VMware AirWatch Enterprise Integration Service Guide

EIS Server Installation and Integration

Workspace ONE UEM v9.6

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Revision Table

The following table displays revisions to this guide since the release of Workspace ONE UEM v9.6.

Date	Reason
June 2018	Initial upload.

Table of Contents

Chapter 1:
Overview

Introduction to EIS

The AirWatch Enterprise Integration Service (EIS) provides organizations the ability to securely integrate with back-end enterprise systems from either the AirWatch SaaS environment or a remote network zone (for example, a DMZ). This integration allows organizations to leverage the benefits of SaaS and their existing LDAP, CA, email, and other back-end systems.

EIS integrates with the following internal components:

- Email Relay (SMTP)
- Directory Services (LDAP / AD)
- Email Management Exchange 2010 (PowerShell)
- BlackBerry Enterprise Server (BES)
- Lotus Domino Web Service (HTTPS)
- Content Repositories (SharePoint, network file shares, etc.)
- Syslog (Event log data)

The following components are only available if you purchased the PKI Integration add-on, which is available separately:

- Microsoft Certificate Services (PKI)
- Simple Certificate Enrollment Protocol (SCEP PKI)
- Third-party Certificate Services (On-premises only)

Prerequisites for EIS Connectivity for On-Premises Environments

Hardware Requirements			
Status Checklist	**Requirement**	**Notes**	
	VM or Physical Server	1 CPU Core (2.0+ GHz) 2 GB RAM or higher 5 GB Disk Space	

General Requirements			
Status Checklist	**Requirement**	**Notes**	
	Ensure that you have remote access to the servers that AirWatch is installed on	AirWatch recommends setting up Remote Desktop Connection Manager for multiple server management, installer can be downloaded from https://www.microsoft.com/en-us/download/details.aspx?id=44989 See **General Requirements**.
	Installation of Notepad++ (Recommended)	Installer can be downloaded from http://download.tuxfamily.org/notepadplus/6.5.1/npp.6.5.1.Installer.exe
	Services accounts for authentication to backend systems	Validate AD connectivity method using LDP.exe tool (See http://www.computerperformance.co.uk/ScriptsGuy/ldp.zip) LDAP, BES, PowerShell, etc.

Software Requirements			
Status Checklist	**Requirement**	**Notes**	
	Windows Server 2008 R2 or Windows Server 2012 or Windows Server 2012 R2	
	Install PowerShell on the server	Optional
	Install Role Services from Server Manager	**Common HTTP Features:** Static Content, Default Document, Directory Browsing, HTTP Errors, HTTP Redirection **Application Development:** ASP.NET, .NET Extensibility, ASP, ISAPI Extensions, ISAPI Filters **Important:** Ensure WebDAV is not installed
	Install Features from Server Manager	**.NET Framework 3.5.1 Features:** Entire module (.NET Framework 3.5.1, WCF Activation) **Telnet Client**
	Install .NET Framework 4.0	Download from http://www.microsoft.com/en-us/download/confirmation.aspx?id=17718
	Externally registered DNS	Register the EIS relay (If Relay-Endpoint) or register the EIS Endpoint (If Endpoint only) See **Server Requirements**.
	SSL Certificate from trusted third party with Subject or Subject Alternative name of DNS	Ensure SSL certificate is trusted by all device types being used. (i.e. not all Comodo certificates are natively trusted by Android)

Software Requirements			
Status Checklist	Requirement	Notes	
	IIS 443 Binding with the same SSL Certificate	Validate that you can connect to the server over HTTPS (https://yourAirWatchDomain.com). At this point, you should see the IIS splash page. See **Server Requirements**.	

For configuring the ports listed below, all traffic is uni-directional (outbound) from the source component to the destination component.

Network Requirements					
	Source Component	Destination Component	Protocol	Port	Verification
	AirWatch DS and Console	AirWatch EIS	HTTPS	443	Telnet from Internet to DS and Console server on port
	AirWatch EIS	AirWatch SOAP API Server	HTTP or HTTPS	80 or 443	Telnet from EIS Server to SOAP API Server
	EIS Relay Server (only for relay-endpoint configurations)	AirWatch EIS Endpoint	HTTPS	443	Telnet from EIS Relay Server to EIS Endpoint Server
	EIS Server (OPTIONAL)	Internal SMTP	SMTP	25	Telnet from EIS Server
	EIS Server (OPTIONAL)	Internal LDAP	LDAP or LDAPS	389, 636, 3268, or 3269	Telnet from EIS Server
	EIS Server (OPTIONAL)	Internal SCEP	HTTP or HTTPS	80 or 443	Telnet from EIS Server
	EIS Server (OPTIONAL)	Internal ADCS	DCOM	135, 1025-5000, 49152-65535	Telnet from EIS Server
	EIS Server (OPTIONAL)	Internal BES	HTTP or HTTPS	80 or 443	Telnet from EIS Server
	EIS Server (OPTIONAL)	Internal Exchange 2010 or higher	HTTP or HTTPS	80 or 443	Telnet from EIS Server

If you are using Content Repositories (e.g., SharePoint, shared drives, etc.), EIS and all repositories must be open to all IP ranges on port 443.

General Requirements

Remote Access to Servers

Ensure that you have remote access to the servers where Workspace ONE UEM is installed. Typically, Workspace ONE UEM consultants perform installations remotely over a web meeting or screen share. Some customers also provide Workspace ONE UEM with VPN credentials to directly access the environment as well.

Server Requirements

External DNS Name

The two main components of Workspace ONE UEM are the Device Services server and the Console server. In a single server deployment, these components reside on the same server, and an external DNS entry needs to be registered for that server.

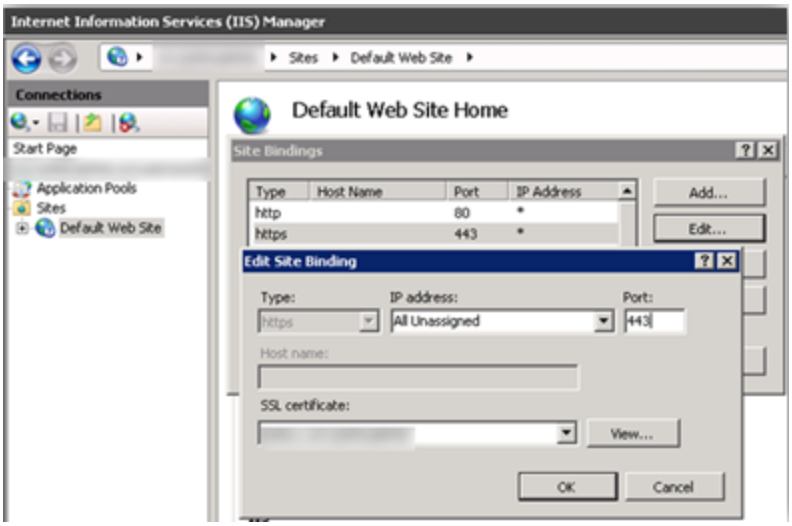
In a multi-server deployment, these components are installed on separate servers, and only the Device Services component requires an external DNS name, while the Console component can remain only internally available.

