AIRWATCH MDM
SUPPLEMENTAL PROCEDURES

Version 1, Release 3

22 January 2016

Developed by AirWatch and DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. SECURITY READINESS REVIEW

1.1 General

When conducting an AirWatch MDM Security Readiness Review (SRR), the Team Lead and the assigned Reviewer identify security deficiencies and provide data from which to predict the effectiveness of proposed or implemented security measures associated with the AirWatch MDM.

1.2 Mobile Policy Review

Detailed policy guidance is available on the DISA Information Assurance Support Environment (IASE) website located at http://iase.disa.mil/stigs/mobility/Pages/policies.aspx.

Use the Mobility Policy STIG and the CMD Management Policy STIG to review the AirWatch MDM asset.

2. AIRWATCH MDM SOFTWARE SECURITY AND CONFIGURATION INFORMATION

2.1 AirWatch Architecture

The AirWatch MDM system architecture is installed entirely on the host DoD network and exists between the host system DMZ and internal network. Figure 2-1, below, shows the architecture of the AirWatch system that is approved for DoD networks and described within this STIG.

Figure 2-1: AirWatch Architecture

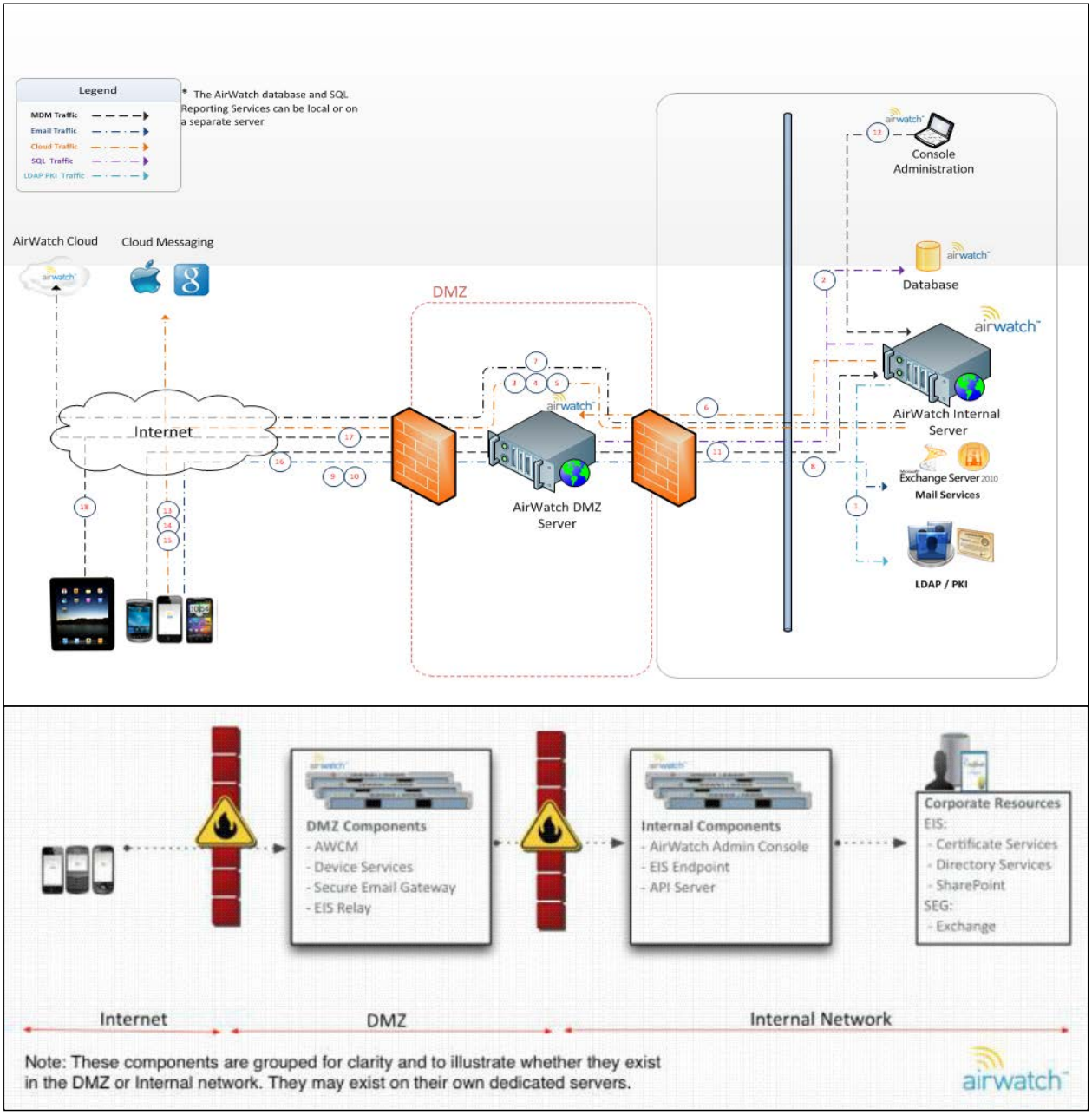

Table 2-1: AirWatch MDM Software Components

Component	Description
AirWatch Administration Console	The AirWatch Administration Console serves as the central portal where administrators log on to view and manage devices. On DoD networks, this server should be assigned an internal URL, and therefore only be internally (inside a corporate network) accessible. Consisting of an IIS application and multiple Windows Services, the web console can be hardware load balanced across multiple servers to allow for high availability and distributed load.
AirWatch Device Services	The Device Services server acts as the interface for the AirWatch system to all managed devices. This server is responsible for receiving check-ins and information updates, while also delivering any queued commands to managed devices. This server is made available to the public Internet to be accessible by devices with Internet access. Consisting of an IIS application and multiple Windows Services, the Device Services server can be hardware load balanced across multiple servers to allow for high availability and distributed load. This server should have an external URL and publicly trusted SSL Certificate bound to port 443 (HTTPS) so that mobile devices can access it via the Internet.
AirWatch Database	AirWatch stores all device and environment data in a Microsoft SQL Server database. Due to the amount of data flowing in and out of the AirWatch database, proper sizing of the database server is crucial to a successful deployment. (For recommended sizing contact AirWatch Professional Services prior to install.) Additionally, AirWatch uses Microsoft SQL Reporting Services to report on data collected by the AirWatch solution. This database server should be located on the internal network only, accessible by the AirWatch Administration Console and Device Services components, and depending on sizing requirements, may be installed on the same server as the AirWatch Administration console (though recommended installation is to have a separate server for the AirWatch database).

Component	Description
AirWatch Enterprise Integration Service (EIS)	The AirWatch Enterprise Integration Service provides organizations the ability to securely integrate with their back-end enterprise systems. It also provides a secure method for individual applications to access corporate resources. This integration allows organizations to leverage their existing LDAP, Active Directory, Certificate Authorities (external or internal certificate authorities for email, Wi-Fi, or intranet authentication as prescribed by applicable STIG), email, and other back-end systems as needed and prescribed by this STIG. (**Note:** AirWatch should not be connected to DoD shared drives or SharePoint resources unless specifically designated for use by mobile devices without CAC authentication capability).
