

VMware AirWatch Windows Autodiscovery Service Installation Guide

Installing and configuring Windows Autodiscovery with AirWatch
For AirWatch versions 8.0 and higher

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

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Table of Contents

Chapter 1: Overview	3
Introduction to the Windows Auto-Discovery Service	4
Windows Auto-Discovery Service Requirements	4
Chapter 2: Cloud Hosted WADS Configuration	7
Cloud-Hosted WADS Overview	8
Obtain an SSL Certificate for Cloud Hosted WADS	8
Add a Domain to Workspace ONE UEM	8
Register the Domain for WADS	9
Chapter 3: WADS On-Premises Installation	11
On-Premises WADS Installation Overview	12
Obtain an SSL Certificate	12
Install the Windows Auto-Discovery Service	12
Bind the SSL Certificate	16
Enable WADS to use Workspace ONE UEM Auto-Discovery and Enrollment	18
Use Server Name Indication for Multi-Domain WADS	20
WADS Installation Verification	23

Chapter 1:

Overview

Introduction to the Windows Auto-Discovery Service	4
Windows Auto-Discovery Service Requirements	4

Introduction to the Windows Auto-Discovery Service

Windows Auto-Discovery provides simplified enrollment using the Workplace or Work Account native MDM client. During enrollment through the Workplace or Work Account native MDM client, the Windows Auto-Discovery service receives the domain name from an end-user's email address and provides their enrollment credentials.

This service simplifies enrollment for the end user. Windows Desktop and Windows Phone end users enter only their email address into the Workplace or Work Account native MDM client to begin the enrollment process.

You can either host your own on-premises WADS server or use the cloud-hosted deployment. Through on-premises deployment, your organization hosts all Workspace ONE UEM components and servers on its internal networks. The cloud-hosted deployment means Workspace ONE UEM hosts the Windows Auto-Discovery Service without the need for extra infrastructure setup and installation required in on-premises deployments.

Supported Configurations

WADS supports various enrollment methods for Windows devices.

- Windows Phone and Windows Desktop Simplified Enrollment.
- Leveraging Server Name Indication (SNI) to support multiple domains.
- Enabling Workplace Web Enrollment for Windows Phone 8.1.
- Using Workspace ONE UEM Auto-Discovery to return users Group ID.

Windows Auto-Discovery Service Requirements

Before configuring the Windows Auto-Discovery Service (WADS), consider the following prerequisites, requirements, supporting materials, and helpful suggestions from the Workspace ONE UEM team. Familiarizing yourself with the information available in this section helps prepare you for configuring the WADS.

Note: You can use Cloud Hosted or on-premises WADS regardless of your Workspace ONE UEM deployment method. On-premises customers can take advantage of Cloud Hosted WADS and SaaS customers can use an on-premises WADS solution.

On-Premises Requirements

Requirement	Notes
Hardware Requirements	
VM or Physical Server	1 CPU Core (2.0+ GHz) 2 GB RAM or higher 1 GB disk space for the WADS application, Windows OS, and .NET runtime. Consider having 5 GB of disk space for use with logging.
Remote access to Windows Servers available to Workspace ONE UEM and Administrator rights	Consider setting up Remote Desktop Connection Manager for multiple server management. Download the installer from: https://www.microsoft.com/en-us/download/details.aspx?id=44989

Requirement	Notes
SSL Certificate for Domain	SSL certificate for <code>enterpriseenrollment.{domain}</code> . For example, if you were to enter <code>jd@contoso.com</code> as your email address, the certificate must be obtained for <code>enterpriseenrollment.contoso.com</code> or <code>*.contoso.com</code> . The SSL certificate can be domain-specific or a wildcard certificate. If you are using Multi-Layer domains, a domain-specific certificate is required.
Software Requirements	
Windows Server 2008 R2 or Windows Server 2012 or Windows Server 2012 R2	Windows Server 2012 R2 is required for SNI support
Internet Information Services (IIS) 7 or higher	IIS is the Web server role in Windows Server Internet Information Services (IIS) 8.5+ is required for SNI support
Install .NET Framework 3.5	Add .NET 3.5 as a feature in Server Manager. After install perform ASP.NET IIS Registration
Install .NET Framework 4.0	Add .NET 4.0 as a feature in Server Manager.
Network Requirement	
443 – HTTPS (Inbound)	<code>EnterpriseEnrollment.<domain></code> (Accessible by devices)
443 – HTTPS (Outbound)	<code>discovery.awmdm.com</code> (OPTIONAL)
CNAME/ANAME	<code>EnterpriseEnrollment.<domain></code> (Accessible by devices)

Remote Access to Servers

Ensure that you have remote access to the servers that WADS is installed on. Typically, installations are performed remotely over a web meeting or screen share that a Workspace ONE UEM consultant provides. Some customers also provide Workspace ONE UEM with VPN credentials to directly access the environment .