SSL Certificate

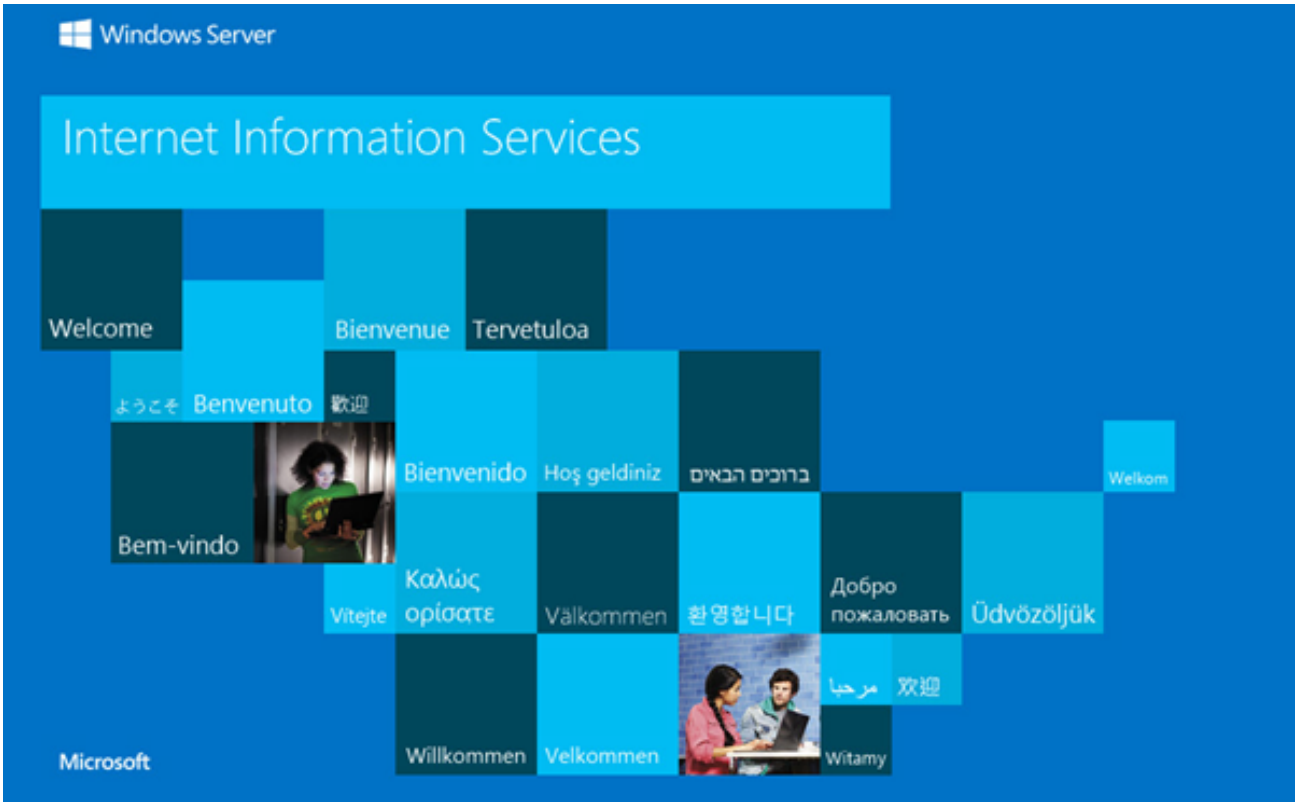
Set up the externally available URL of the Workspace ONE UEM server with a trusted SSL certificate. A wildcard or individual website certificate is required.

Note: If SSL is used for admin console access, ensure that FQDN is enabled or the host file is configured.

1. Obtain SSL certificates for each of your external DNS entries. A list of root certificates natively trusted by iOS can be found here: http://support.apple.com/kb/HT5012
2. Upload your SSL certificate to the Workspace ONE UEM server(s). Your certificate provider has instructions for this process.
3. Once uploaded on your server you can use it to add a 443 binding to the Default Website in IIS. The bindings for a completed server look like the following. Your SSL certificate appears in the drop-down menu of available certificates.



4. Validate that you can connect to the server over HTTPS (https://yourAirWatchDomain.com). At this point, you see the IIS splash page.



Chapter 2:
Architecture & Security

Overview

The EIS is a lightweight ASP.NET IIS web application that you can install on physical or virtual servers, Windows 2008 or higher. Install EIS on an on-premises server in either a DMZ or secured internal network zone.

When the Workspace ONE UEM application needs to query one of the systems it integrates with, EIS encrypts the request and sends it to the EIS server to make a local request to the back-end enterprise system. EIS secures the traffic between Workspace ONE UEM and the corporate network using unique X.509 certificates for mutual authentication and encryption.

Supported Configurations

Use EIS in the following configurations:

- Sitting behind a network load balancer for high availability deployments.
- Supporting SSL offloading.
- Using HTTP or HTTPS transport.
- Supporting HTTP authentication of traffic from a network reverse proxy or Web Application Firewall (WAF).
- Acting as a relay (EISR) node to secure traffic through multiple network zones.

Deployment Models

Deploy EIS in any one of the following models:

SaaS Deployments

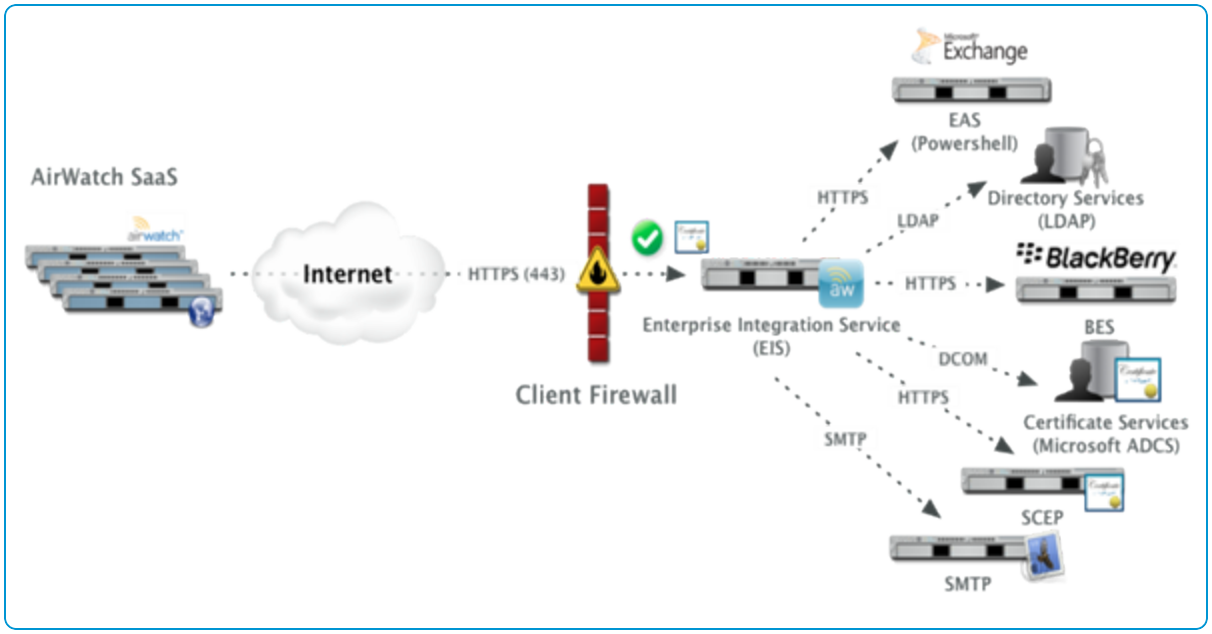
- Basic Endpoint
- Reverse Proxy / WAF
- DMZ Relay