AirWatch Secure Email Gateway (SEG)	The SEG server is a proxy that operates as an end-point for mobile devices to reach their host network Exchange mail system and was used in the testing and validation of this STIG. The SEG can be installed on the same DMZ server as Device Services, or load balanced and installed separately depending on anticipated traffic. (Consult AirWatch Professional Services to determine proper sizing). The SEG should be assigned a publicly accessible DNS name and SSL certificate bound to port 443 on the server's IIS service and acts as a proxy between mobile devices and the DoD Exchange Server component. This enables the following advanced security features in AirWatch Administration Console: • Detection and remediation of rogue devices connecting to email • Required mobile device management for email access • Advanced access control for administrators • Integration with the AirWatch compliance engine • Enhanced traffic visibility through interactive email dashboards • Certificate integration for advanced protection • Email attachment control and encryption
AirWatch Cloud Messaging server (AWCM)	AWCM streamlines the delivery of messages and commands from the console by eliminating the need for end users to access the public Internet and procure Google IDs. AWCM also serves as a comprehensive substitute for Google Cloud Messaging (GCM) for Android devices, meaning that the AirWatch Administration Console and Device Services components can manage devices directly from the DoD network without traversing the Google Cloud.

Component	Description
Organizations Enterprise Services (e.g., Active Directory, Certificate Services, etc.)	The AirWatch EIS component can be used to connect to several backend infrastructure components to make them available to administrators and mobile device users, but should only be used in conjunction with mobile devices that support CAC authentication to backend file systems and web servers. Information on how to apply these services is contained within the STIG and includes Active Directory and LDAP services, Certificate Authority services, and corporate content repositories. (**Note:** AirWatch should not be connected to DoD shared drives or SharePoint resources unless specifically designated for use by mobile devices with CAC authentication capability.)

2.1.1 Required Hardware Components

When deployed within an organization's network infrastructure, AirWatch can adhere to DISA security policies by storing all data on-site. In addition, AirWatch has been designed to run in virtual environments, which allows for seamless deployments on a number of different configurations. When determining the hardware requirements needed to build out an AirWatch environment, it is important to consider the number of managed devices, the device transaction frequency, the device check-in interval, and also the number of administrative users that AirWatch will be managing. It may also be beneficial to consider the growth potential of the organization’s device fleet as well. Below are the minimum hardware requirements for installation of the AirWatch MDM Software. Note that some AirWatch components can be installed on the same internal or external server as the AirWatch Administration Console or Device Services components. In these cases, hardware requirements should be added to provide proper support. For AirWatch hardware components and minimum requirements, please reference AirWatch installation and architecture guides provided with the AirWatch MDM Software.

2.1.2 Required Software Components and Installation Pre-Requisites

This section covers the required software setup for each listed server before the installation can occur. AirWatch MDM Software runs on a Windows Server 2008 R2 or Windows Server 2012 operating system with specific services installed and running. All services and the operating system should be properly hardened in accordance with their specific STIG. For AirWatch Software requirements, which are matched specifically to the size and anticipated data traffic of the environment, reference the AirWatch installation and architecture guides provided with the AirWatch MDM Software.

2.1.3 Required Firewall, DNS, SSL, and Configured Ports for AirWatch MDM Software

The AirWatch MDM Software requires bidirectional communication between the mobile devices under management and the AirWatch Device Services and SEG servers. This traffic occurs via port 443 on both servers and requires the usage of an organization-procured, publicly trusted

SSL Certificate. This SSL Certificate should meet the requirements of this STIG and be bound to port 443 via IIS on the applicable servers, and matched to the externally accessible DNS names assigned to those servers. This enables mobile devices to reach the services via the Internet and to be managed by the AirWatch MDM Software components.