Cloud Hosted Requirements

Cloud Hosted Windows Auto-Discovery requires a domain-specific SSL certificate for `enterpriseenrollment.{domain}`.

Requirement	Notes
Hardware Requirements	
SSL Certificate for Domain	<p>SSL certificate for enterpriseenrollment.{domain}. For example, if you were to enter jdoe@contoso.com as your email address, the certificate must be obtained for enterpriseenrollment.contoso.com.</p> <p>The SSL certificate can be domain-specific. If you are using Multi-Layer domains, a domain-specific certificate is required.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>Note: Cloud Hosted Windows Auto-Discovery does NOT support wildcard SSL certificates.</p> </div>
Network Requirement	
CNAME/ANAME	EnterpriseEnrollment.<domain> (Accessible by devices)

Chapter 2:

Cloud Hosted WADS Configuration

Cloud-Hosted WADS Overview	8
Obtain an SSL Certificate for Cloud Hosted WADS	8
Add a Domain to Workspace ONE UEM	8
Register the Domain for WADS	9

Cloud-Hosted WADS Overview

Instead of hosting an on-premises deployment of the Windows Auto-Discovery Service, you can use the cloud-hosted deployment from Workspace ONE UEM. The cloud-hosted deployment means Workspace ONE UEM hosts the Windows Auto-Discovery Service without the need for extra infrastructure setup and installation required in on-premises deployments.

The Cloud Hosted Windows Auto-Discovery Service configuration wizard guides provides step-by-step instructions for hosting your Window Auto Discovery Service through Workspace ONE UEM.

Cloud Hosted Auto-Discovery requires a domain-specific SSL Certificate for the enterpriseenrollment subdomain to be uploaded to Workspace ONE UEM before configuration.

Important: Cloud-Hosted WADS requires AirWatch v8.0 and above.

Obtain an SSL Certificate for Cloud Hosted WADS

The Windows Auto-Discovery Service (WADS) requires because native enrollment for Windows devices does not connect to untrusted servers. Obtain a domain-specific or wildcard SSL certificate for **enterpriseenrollment.{domain}**.

You must obtain this certificate yourself. Consider purchasing a certificate that remains active for at least three (3) years to minimize time and resources required to perform the administrative tasks of renewing certificates.

Note: You must generate your own CSRs for your SSL certificates using your own servers regardless of using cloud-hosted WADS or on-premises WADS.

To obtain an SSL certificate:

1. Obtain a domain-specific or wildcard SSL certificate for **enterpriseenrollment.{domain}**. The certificate must be a certificate type that contains the private key such as .pfx or .p12. If your certificate is not one of those file types, you must convert it before uploading it to the Workspace ONE UEM Console.

For instance, if you were to enter jdoe@acme.com as your email address, the certificate must be obtained for enterpriseenrollment.acme.com or *.acme.com. If you are using a sub domain, the certificate cannot be a wildcard certificate and must be domain-specific. For example, if you are entering jdoe@ga.acme.com as your email address the certificate must be obtained for **enterpriseenrollment.ga.acme.com**.

2. Create a CNAME/ANAME record for enterpriseenrollment.{domain} to point to your WADS server.

Add a Domain to Workspace ONE UEM

Before you can register a domain using an SSL certificate, you must first add the domain to the Workspace ONE UEM console. This domain associates end-user email addresses with their enrollment credentials.

To add a domain:

1. Navigate to **Devices > Device Settings > Devices & Users > General > Enrollment**, select the **Authentication** tab and then select **Add Email Domain**.

2. Select the **Organization Group** you want to associate with this domain and then enter your **Business Email Domain** and **Confirmation Email Address**. This organization group associates end users to your environment and serves as the starting point for possible Group ID selection prompts.
3. Verify your email address by selecting the confirmation link in the email sent to the address you provided.
4. Add more **Business Email Domains** as required, such as "us.example.com" or "eu.example.com."
 - Multiple email domains can be added to the same organization group level.
 - Consider adding alternative email domains to other organization groups to facilitate multi-tenancy.
5. Select **Save** to complete the autodiscovery setup.

Register the Domain for WADS

After obtaining an SSL certificate, register your domain for Auto-Discovery in the Workspace ONE UEM Console. The registered domain connects end-user email addresses to the enrollment credentials.