On-Premise (non-SaaS) Deployments

- Relay for Multiple Network Zones

Basic Endpoint

In a basic endpoint deployment, the EIS is behind a WAF and resides on an internal network. The traffic from the AirWatch SaaS is sent securely over an HTTP or HTTPS transport and its message level is signed using unique X.509 certificates.

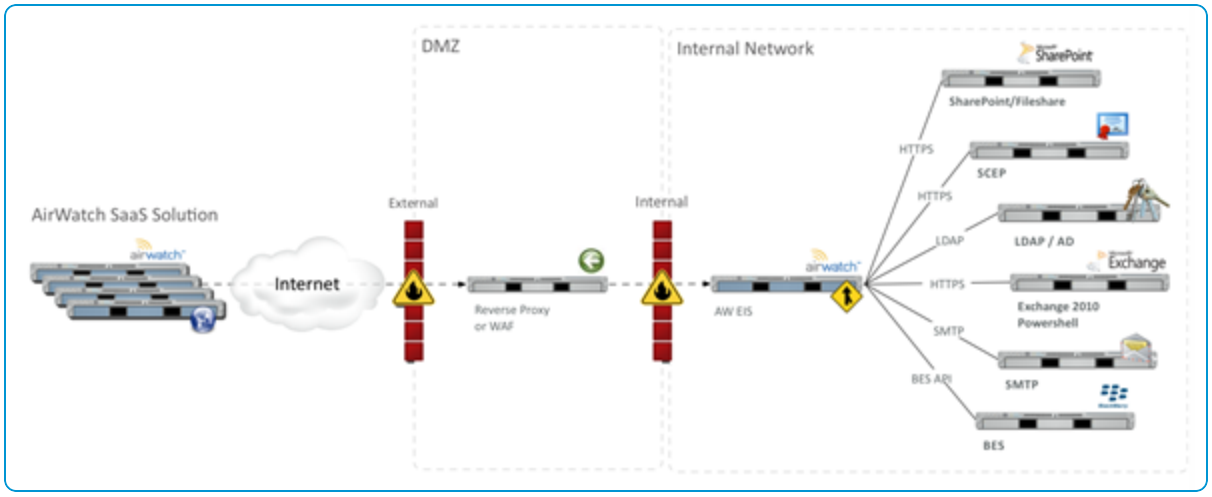


Reverse Proxy / WAF

In a reverse proxy/WAF deployment, the EIS is behind a reverse proxy such as Microsoft's ISA or Forefront TMG or a WAF and resides on an internal network. The traffic from the Workspace ONE UEM SaaS is sent securely over an HTTP or HTTPS transport and its message level is signed using unique X.509 certificates.

Note: If you are configuring EIS to run behind a reverse proxy server, you will need to perform the following steps:

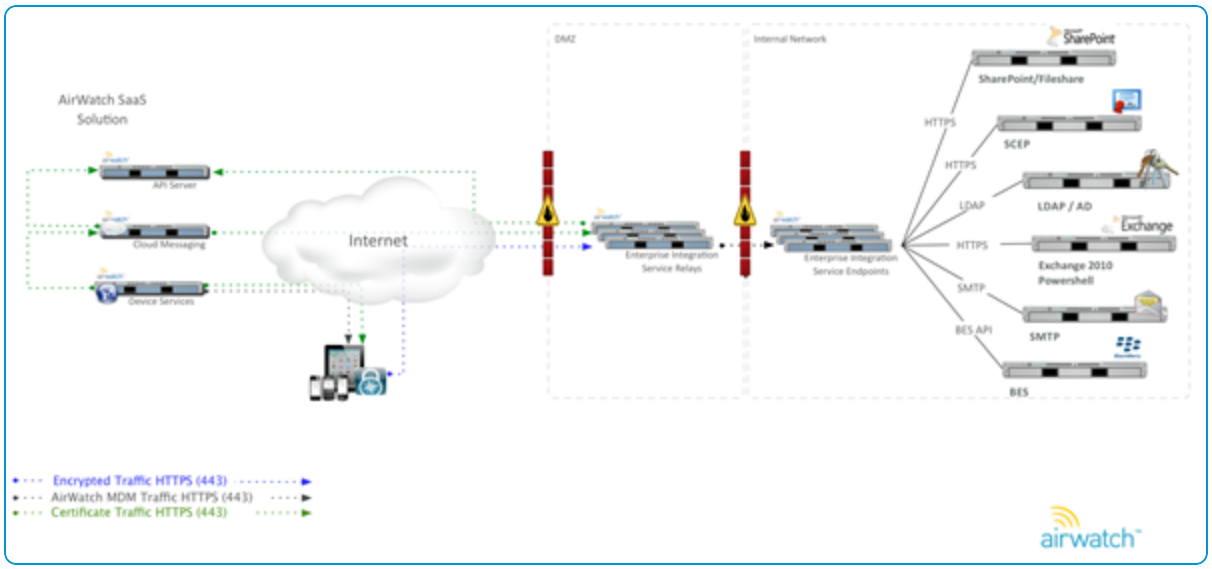
- Ensure the SSL Offloading option is selected when running the EIS Configuration Wizard.
- Place the certificate you are using for authentication on the reverse proxy server.