Table 2-2: AirWatch MDM Software DNS, SSL, and Load Balancer Information

Requirement	Description
DNS Settings/Configuration	• External URL (DNS Record) resolving to the AirWatch DMZ server (Device Services). (**Note:** If SEG and/or EIS are located on separate servers, they must also be associated with this or another specific DNS Record that is externally accessible to mobile device users.) Should be associated with public IP address. • Internal URL for internal CAS/EAS server to relay traffic from the AirWatch SEG server. • Internal URL (DNS Record) resolving to the AirWatch Internal server (Administration Console).
SSL Certificate Settings	• Publicly trusted SSL Certificate to match the External DNS for the AirWatch DMZ server (bound to port 443 in IIS of Device Services server, SEG, or EIS). • SSL certificate to match the Internal URL for the AirWatch Internal server (Administration Console).
Load Balancer Settings (Optional)	• Load balancers are to be configured with a round robin load-balancing mechanism and SSL session persistence of 15-minute sessions. • Load balancers are recommended to redirect all HTTP requests to HTTPS. • SSL offloading supported for all services except API services. If offloading SSL, load balancer must forward secure cookies to and from the AirWatch servers.

Table 2-3: Internal Network Server (Administration Console) Firewall Port Numbers

Connection	Connection Type	Default Port Number
To/from internal Domain Controller for Active Directory Sync	HTTPS	389
To/from internal CAS or EAS for email policy control	HTTPS	443
To/from AirWatch Database (SQL) server for delivery/retrieval of database information	TCP	1443
To/from AirWatch Database (SQL) server for server reporting sync	HTTPS	443

Connection	Connection Type	Default Port Number
To Apple Push Notification Services (APNS) cloud for control of iOS devices DNS Names to reach: • gateway.push.apple.com • feedback.push.apple.com IP Addresses to reach: • 17.X.0.0/8	TCP	2195, 2196
To Apple iTunes cloud for assigning public applications to iOS devices through Administration Console DNS names to reach: • *.itunes.apple.com • *.phobos.apple.com IP IP Addresses to reach: • Any (IP addresses do not remain static)	HTTPS	443
To Cell Trust SMS for sending mobile devices SMS messages DNS name to reach: • gateway.celltrust.net IP Addresses to reach: • 162.42.205.0/2-4	HTTPS	443
To AirWatch DMZ Device Services Server DNS Name to reach: • {AirWatch DNS Server Name} IP Address to reach: • {AirWatch DMZ Server IP}	HTTPS	443
To AirWatch Cloud Messaging Server (occurs over port 2001, which is configurable). AWCM is typically installed on AirWatch DMZ Device Services server but can be installed on a standalone server. DNS Name to reach: • {AirWatch DNS Server Name} IP Address to reach: • {AirWatch DMZ Server IP}	TCP	443 (if installed on standalone server) or 2001 (if installed on same server as AirWatch Device Services)

Table 2-4: DMZ Network Server (Device Services) Firewall Port Numbers

Connection	Connection Type	Default Port Number
To internal CAS or EAS server (**Note:** If SEG is installed on DMZ Device Services Server. If SEG is standalone, this port only needs to be opened on that SEG server.) DNS Name to reach: • {Internal EAS URL}	HTTPS	443
To Apple Push Notification Services (APNS) cloud for control of iOS devices DNS Names to reach: • gateway.push.apple.com • feedback.push.apple.com IP Addresses to reach: • 17.X.0.0/8	TCP	2195, 2196
To/from devices for AirWatch Cloud Messaging Services (AWCM)	TCP	443 (if installed on standalone server) or 2001(if installed on same server as AirWatch Device Services)
To organization-chosen SSL Certificate Revocation List website	HTTP	80 (should be open to website provided by SSL Certificate issuing authority)
To AirWatch Internal Server (Administration Console)	HTTPS	443, 2010
To AirWatch Internal Database Server (SQL)	TCP	1433

Table 2-5: Mobile Devices (iOS and Knox) Firewall Port Numbers

(for configuration information see applicable MOS STIG)

Connection	Connection Type	Default Port Number
To Apple Push Notification Services (APNS) for iOS devices only DNS Names to reach: • #-courier.push.apple.com • gateway.push.apple.com IP Addresses to reach: • 17.X.0.0/8	TCP	5223

Connection	Connection Type	Default Port Number
To Apple iTunes Cloud for iOS devices only DNS Names to reach: • phobos.apple.com • oscp.apple.com • ax.itunes.apple.com IP Addresses to reach: • Any (IP addresses do not remain static)	HTTP/HTTPS	80, 443
AirWatch DMZ Device Services Server DNS Name to reach: • {AirWatch DNS Server Name}	HTTPS	443, 2001 (AWCM), 2010

2.1.4 Required AirWatch Service Accounts

Prior to installation and configuration of the AirWatch MDM Software, specific service accounts must be created to enable the system components to authenticate and transfer information to each other. These service accounts were tested during the validation of this STIG and should be referenced and created by using the chart below.

Table 2-6: Required AirWatch Service Accounts

Title	Description & Purpose	Permissions & Roles
AirWatch Database Server SQL Service Account	SQL service account to install the AirWatch database	• SQLAgentUser and DBdatareader roles
AirWatch Database Connection User SQL Account	SQL user account to send commands and information to the database	• db_datareader permission • db_datawriter permission • db_execute permission
LDAP Binding Account	Used for network Directory Services integration (e.g., Active Directory authentication). Client LDAP service account to authenticate binding requests into the Client LDAP directory for all users in the desired organizational unit.	• Read permissions (**Note:** Service account running app pools in IIS on AirWatch EIS server should also have these permissions assigned.)

Title	Description & Purpose	Permissions & Roles
Certificate Authority (CA) Service Account (optional)	Client CA service account to issue and revoke certificates from the CA.	Account roles and permission vary by CA type. Permission should be granted for the following: • Requires these permissions on the CA: o Issue and Manage Certificates o Request Certificates • Requires these permissions on the Certificate Template: o Read o Enroll

(**Note:** Some of the above accounts are optional depending on deployment requirements; contact AirWatch Professional Services for more information. Also contact AirWatch Professional Services if attempting to integrate BES, SCCM, or other services, and check applicable system STIG for specific requirements.)