To register a domain:

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Auto-Discovery**.
2. Set the **Auto Discovery Mode** to **Cloud Hosted**.
3. Select **Register Domain for Windows Auto-Discovery**.

The screenshot shows the 'Windows Auto-Discovery' configuration interface. It is divided into three numbered sections:

- 1 Please select the domain for which you want to register Windows Auto-Discovery or [Register a new domain](#)**
 Domain: Refresh List
- 2 Create CNAME Record**
 - a. Navigate to your DNS Management page and find the CNAME settings.
 - b. Enter the following CNAME value or alias :
 - c. Set The CName Destination Url
 - d. Save The Changes And Verify By Clicking
- 3 Upload SSL Certificate For**
 SSL Certificate:

A yellow warning banner at the bottom states: **⚠ AirWatch will only accept a domain specific certificate and not a wildcard certificate.**

At the bottom of the form are and buttons.

4. Select the **Domain** for which you want to register WADS. If you have not yet created a domain, select **Register a new domain**. For more information on setting up an email domain, see [Add a Domain to Workspace ONE UEM](#).
5. Create a CNAME Record by following the steps on the screen.

6. Select **Upload** to add your SSL certificate.

Note: Workspace ONE UEM only accepts a domain-specific certificate and not a wildcard certificate.

7. Select **Save**.
8. Confirm that your domain is properly added and registered and select **Save**.

Note: It may take up to 30 minutes to register the domain for cloud-hosted WADS.

Chapter 3:

WADS On-Premises Installation

On-Premises WADS Installation Overview	12
Obtain an SSL Certificate	12
Install the Windows Auto-Discovery Service	12
Bind the SSL Certificate	16
Enable WADS to use Workspace ONE UEM Auto-Discovery and Enrollment	18
Use Server Name Indication for Multi-Domain WADS	20
WADS Installation Verification	23

On-Premises WADS Installation Overview

Windows Auto-Discovery for Windows devices requires the Windows Auto-Discovery Service installed onto a server. This server must meet the minimum requirements and have access to your internal network.

The Windows Auto-Discovery Service (WADS) is a web service installed on a physical or virtual server running Windows 2008 R2+ on Internet Information Services (IIS) 7+. It operates from within your DMZ or internal network and can be configured behind any existing Web Application Firewalls (WAF) or load balancers. By initiating a secure HTTPS connection from the Windows Phone or Windows Desktop devices to the WADS server, end users receive enrollment credentials, depending on optional configurations.

The installation process requires:

- Obtaining an SSL certificate for EnterpriseEnrollment.<domain>.
- Obtaining the executable for the Windows Auto-Discovery Service.
- Downloading and installing WADS onto server.
- Binding SSL certificate to the EnrollmentServer virtual directory.
- (Optional) enabling WADS to use Workspace ONE UEM Auto-Discovery.
- (Optional) enabling WADS to use Workplace Web Enrollment.

Obtain an SSL Certificate

The Windows Auto-Discovery Service (WADS) requires because native enrollment for Windows devices does not connect to untrusted servers. Obtain a domain-specific or wildcard SSL certificate for **enterpriseenrollment.{domain}**.

You must obtain this certificate yourself. Consider purchasing a certificate that remains active for at least three (3) years to minimize time and resources required to perform the administrative tasks of renewing certificates.

To obtain an SSL certificate:

1. Obtain a domain-specific or wildcard SSL certificate for **enterpriseenrollment.{domain}**.
For instance, if you were to enter `jdoe@acme.com` as your email address, the certificate must be obtained for `enterpriseenrollment.acme.com` or `*.acme.com`. If you are using a sub domain, the certificate cannot be a wildcard certificate and must be domain-specific. For example, if you are entering `jdoe@ga.acme.com` as your email address the certificate must be obtained for **enterpriseenrollment.ga.acme.com**.
2. Create a CNAME/ANAME record for `enterpriseenrollment.{domain}` to point to your WADS server.