DMZ Relay

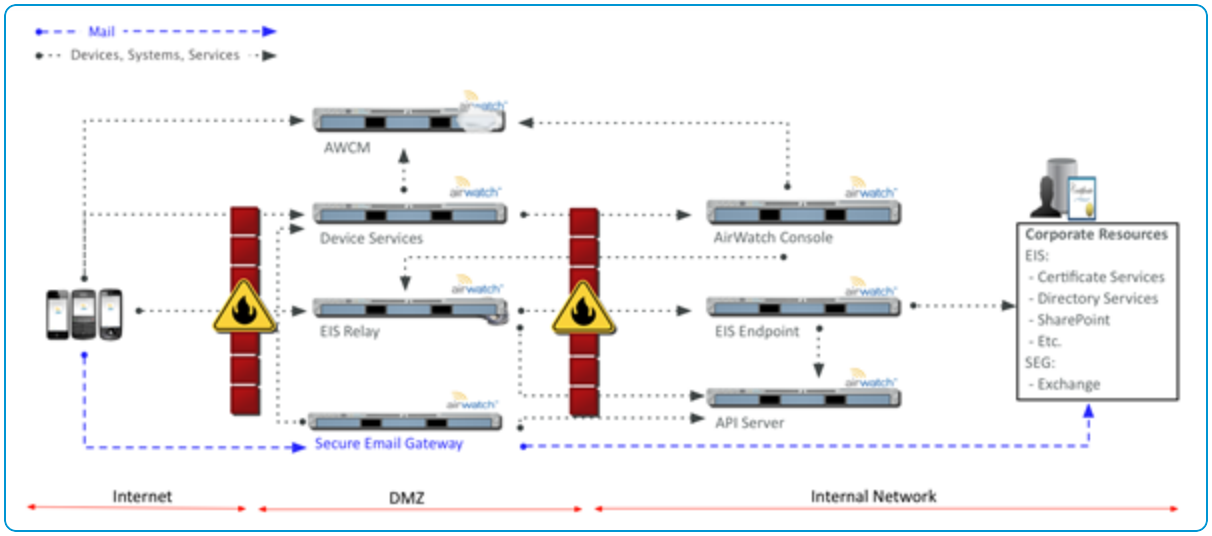
In a DMZ relay deployment, the EIS is in the DMZ and internal network as either an endpoint or EIS relay because organizations do not have a WAF or reverse proxy. This model allows requests from Workspace ONE UEM to securely connect to the EIS relay node in the DMZ. It also allows for the relay node to further send traffic to an internal EIS endpoint node for back-end system integration.

The EIS server encrypts all traffic requests to the EIS relay and EIS endpoint using unique X.509 certificates. It is setup for either HTTP or HTTPS transport.



Relay for Multiple Network Zones

In a multiple network zones deployment, the EIS is used in an on-premises (non-SaaS) environment to integrate with internal systems from a DMZ server connection.



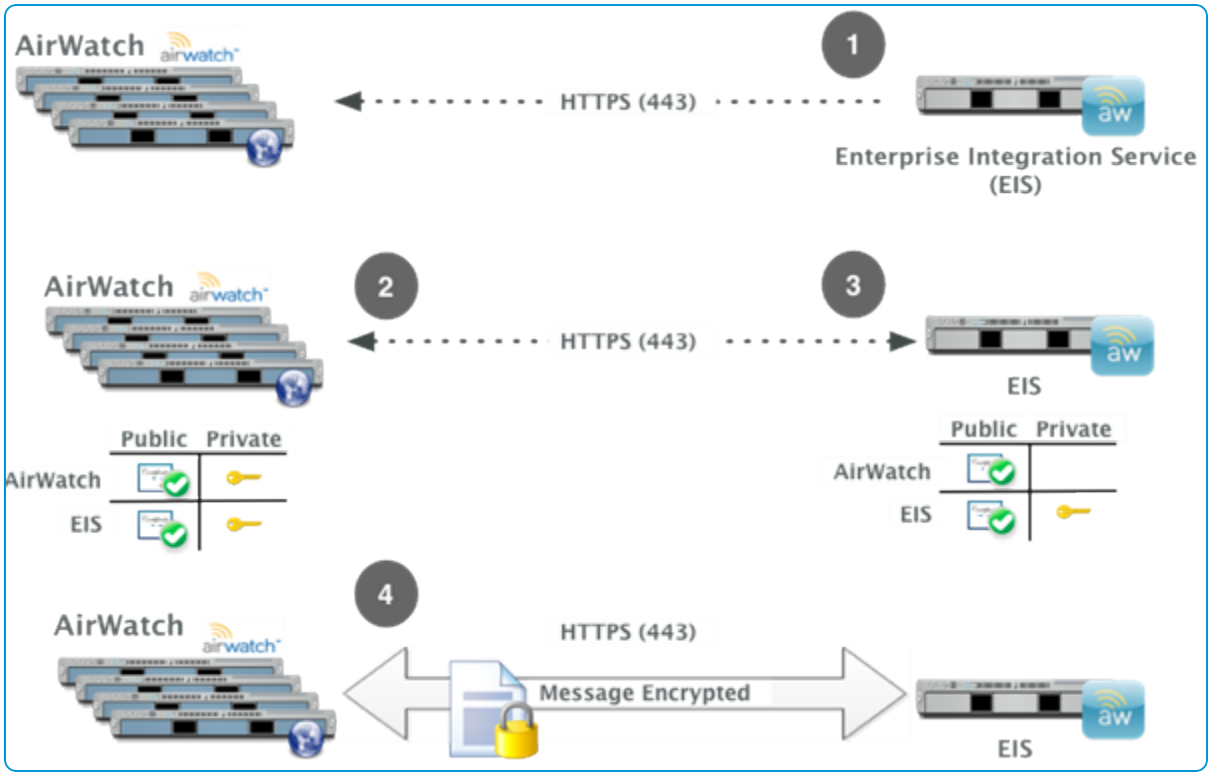
Chapter 3:
EIS Security & Certificates

Initial Setup

1. The EIS connects to the AirWatch API and authenticates with the AirWatch Console **Username** and **Password**.
   - Traffic requests are SSL encrypted using HTTPS.
   - Setup authorization is restricted to admin accounts with a role enabled for an EIS setup role (see preliminary steps).
2. AirWatch generates a unique identity certificate pair for both the AirWatch and EIS environments.
   - The AirWatch certificate is unique to the group selected in the AirWatch Console.
   - Both certificates are generated from a trusted AirWatch root.
3. AirWatch sends the unique certificates and trust configuration back to the EIS server over HTTPS.

The EIS configuration trusts only messages signed from the AirWatch environment. This trust is unique per group.

Note: Any additional EIS server set up in the same AirWatch group (for example, load balanced) is issued the same unique EIS certificate.



Integration Cycle

The AirWatch server sends each request as an encrypted message to the EIS endpoint, and the EIS endpoint responds with an encrypted message.

- Messages are encrypted using the unique public key of the EIS instance. Only EIS can decrypt the public key.
- Messages are signed using the private key of the AirWatch MDM instance that is unique for each group.Therefore, EIS trusts the requests *only* from the configured AirWatch server.
- Responses from EIS to the AirWatch MDM server are encrypted with the AirWatch MDM public key and signed with the EIS private key.

Chapter 4:
EIS Installation Preparation

Considerations and Recommendations Prior to Upgrading EIS

If a previous version of EIS is installed, consider the following prior to upgrading:

- You do NOT need to stop any AirWatch functionality in order to upgrade EIS. The installer has been designed to seamlessly upgrade without disruption.
- If you choose to upgrade, stage EIS on the EIS server and consider taking a Virtual Machine (VM) snapshot to back it up.
- If a previous version of EIS is installed, the installer auto-detects it and gives you the option of upgrading to the latest version.