2.2 Server Access Control

AirWatch MDM Software is installed on host network servers running Windows Server 2008 R2 or 2012 operating systems. As a result, all server-related requirements for Access Control, including Administrator Account creation (but not specific role management), and operating system updates and maintenance are managed by the host operating system.

The integrity of remote sessions between the AirWatch MDM Server is accomplished via SSL (SSL Certificate obtained by the organization as outlined in this document) and connections to the host AirWatch Administration Server, set to use an internal URL, occur over organization-approved methods such as VPN, which are separate from the AirWatch MDM Software system.

2.3 Information Auditing and Accountability

Audit and accountability on the host network servers, or any functions related to the functioning of the host server or network (e.g., traffic monitoring, firewall configurations, malware detection, etc.), are the responsibility of the host operating system.

2.3.1 AirWatch Syslog Output to External Auditing Systems

Information obtained and recorded in the AirWatch MDM Software system is able to be exported to an external auditing system via Syslog configuration in the AirWatch Administration Console:

1. Click on “Menu” on the top toolbar on the Administration Console home screen.
2. Click “System Configuration” under heading “Configuration”.
3. On the left-hand tool bar, click “System” and “Enterprise Integration” and select “Syslog”.
4. Verify or enter connection information to external logging server as needed.

2.3.2 AirWatch Reports and Events Logging System

The AirWatch MDM Software contains 91 available Report options, which are recorded automatically in the system when an SSRS system is used in conjunction with the AirWatch Database Server. These reports can be exported on-demand or subscribed to via email. To view AirWatch Reports:

1. Click on “Menu” on the top toolbar on the Administration Console home screen.
2. Click on “Reports” under the “Reports & Analytics” heading.
3. Click on the applicable Report to view, export, or subscribe to.

The AirWatch system also records all significant security events on the Administration Console and mobile devices. To view Events and sort by selected criteria:

1. Click on “Menu” on the top toolbar on the Administration Console home screen.
2. Click on “Events” under the “Reports & Analytics” heading.
3. On the left-hand tool bar, choose “Device Events” or “Console Events”.
4. Click on the applicable Event to view.

2.3.3 Device-Specific Logging

For device-specific logs, see the applicable MOS STIG. The recording of some information is not accessible over the air and is out of scope for the AirWatch MDM Software suite. To view specific device information recorded by the AirWatch MDM software, use the “Events” option above and view “Device Events” or view a device individually using the following procedure:

1. From the Administration Console home screen, locate the list of managed mobile devices on the lower half of the “Asset Tracking” screen.
2. Search for the device by using the search engine provided and click on “Friendly Name”.
3. View the applicable device information or click on “Friendly Name” in the top left corner to view more granular collected device information.

2.4 Mobile Device User Identification, Authentication, and Enrollment

To manage devices using AirWatch MDM Software, the mobile device must be “Enrolled” into the AirWatch system using a combination of AirWatch system criteria and Active Directory credentials. During this process, an MOS will automatically be provisioned and granted access based on the organization’s specified settings in the AirWatch Administrative Console.

2.4.1 AirWatch and Active Directory Sync

On DoD networks, the AirWatch MDM Software should be set up to use Active Directory for identification, authentication, importing of users and user groups, and the establishment of "Organization Groups" in the AirWatch system. Follow the steps below to configure the AirWatch system to sync to Active Directory.

To create initial sync to Active Directory system:

1. Click on "Menu" on the top toolbar on the Administration Console home screen.
2. Click "System Configuration" under the heading "Configuration".
3. On the left-hand tool bar, click "System", then "Enterprise Integration", and select "Directory Services".
4. On the "Server" tab, fill out the following information as applicable:

- **Directory Type** – Select the type of directory service your organization uses.
- **Server** – Enter the address of your domain controller.
- **Encryption Type** – Select the type of encryption to use for directory services communication.
- **Port** – Enter the TCP port used to communicate with the domain controller. The default for unencrypted directory service communication is 389.
- **Verify SSL Certificate** – Select the check box to receive SSL errors when the Encryption Type is None. On DoD networks, the Directory Server should have an SSL Certificate assigned as required by the applicable STIG (all information occurs on internal network only).
- **Protocol Version** – Select the version of the LDAP protocol that is in use. Active Directory uses LDAP versions 2 or 3. If you are unsure of which protocol version to use, try the commonly used value of "3".
- **Use Service Account Credentials** – Select the check box to use the credentials from the App pool of the server on which EIS is installed for authenticating with the domain controller. Enabling this option hides the "Bind Username" and "Bind Password" fields.
- **Bind Authentication Type** – Select the type of bind authentication that is used to enable the AirWatch server to communicate with the domain controller. If you are unsure of which protocol version to use, try the commonly used value of "GSS- NEGOTIATE".
- **Bind Username and Bind Password** – Enter the credentials used to authenticate with the domain controller. This account allows read-access permission on your directory server and binds the connection when authenticating the users. Select the "Clear Bind Password" check box to clear the bind password from the database.
- **Search Subdomains** – Select the check box to enable subdomain searching to find nested users. Leaving this box unchecked can make searches faster and avoid network issues, but users and groups located in subdomains under the base DN will not be identified.
- **Domain** – Enter the default domain for any directory-based user accounts. If

only one domain is used for all directory user accounts, fill in the field with the domain so that users are authenticated without explicitly stating their domain.

