information and return it to the factory default configuration. The carrier will need to be involved to prevent the now factory fresh device from having a resale value.

The exact response an enterprise would take in the event of a stolen device should not be public knowledge, especially where a Full Wipe is issued since the response could be an incentive to some criminals.

Application Distribution

Applications can be marked as required or optional. Required applications are usually automatically pushed to the device. Users can browse optional applications using the AirWatch App Catalog on their device. Applications can be from the public application store or developed in-house. Apple and Google both offer a volume purchasing program if paid applications are distributed. In house, iOS applications developed with AirWatch’s SDK can be customized with application profiles. Application management will be explored in future releases of this document. Readers are encouraged to refer to the AirWatch Administrator’s guide for additional information.

Cisco Applications (Jabber, etc.)

Cisco offers a wide range of mobile business applications for both increased productive and security. [Table 7](#) shows some popular applications.

Table 7 Popular Cisco Mobile Applications

	AnyConnect—AnyConnect is a security application for improved VPN access, including on-demand domain-based split tunneling.
	WebEx—WebEx is a productive application to allow mobile users to connect to online meetings. The application allows content sharing, video sharing, and VoIP or cellular audio.
	Jabber—Jabber is a productivity application that integrates IP telephony, chat, and video conferencing using Cisco Call managers.

AirWatch allows users to pre-provision the AnyConnect application using an application profile. Users can be prompted to enter their username and password or the profile can include a certificate payload that can be used to authenticate the users. The provisioning is found as part of a VPN profile, as shown in [Figure 25](#).

Figure 25 AnyConnect Provisioning Profile

VPN

Connection Info

Connection Name* VPN Configuration

Connection Type* Cisco AnyConnect

Server* ignore.sdulab.com

Account {EnrollmentUser} ⓘ

Send All Traffic

Authentication

User Authentication* Certificate

Group Name TopSecretKey

Identity Certificate None

Enable VPN On Demand

VPN On Demand	Match Domain or Host	On Demand Action
	sdulab.com	Always Establish ⓘ

203823

Conclusion

The integration of the network policy enforced by Cisco ISE and device policy offered by AirWatch’s Mobile Device Manager provides a new paradigm for BYOD deployments where security and productivity are not competing objectives.

Disclaimer

The AirWatch configurations shown in this document should not be considered validated design guidance with respect to how the AirWatch MDM should be configured and deployed. They are provided as a working example that details how the case studies explored in the CVD can be carried forward to the MDM in an effort to provide a fully integrated and complementary policy across both platforms. This in turn will result in a comprehensive solution where the network and mobile devices are in pursuit of a common business objective. AirWatch is the only source for recommendations and best practices as it applies to their products and offerings.