Performing Preliminary Installation Steps

Prepare for the installation by performing the following steps:

1. Download the EIS installation files from the AirWatch Console located in **Groups & Settings > All Settings > System > Enterprise Integration > Enterprise Integration Services.**

   Note: You might need to temporarily disable User Account Control (UAC) for the installation to take place, and then re-enable it after the installation. This is a consideration based on your environment and it varies depending on the server deployment.

2. Create an admin account for EIS with the resource **SOAP API** > **Read / Write / Update** in the AirWatch Console. This resource is required for installation.

   Note: The EIS account must use a role with permissions enabled. The SOAP API allows access to all AirWatch Services APIs except Enterprise Wipe and Device Wipe.

Chapter 5:
EIS Installation

Running the EIS Installer

Perform the following steps to install the EIS.

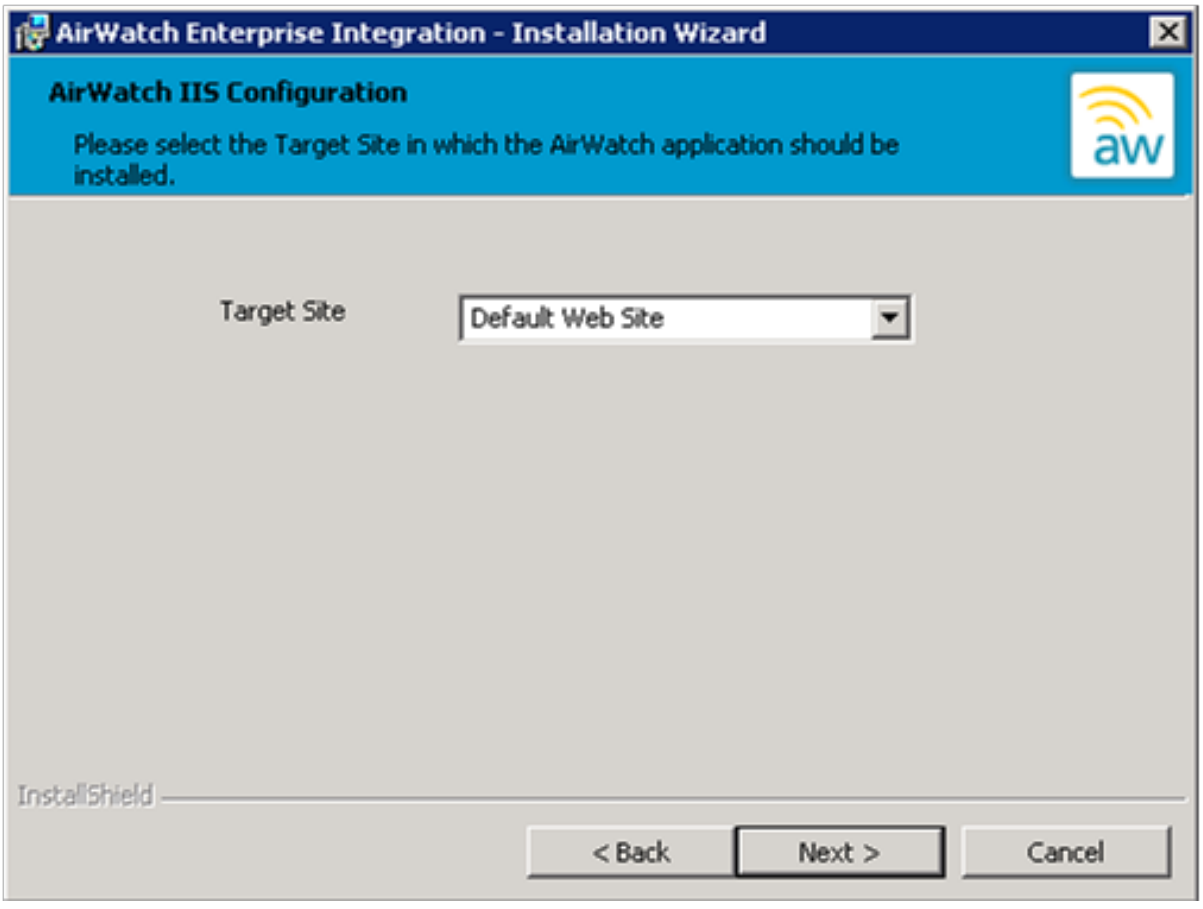
1. Open the installer.

   Note: The installer verifies prerequisites on your EIS server.

   Note: If a previous version of EIS is installed, the installer auto-detects it and offers the option to upgrade to the latest version.

2. Accept the license agreement and then select **Next**.
3. Click **Change** to select the installation directory and the IIS website to use (for example, Default Website).

   Note: This step creates a dedicated folder and a virtual directory for EIS.