5. On the "User" tab, fill out the following information as applicable:
   - **Base DN** – Click the **Fetch DN** information icon ( ) next to the Base DN field. This should display a list of Base DNs from which you can select to populate this field. If it does not, revisit the fields and settings you entered on the **Server** tab before continuing.
   - **User Object Class** – Enter the appropriate Object Class. In most cases this value should be "user".
   - **User Search Filter** – Enter the search parameter used to associate user accounts with active directory accounts. The recommended format is "<LDAPUserIdentifier>={EnrollmentUser}" where <LDAPUserIdentifier> is the parameter used on the directory services server to identify the specific user.
     - For AD servers, use "samAccountName={EnrollmentUser}"
     - For other LDAP servers, use "CN={EnrollmentUser}" or "UID={EnrollmentUser}"
   - Select **Show Advanced** to display additional settings.
     - **Auto Merge** – Select this check box to allow user group updates from your directory service to automatically merge with the associated users and groups in AirWatch.
     - **Automatically Set Disabled Users to Inactive** – Select this check box to deactivate the associated user in AirWatch when a user is disabled in your directory service.
     - **Enable Custom Attributes** – Select this check box to enable custom attributes.
6. On the "Group" tab, fill out the following information as applicable:
   - **Base DN** – Click the **Fetch DN** information icon ( ) next to the Base DN field. This should display a list of Base DNs from which you can select to populate this field. If it does not, revisit the fields and settings you entered on the **Server** tab before continuing.
   - **Group Object Class** – Enter the appropriate Object Class. In most cases this value should be "group".
   - **Organizational Unit Object Class** – Enter the appropriate Organizational User Object Class.
   - Select **Show Advanced** to display additional settings. Enter data in the following fields:
     - **Group Search Filter** – Enter the search parameter used to associate user groups with directory service accounts.
     - **Auto Sync Default** – Select this check box to automatically add or remove users in AirWatch configured user groups based on their membership in your directory service.
     - **Auto Merge Default** – Select this check box to automatically apply sync changes without administrative approval.
     - **Maximum Allowable Changes** – Enter the number of maximum allowable group membership changes to be merged into AirWatch. Any

number of changes detected upon syncing with the directory service database that are under this number will be automatically merged. If the number of changes exceeds this threshold, an administrator must manually approve the changes before they are applied. A single change is defined by a user either leaving or joining a group.

2.4.1.1 Adding Users and User Groups from Active Directory to AirWatch MDM Software to Utilize Active Directory Authentication

In the establishment of creating the sync to Active Directory in the above steps, users and user groups can be imported automatically by the AirWatch system. However, users and user groups can also be added manually into the AirWatch system and designated to their appropriate Organization Group.

To add a single user to the AirWatch system using Active Directory Sync:

1. Click on “Menu” on the top tool bar on the Administration Console home screen.
2. Click “Users” under the heading “Accounts”.
3. Click “Add”, then “Add User”.
4. Change “Security Type” to “Directory”, enter User Name, and click “Check User”.
5. Edit user attributes, permissions, and Organizational Group information as necessary, and click “Save”.

To add a user group to the AirWatch system using Active Directory Sync:

1. Click on “Menu” on the top tool bar on the Administration Console home screen.
2. Click “Users” under the heading “Accounts”.
3. Click “Add”.
4. Type in “Search Text” for applicable Group and click Search.
5. View the summary of attributes and click “Save”.

2.4.2 Mobile Device Enrollment Process

“Enrollment” is the process by which mobile devices first authenticate to the AirWatch MDM Server and are provisioned access. It is also the process by which devices are initially checked for compliance and security as outlined by the Administrator in the AirWatch system. To configure enrollment to the organization’s settings, the steps below should be followed in the Administration Console and by the user during enrollment.

2.4.2.1 Setting Enrollment Restrictions in the Administration Console

1. Click on “Menu” on the top toolbar on the Administration Console home screen.
2. Click “System Configuration” under the heading “Configuration”.
3. Click “Devices & Users”, “General”, and “Enrollment”.
4. On the “Authentication Tab”, click the box that says “Override” and set the following options in addition to loaded defaults:

- Uncheck the box labeled "Basic" next to "Authentication Mode" (this will enable only Active Directory authentication for device enrollment).
- Check the box labeled "Require Agent Enrollment for iOS" (this will enforce users to utilize the AirWatch MDM Agent for enrollment on iOS devices as opposed to the Safari browser, which enables compliance detection; see Section 2.7 for more information on the AirWatch MDM Agent).

5. Click the "Terms of Use" tab and upload an assigned organization EULA; check the box labeled "Require Enrollment Terms of Use Acceptance".
6. Click the "Restrictions" tab and follow the procedures below:
   - Under "Policy Settings", click "Add Policy".
     - Set Organization-defined device types, device limits, and check the box labeled "Limit enrollment to specific platforms, models, or operating systems".
       - Specify only STIG-allowed iOS and Samsung Knox operating systems.
     - Click "Save".
7. Fill out other tabs and options as required by the organization for MDM capability and click "Save".

2.4.2.2 User Device Enrollment

To enroll into the AirWatch system, the user will need to acquire or be provided the following prerequisites by their Administrator:

- AirWatch MDM Agent application: Can be procured from iOS or Android public application stores directly from devices. For more information on the AirWatch MDM Agent, see Section 2.7.
- Public URL for Device Services Server (e.g., https://disa.mdm.com). To view URL, follow the procedure below:
  - Click on "Menu" on the top toolbar on the Administration Console home screen.
  - Click "System Configuration" under the heading "Configuration".
  - Click "System", "Advanced", and "Site URLs".
  - Provide the user the first part of "Enrollment URL", prior to section "DeviceManagement/Enrollment".
- Group ID: A "Group ID" is an associated acronym used in AirWatch in conjunction with Organization Groups, which is a hierarchy created by Administrators to associate policies and accesses with particular groups of users. To create, view, or modify "Organization Groups", use the following procedure:
  - Click on "Menu" on the top toolbar on the Administration Console home screen.
  - Click "Organization Groups" under the "Configuration" heading.
  - View the current organizational tree by using the structure on the left-hand toolbar, or create new groups by clicking the "Add Child Organization Group" tab and entering applicable information.
    - "Group ID" required for enrollment is located here by clicking on each Organizational Group name required and viewing the second drop-down box.
- Active Directory username and password.