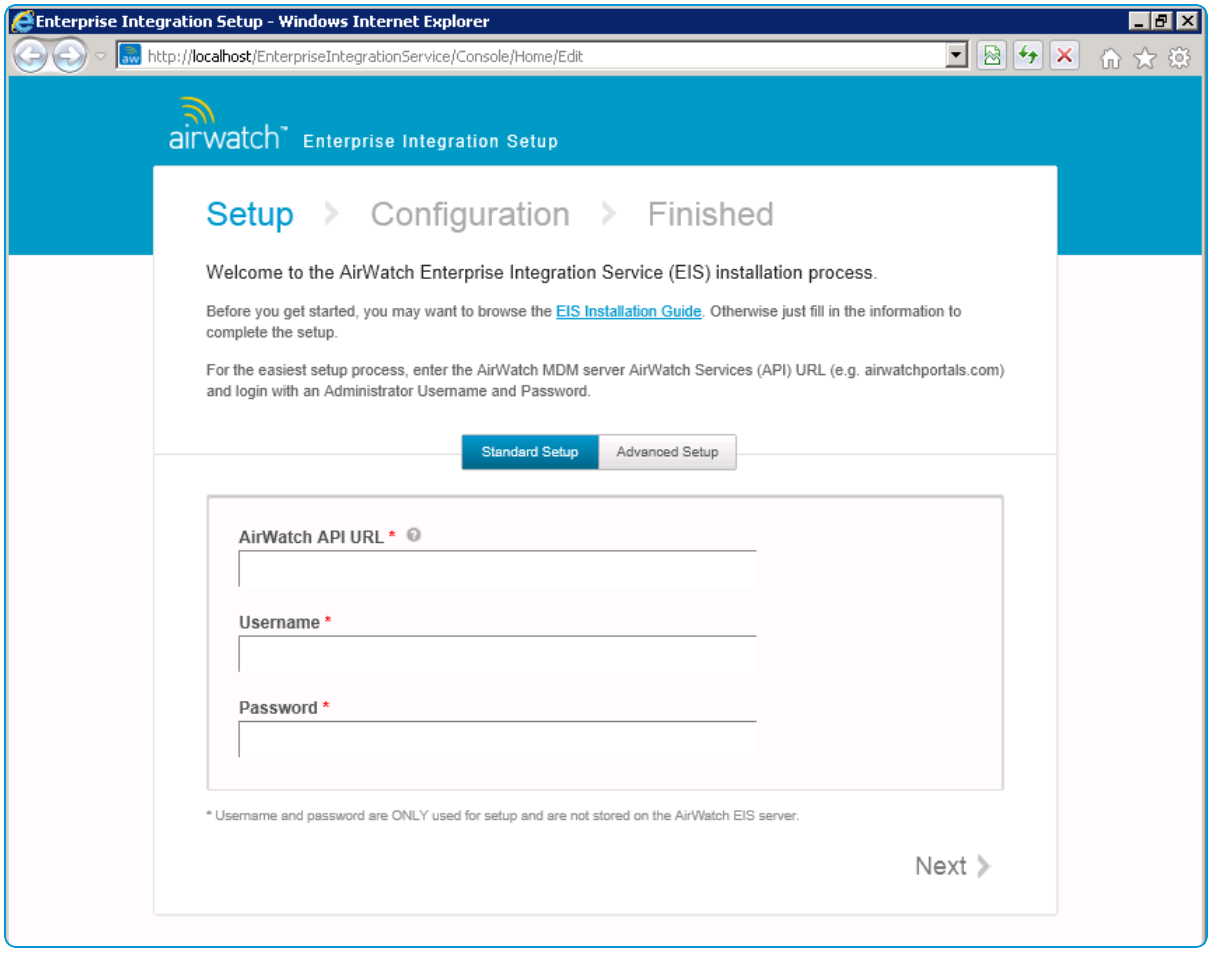


4. Click **Next** to proceed. When the installation screen appears, select **Install** to begin.
5. Click **Finish**. The configuration page below automatically opens.

Configuring EIS

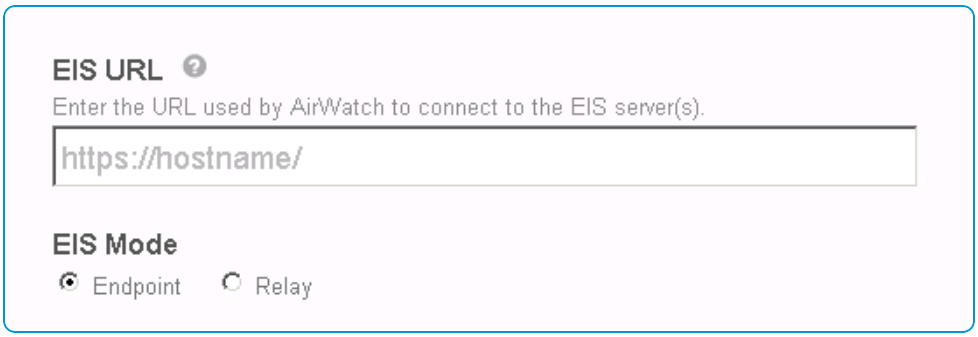
Perform the following steps to configure EIS to communicate with AirWatch.

Note: If you are installing an EIS Relay server, advance to Appendix B - Configuring and Installing EISR, install and configure EISR, and then return to this point and configure EIS.



1. In the **AirWatch API URL** field, enter a URL based on the environment:
   - SaaS deployments typically use https://cnXX.AirWatchportals.com or cnXXXawmdm.com, where XX or XXX is your unique environment to access the SaaS environment. Enter that URL, but replace the "cn" with "as" in the URL. (https://asXX.AirWatchportals.com or https://asXXX.awmdm.com).
   - On-premises (non-SaaS) deployments use the URL that accesses the AirWatch Console.
2. Enter the **Username** and **Password** for the EIS admin account.
3. Click **Next**. The installation advances to the **Configuration** screen.
4. Click the **AirWatch Group** drop-down arrow and select the top-level or a custom group to limit integration. Selecting the top-level allows for all child organization groups below that level to inherit these configurations and leverage EIS integration.

5. Enter the URL to connect to the EIS server (for example, https://aweis.corporatecorp.com).

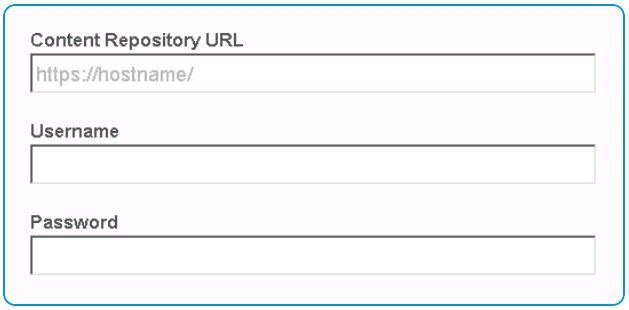


Note: You must have an EIS URL. If not, obtain a URL by registering a Domain Name Server (DNS) name. After obtaining it, enter the URL in this field so that AirWatch can connect to the EIS server(s).

6. Select the **EIS Mode**. Most installations should choose **Endpoint** as the EIS mode.

Note: If the EIS server you are installing is not the server that can reach the integrated systems, select **Relay** to enter the target server address to forward requests to. Verification can be made if that server is ready.

7. The next screen allows you to configure EIS to connect with your content repository (for example, an internal file share or SharePoint server). Instead of configuring these fields here, consider configuring them in the AirWatch Console.



Note: Integrating through the EIS installer allows integration with only one repository. Integrating with content repositories within the EIS installer prevents admin credentials from being stored within the AirWatch database.

Note: Integrating with content repositories from the AirWatch Console allows integration with multiple repositories. The AirWatch Console can limit user access to specific repository folders, whereas EIS does not provide this functionality.

Enter the following information if you choose to configure these settings in EIS:

- **Content Repository URL** – Path should point to the global root level directory of the EIS content repository.
- **Admin Username** and **Password** – Requires WebDAV access, which is needed to connect to the server.

If you choose to configure the content repository in the AirWatch Console, after you complete and verify this installation, navigate to **Groups & Settings > All Settings > Content > Content Repository > Add**. For more information on integrating with a content repository, refer to the **VMware AirWatch Mobile Content Management Guide**, available on AirWatch Resources.

8. Click **Next**. The installation advances to the **Finished** screen, which indicates that EIS is successfully installed on your AirWatch server.