To enroll into the AirWatch MDM Software system, the user should follow the steps below:

1. Launch the AirWatch MDM Agent on the mobile device.
2. Click "Continue without email address". (**Note:** Used for Autodiscovery customers only; not applicable to DoD networks.)
3. Enter in Device Services URL and Group ID and click "Next".
4. Enter in Active Directory user name and password and click "Enroll".
5. User will automatically be added to the AirWatch system and their device assigned applicable accesses and applications as granted by the Administrator. At this time, the device will also be viewable and manageable via the Administration Console.

2.5 AirWatch Mobile Device Configuration Management and IT Policy Establishment

The AirWatch MDM Software is able to configure devices automatically by allowing the Administrator to create Organizational Group (OG)-specific "Profiles" for Mobile Devices to enforce policies and restrictions on the device MOS. These "Profiles" are platform specific, meaning that iOS and Samsung Knox devices are not necessarily alike in the software configuration they allow an Administrator to perform over-the-air from an MDM server. For any configurations not supported, see the applicable MOS STIG for more information on configuration. As these functions are made available from the MOS developer, they will also be added to the AirWatch system. For more information on specific functionalities and timelines for support, contact AirWatch Professional Services.

To add Profiles and set specific security settings for a particular MOS, follow the procedure below:

1. Click "Add" from the top toolbar of the Administration Console home screen and select "Profile".
2. Select mobile platform (Apple iOS, or Android for Samsung Knox). (**Note:** For Android, you will be presented with two options, "Device" and "Container". Selecting "Container" will activate Profile on the Knox application side of the mobile device, while "Device" sets the Profile at the core device level.)
3. Give the Profile a name under the "General Tab" and assign to particular User or Organizational Groups.
4. Use the tabs on the left-hand toolbar to control particular settings and functions to include "Passcode" settings (device encryption enforcement is located here), general "Restrictions", which are on the MOS and can be controlled over-the-air (for any not listed items, these are not available to MDM vendors by the MOS developer; see appropriate MOS STIG for configuration details), "Exchange Active Sync" configurations, and "Wi-Fi" network control. These settings, located on the left-hand toolbar of the main Profile configuration screen, are referred to as "Payloads". For each "Payload" used, a new Profile specifically for that function should be used.

Additionally, the AirWatch system provides an automated "Compliance Engine" to verify administrator-defined integrity rules for MOSs, and takes action automatically when devices are detected to be compromised. To configure "Compliance Policies", use the procedure below:

1. Click “Add” from the top toolbar of the Administration Console home screen and select “Compliance Policy”.
2. On the “Rules” tab, select whether “All” or “Any” of the specified rules should be followed (“All” refers to all rules being broken in one instance; “Any” refers to any one of the specified rules being broken).
3. In the first drop-down box, select the type of rule to set, and in the second drop-down box, select the specific criteria associated with that rule. Click “Next”.
4. On the “Actions” tab in first drop-down box, select the appropriate action type to take, and in the second drop-down box, select the specific actions to take based on the action type selected. Click “Next”.
5. On the “Assignment” tab, select Users, Organization Groups, or device criteria to assign Policy to. Click “Next”.
6. View “Summary”, and click “Finish and Activate”.

2.6 Mobile Device Application Management

AirWatch MDM Software allows for robust application management functionality on mobile devices, to include the distribution of internal applications, wrapping of internally developed applications for enhanced security, assignment and recommendation of public applications, and deployment of an internal application catalog to substitute for a blocked application store (executed by enabling the device Profile on Android, or configure iOS devices in System Configuration). Additionally, AirWatch can create standards for black-listed, white-listed, and required applications, which the organization can build compliance policies around, and deploy Profiles to operate in conjunction with. Below are some of the main application management features and configuration steps to be used on DoD networks. For more specific information, contact AirWatch Professional Services.

Create and deploy an organizational application store for MOS users:

1. Click on “Menu” on the top toolbar on the Administration Console home screen.
2. Click “System Configuration” under the “Configuration” heading.
3. On the left-hand tool bar, click “Apps”, “Catalog”, and “General”.
4. On the “General” tab, set authentication options for the catalog.
5. On the “Publishing” tab, give the catalog a name and icon and assign it to particular device types (iOS and Android).
6. Click “Save”.

Create “Smart Groups”, which are required for application distribution:

1. Click on “Menu” on the top toolbar on the Administration Console home screen.
2. Click “Applications” under the “Catalog” heading.
3. On the left-hand tool bar, choose “Smart Groups” and click “Add Smart Group”.
4. Give the Smart Group a name and choose applicable users, groups, or device types to add. Applications can now be assigned to the created “Smart Group”.

Assign Internal, Public, and Purchased Applications to mobile device users:

1. Click on “Menu” on the top toolbar on the Administration Console home screen.
2. Click “Applications” under the “Catalog” heading.
3. On the left-hand tool bar, choose “Internal”, “Public”, or “Purchased” application type and follow the specific procedure below:
    - For Internal Applications: Click “Add Application”, upload application file and assign to appropriate groups or users, upload custom EULA, and modify other organization-specific information. Click “Save and Assign”.
    - For Public Applications: Click “Add Application”, select platform, type in application name, and click “Next”. Locate application on presented list and click “Select”. Assign to appropriate groups or users, upload custom EULA, and modify other organization-specific information. Click “Save and Assign”.
    - For Purchased Applications: Click “Add Order”, choose whether it is a custom purchased app or public purchased app (e.g., Apple iOS VPP or B2B program). Upload custom .csv or .xls file (provided by application vendor) and click "Save".

Create mandatory Blacklists, Whitelists, or Required Application Groups:

1. Click on “Menu” on the top toolbar on the Administration Console home screen.
2. Click “Applications” under the “Catalog” heading.
3. On the left-hand toolbar, choose “Application Groups” and click “Add Group”.
4. Using drop-down menus, select group type, platform (MOS) for application, and give a name.
5. Enter application names as necessary and click “Next”.
6. On the “Assignment” tab, select users or devices to assign the list to and click “Finish”.
7. **Note:** Based on these created groups, Compliance Policies and Profiles can be assigned for enforcement and integrity tracking as described by procedures in Section 3.5.

Create advanced application wrapping profiles for internal applications:

1. Click on “Menu” on the top toolbar on the Administration Console home screen.
2. Click “Applications” under the “Catalog” heading.
3. On the left-hand tool bar, choose “Settings and Policies” and click “Profiles”. This will redirect to the System Configuration screen; click “Add Profile”.
4. Choose type of Profile (“SDK”, “Application Profile”, or “App Wrapping Profile”) to create.
5. Select platform type (iOS or Android).
6. In the left-hand toolbar, select policies or configurations to add to the application.
7. Click “Save” and apply to the uploaded internal application.

2.7 Description of AirWatch-Developed On-Device Applications and Usage Instructions

To execute maximum security and usability on mobile devices, the AirWatch MDM Software works in conjunction with four core AirWatch-developed and proprietary applications, which should be used in conjunction with DoD MDM deployments: AirWatch MDM Agent, Secure Content Locker (SCL), AirWatch Browser, and the AirWatch Email Client (AWEC). Below is a description of each application and its particular use case when used in conjunction with DoD mobile device deployments. All applications are available in the public iOS and Android application stores and can be deployed and managed from the AirWatch Administration Console.

AirWatch MDM Agent: The AirWatch MDM Agent is an application installed on managed devices that collects and delivers device information to the AirWatch Administration Console. The information the Agent transmits may contain sensitive data such as GPS coordinates or compromised device status, and therefore occurs over an SSL connection to the Device Services server. The Agent also performs background compliance checks on the device, to include jailbreak and rooted MOS detection, and therefore should be mandatory to be used in the device enrollment process as specified in Section 2.4.2.2. Additionally, the AirWatch Agent allows for the exchange of X.509 certificates with the AirWatch system to further identify itself and the device to the server (for more information see Section 2.8). The AirWatch MDM Agent, however, does not enable access to any corporate content or house data, and therefore does not require authentication for application access. Removal of the AirWatch Agent from the mobile device MOS will automatically result in an "Enterprise Wipe", which is the removal of all corporate content, applications, and access to the host network.

Secure Content Locker (SCL): The SCL, AirWatch's Mobile Content Management (MCM) solution, allows IT administrators to manage mobile access to network file shares and control the distribution of corporate documents through a web-based console. The SCL can be used for several functions, to include the viewing of corporate content as provided by the AirWatch Administrator through the Administration Console; the opening of encrypted email attachments (occurs in conjunction with SEG server; email attachments should be made to be encrypted by default); and restricting the ability to copy/paste from corporate documents, forward documents via email, or open documents in third-party applications. The SCL uses a FIPS 140-2 validated cryptographic module and therefore protects data to the maximum extent possible. (**Note:** Full device encryption as required by the applicable MOS STIGs should still remain enabled.) Currently, the SCL is not CAC-enabled and should not be used to access corporate content repositories or backend systems requiring such access. However, the SCL can be used to access content loaded purposely for mobile device use by the Administrator, or to access AirWatch/mobile-specific content shares. CAC authentication capability is expected in a future release of the SCL. To verify that the SCL is not connected to an internal file share or content repository system, use the following procedure:

1. Click on "Menu" on the top toolbar on the Administration Console home screen.
2. Click on "Content Management" under the "Content" heading.
3. On the left-hand toolbar, click "Content Repository" under the "Configuration" heading.
4. Verify that no content repository system or file shares requiring CAC access are listed on an adjacent listing.

AirWatch Browser: The AirWatch Browser application provides a safe, accessible, and manageable alternative to Internet browsing using native device browsers. On DoD networks, native device browsers can be blocked via Profile (see the "Restriction" section of Profile and Section 3.5) and the AirWatch Browser can be used to blacklist and whitelist particular web addresses mobile users attempt to access. Furthermore, the AirWatch Browser can be used to point to a host network proxy system for web traffic auditing. Currently, the AirWatch Browser is not CAC-enabled and should not be used for direct tunneling to intranet DoD sites that typically require CAC authentication. However, if this feature is needed, the organization can deploy a standard VPN Profile using the information in Section 2.5 to authenticate to the DoD network, and should consult the STIG that relates to that form of remote session.

AirWatch Email Client (AWEC): The AWEC is currently deployable on Android devices, to include Samsung Knox, and will soon be released for iOS devices. While not currently required on DoD networks, the AWEC can be used to containerize corporate email in a separate application than native device mail. FIPS 140-2 encryption is also available and can be provided to DoD customers (contact AirWatch Professional Services for more information). CAC functionality is currently not supported, to include S/MIME capability (S/MIME with CAC), and therefore, emails that require such authentication are readable on the mobile device; nor is digital signing capability from CAC available. This capability is expected in a future release of the AWEC.