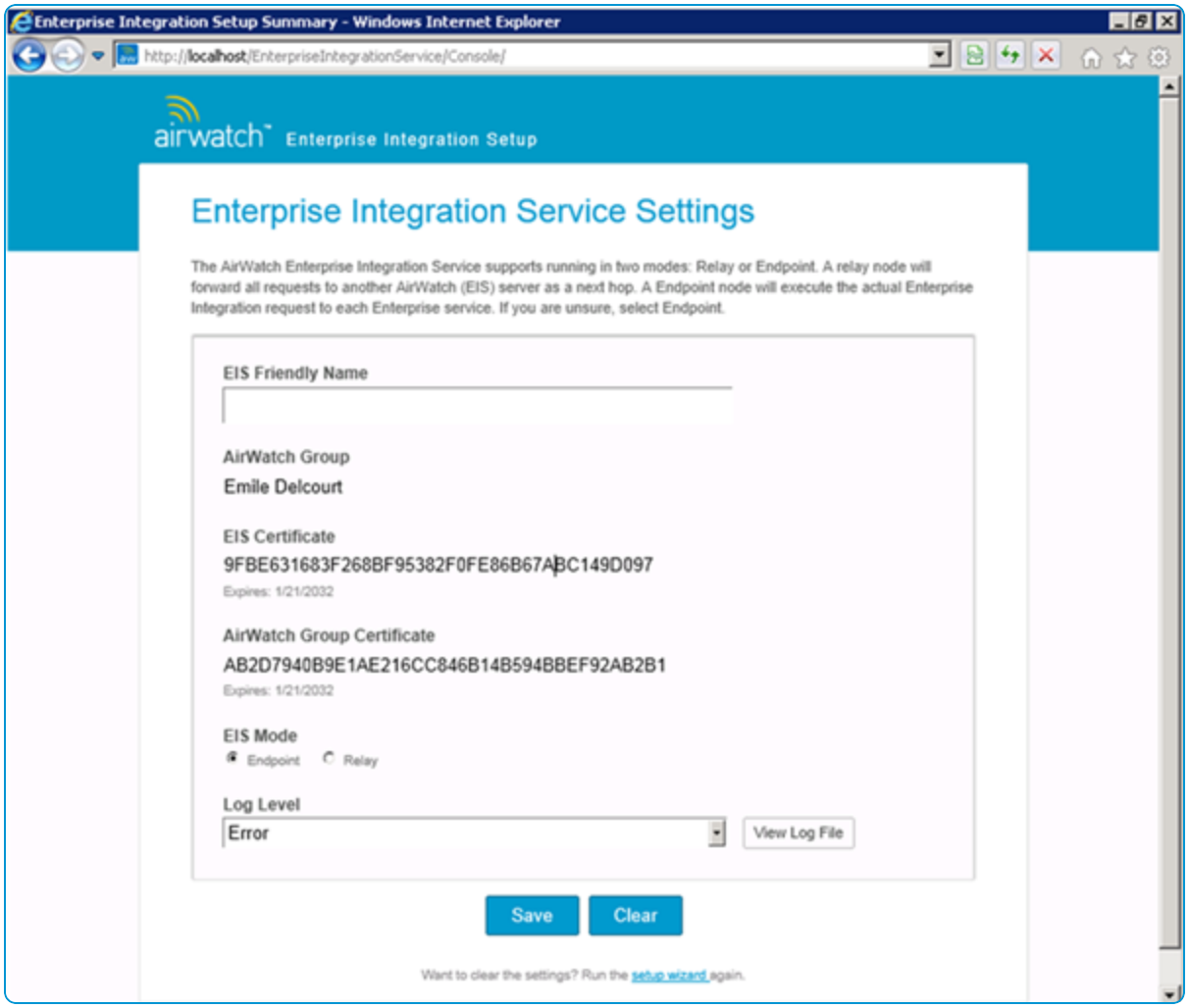
Chapter 6:
EIS Installation Verification

Overview

Perform the following tasks to verify that the EIS installation was successful.

Verifying a Successful Installation or Upgrade

The screen below shows a friendly name for easy identification of this server, a summary of the certificate(s) in use for the integration and an option to change the log level.



Always set the **Log Level** to **Error** unless you are troubleshooting EIS. After troubleshooting, return the selection to **Error**.

1. Click **Test Connection** from any system bound through EIS. For example, test the connection from the directory services, the SMTP or the certificate authority in the AirWatch Console.
2. If upgrading, determine which features are new in the EIS upgrade and test the new functionality to verify the upgrade was successful.

Changing the Settings or Re-Installing EIS

To make changes, perform the following steps:

1. Return to the configuration page (http://localhost/EnterpriseIntegrationService/Console) at any time to modify settings.
2. Click the link **setup wizard** at the bottom of the screen to start the configuration wizard that allowed you to connect to the AirWatch environment.

Chapter 7:
EIS System Settings

Overview

After installation, you can view and adjust the EIS server configuration in the AirWatch server **Console Settings** using the following step-by-step instructions.

Configuring EIS Admin Console Settings

1. Log in to the AirWatch Console and navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Enterprise Integration Services.**

2. Configure the following settings:

Setting	Description
Enable Enterprise Integration Service	Enable this check box to begin integrating your enterprise services.
EIS URL	Enter the EIS URL. An example URL format is https://AWintegration.Corporate.com/EnterpriseIntegrationService/. **Note:** The hostname must have a valid SSL certificate. Verify that the EIS URL is correct by selecting the **Verify** button. **Note:** Clicking on the **Verify** button lets you know immediately if AirWatch can connect to EIS. If you receive an error, continue with this procedure and then refer to Appendix A: Advanced Setup for information on how to manually configure AirWatch and EIS.
Authentication	Select the method AirWatch uses to authenticate to the EIS server: • **Certificate** – Uses message-level encryption over HTTPS. • **AirWatch Cert & HTTP Auth** – Includes a certificate and adds a username/password sent in an HTTP authentication header.

Setting	Description
Enterprise Services	Enable or Disable the services that AirWatch needs to integrate with EIS. • SMTP (Email Relay) **Note:** AirWatch SaaS offers email delivery through SMTP, but you can enable EIS to use another SMTP server here. Enter SMTP servers settings for email in **Groups & Settings > All Settings > System > Enterprise Integration > Email (SMTP).** • Directory Services (LDAP / AD) • Exchange PowerShell (for certain secure email gateways) • BES (BlackBerry sync user and mobile device information) The following components are only available if you purchased the PKI Integration add-on, which is available separately: • Microsoft Certificate Services (PKI) • Simple Certificate Enrollment Protocol (SCEP PKI) • OpenTrust CMS Mobile (third-party certificate services) • Entrust PKI (third-party certificate services) • Symantec MPKI (third-party certificate services) **Note:** Since there is no need to go through EIS for cloud certificate services, if you want to integrate with certificate services (like Symantec MPKI) by selecting one of the check boxes in the screen above, the service you select must be on premises, not in the cloud.
AirWatch Services	Select which AirWatch components should use EIS configuration: • Device Services • Device Management (Enrollment, App Catalog) • Self-Service Portal • All Other Components

3. Click **Save** to keep these settings. View information about the authentication certificates used between AirWatch and the EIS server.