2.8 Encryption, Certificates, and SSL

The AirWatch MDM Software suite uses a variety of encryption security methods to protect data at rest, data in transit, and information on mobile devices. These encryption modules and certificates that are used to protect information are divided between the host network servers and the mobile devices MOSs, and those applicable STIGs and their qualifications should be taken into account prior to installing AirWatch MDM Software.

On the host network servers running Windows Server 2008 R2 or 2012 operating systems, the AirWatch MDM Software uses the cryptographic modules of these systems, the configuration of which is noted in the applicable OS STIG.

For data in transit from mobile devices to the host network, the organization should procure a publicly trusted SSL Certificate that is bound to port 443 in the IIS of the AirWatch Device Services server. The organization should check the applicable STIG to ensure that the procured SSL Certificate meets FIPS 140-2 requirements and any other applicable standards prior to installation.

With regard to data at rest on the mobile devices, AirWatch MDM Software leverages the native device encryption on Apple iOS and Samsung Knox devices and guards all information, applications, and utilities on the mobile device. Information on the cryptographic modules used by these MOSs can be obtained from the applicable STIG. The AirWatch MDM Software can be used to enforce mobile device encryption and track compliance by following the procedures below.

To enforce encryption on Apple iOS devices (see the Apple iOS STIG for more information on how passcode settings auto activate iOS encryption):

1. From the AirWatch Administration Console main screen, click “Add” on the top toolbar and choose “Profile”.
2. Click “Apple iOS” and give the Profile an assigned name and group/user assignment on the “General” tab.
3. On the left-hand toolbar, choose “Passcode”, click “Configure”, and check the box labeled “Require passcode on device”.
4. Set the passcode to the required settings outlined in the Apple iOS STIG and click “Save & Publish”.

To enforce encryption on Samsung Knox devices:

1. From the AirWatch Administration Console main screen, click “Add” on the top toolbar and choose “Profile”.
2. Click “Android”, choose whether to configure your action on the “Device” or “Container” (Knox application side only), and give the Profile an assigned name and group/user assignment on the “General” tab.
3. On the left-hand toolbar, choose “Passcode”, click “Configure”, and set the passcode to the required settings outlined in the Samsung Knox STIG.
4. On the same page, check the boxes labeled “Require Storage Encryption” and “Require SD Card Encryption” and click “Save & Publish”.

To set a Compliance Policy to remove DoD network content and access if encryption is removed, and to verify policy is in place after setting the Compliance Policy:

1. From the AirWatch Administration Console main screen, click “Add” on the top toolbar and choose “Compliance Policy”.
2. On the “Rules” tab, in the first drop-down box, select “Encryption”, in the second drop-down box, select “Is Not Enabled”, and click “Next”.
3. On the “Actions” tab, in the first drop-down box, select “Command”, in the second drop-down box, select “Enterprise Wipe”, and click “Next”.
4. On the “Assignment” tab, choose the applicable platform and assign to users and groups as necessary, then click “Next”.
5. On the “Summary” tab, view information, change as necessary, and click “Finish and Activate”.
6. To check this feature is enabled and functional, remove encryption from a test mobile device and verify that “Enterprise Wipe” executes and DoD network access is removed.

2.9 Removing Mobile Device Access to the DoD Network (Device Wipe)

AirWatch MDM Software is capable of executing two forms of device wipes, which are defined below:

- "Enterprise Wipe": Removes all assigned DoD content, accesses, and applications, but leaves core operating system and user information intact.
- "Device Wipe": Performs factory reset of the mobile device.

The applicable MOS STIG should be checked for recommendation on which type to perform in particular scenarios. These wipe functions can be tied to the Compliance Engine policies as described in Section 3.8 or can be manually performed on individual devices using the following procedure:

1. From the Administration Console home screen, locate the list of managed mobile devices on the lower half of the "Asset Tracking" screen.
2. Search for the device by using the search engine provided and click on "Friendly Name".
3. On the top toolbar, click "Device Wipe" or "Enterprise Wipe" as applicable.

2.10 Maintenance and Updates of AirWatch MDM Software

Updates to the AirWatch MDM Software, when installed entirely on DoD networks, can occur by a variety of methods that are the decision of the organization and their particular application update policies and applicable STIGs. Upon release of an AirWatch update, an AirWatch Professional Services representative will contact the organization to make them aware and offer technical support if needed. The organization will be given a link to an FTP download site to obtain the necessary executable files and instructions. Prior to running any application updates, the virtual servers should be backed up and made recoverable in case any issue arises during update.

AirWatch executable files for system updates are first run on the Device Services, AirWatch Administration Console, and other applicable application servers (e.g., SEG, EIS). The update process is then paused and a separate executable is run on the AirWatch Database Server. Upon conclusion of the Database Server update, the application server updates can be concluded. The system should be logged on to immediately to check for performance. For more information or assistance in executing AirWatch MDM Software updates, contact your AirWatch Professional Services representative.

Updates to the Windows Server OS, or Apple iOS and Samsung Knox MOSs, are the responsibility of those operating systems. For information on updating these systems, see the applicable OS and MOS STIGs.

2.11 Malware and Device Integrity Scanning

Malware detection and device integrity scanning occur on the applicable Windows Server OS, Apple iOS MOS, or Samsung Knox MOS, and are out of scope of the AirWatch MDM Software. For information on malware detection or integrity scanning tools for these systems, see applicable OS and MOS STIGs.

2.12 AirWatch Support and Additional Documentation

AirWatch support is available via phone at 1-866-501-7705 or by emailing: Support@air-watch.com.