Note: The certificate generated during auto-configuration has the thumbprint located here. To clear and renew certificates, select **Clear Certificates** and follow the prompts

Appendix: Advanced Setup

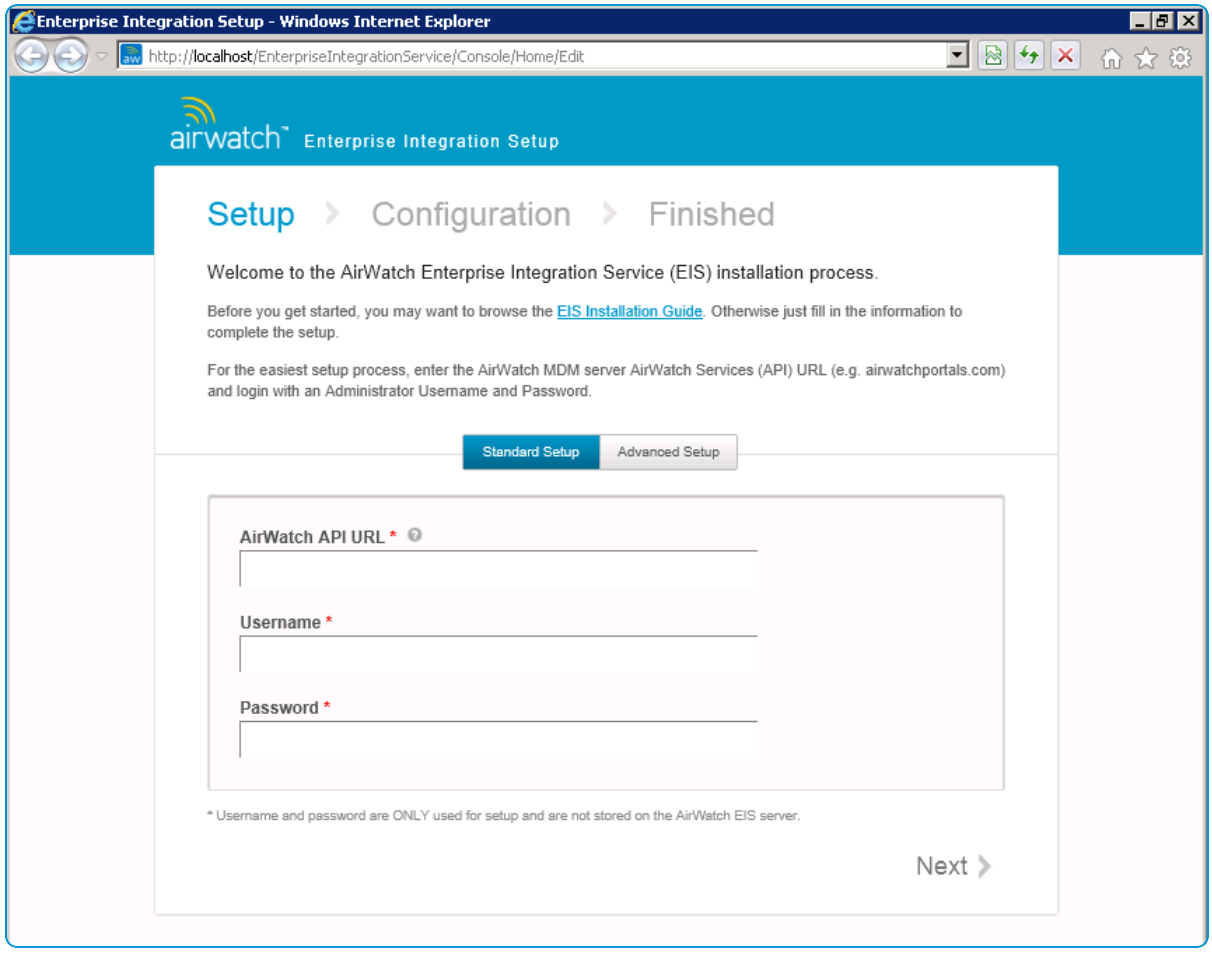
Overview

If EIS was unable to connect to the API during installation, or the firewall prevented connecting to the cloud, manually integrate AirWatch and EIS. To configure EIS offline, perform the following steps:

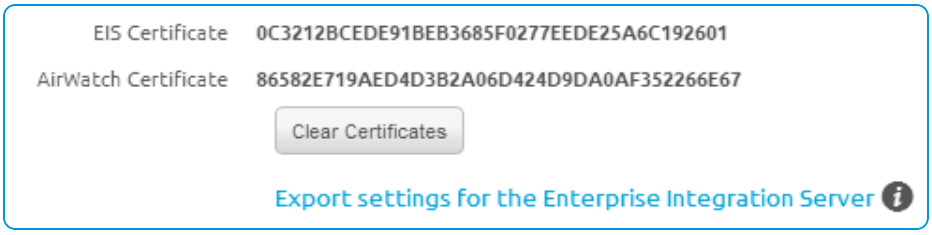
1. Generate Workspace ONE UEM and EIS certificates.
2. Export the settings in XML format from AirWatch.
3. Import the XML file into the **Advanced Setup** of the EIS configuration page.

Manually Integrating Workspace ONE UEM and EIS

1. Follow the EIS guide up to the point where you complete the installation and select **Finish**. For information, see EIS Installation
2. Choose the **Advanced Setup** tab after the EIS configuration page opens.



3. Reconfigure Workspace ONE UEM by performing all the steps in Configure Console.
4. Click **Export settings for the Enterprise Integration Service** after the EIS and Workspace ONE UEM certificates are created.



5. Set a password for the EIS certificate file.

> **Important:** Remember or write down this password because you will need it to upload the file into EIS.

6. Click **Export EIS Settings**. This step exports an XML file from the UEM console.
7. Upload the XML file from the previous step. Find the file on the **Advanced Setup** tab located on the EIS Configuration page. When prompted, enter the EIS password you entered in the **Export EIS Settings** screen. This export configures the EIS server with the settings in the XML file.

Appendix:
Configuring and Installing EISR

This is only for those who are installing a DMZ Relay. For a successful installation, you must do the following:

1. Install EIS server, but do not configure it. See Installing EIS.
2. Install EISR server. See Installing EIS.
3. Configure the EISR server by doing following:
   - Enter **AirWatch API URL** (e.g., asXX.airwatchportals.com).
   - Enter **Username** and **Password** for EIS server created within the UEM console.
   - Click **Next**.
   - Select appropriate **Organization Group**.
   - Click **Relay** radio button to select.
   - Enter the **EIS URL** (i.e., EIS server address).

     Make sure you can verify the EIS URL. Depending on how EIS is configured, you can verify the EIS URL using HTTP or HTTPS.
   - Click **Next** and then **Finish**.
4. Configure the EIS server as follows:
   - Enter **AirWatch API URL** (e.g., asXX.airwatchportals.com).
   - Enter the same **Username** and **Password** you used to configure EISR.
   - Click **Next**.
   - Select the same **Organization Group** you used to configure EISR.
   - Click **Endpoint** radio button to select.
   - Enter the **EIS URL** (i.e., EIS server address).
   - Click **Next** and then **Finish**.

   The VMware AirWatch API knows to forward all traffic through EISR to the EIS server. Respectively, EIS knows to forward all traffic through EISR to communicate with the Workspace ONE UEM SaaS.

Accessing Other Documents

While reading this documentation you may encounter references to documents that are not included here.

The quickest and easiest way to find a particular document is to navigate to docs.vmware.com and search for the document you need. Each release-specific document has a link to its PDF copy on myAirWatch.

Alternatively, you can navigate directly to myAirWatch (resources.air-watch.com) and execute a search. When searching for documentation on myAirWatch, be sure to select your Workspace ONE UEM version. You can use the filters to sort by PDF file type and Workspace ONE UEM v9.6.