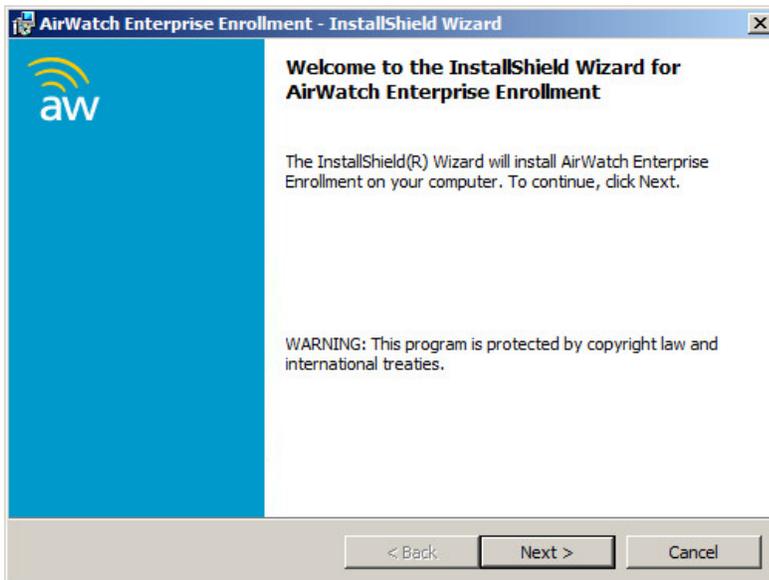
Install the Windows Auto-Discovery Service

The Windows Auto-Discovery Service Installer guides you through a step-by-step process for installing and configuring WADS for an on-premises deployment.

To install WADS:

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Auto-Discovery**.
2. Set the **Auto Discovery Mode** to **On-Prem**.

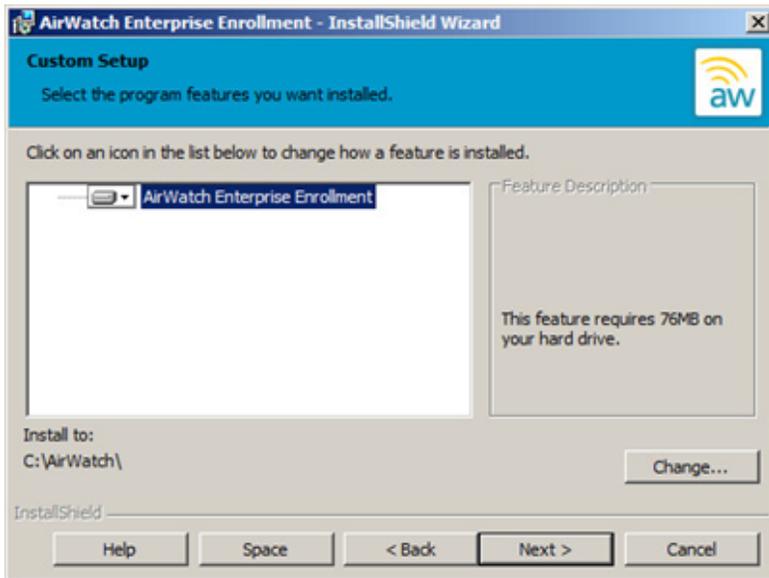
3. Select **Download Windows Auto-Discovery Installer**.
4. Unpackage the installer.
5. Run the installer as an Administrator.



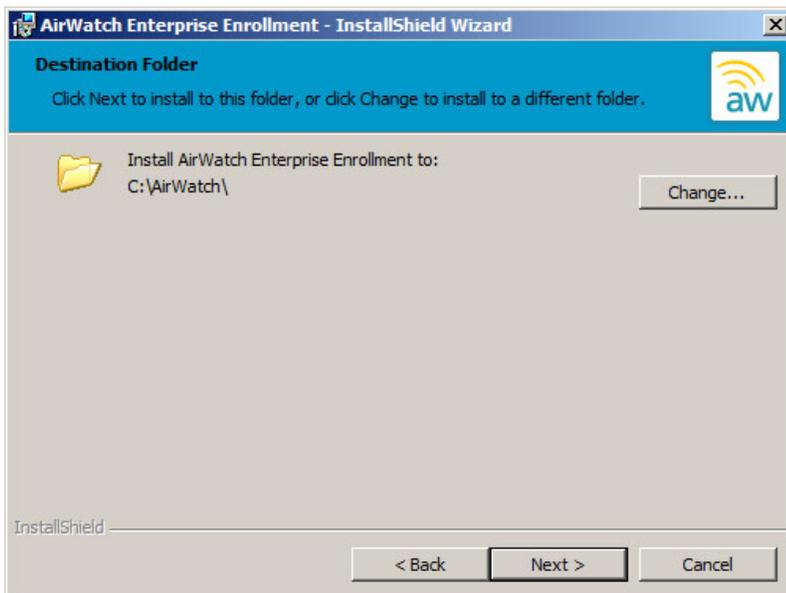
6. Click **Next** to begin installing WADS.
7. Accept the terms in the EULA to continue.



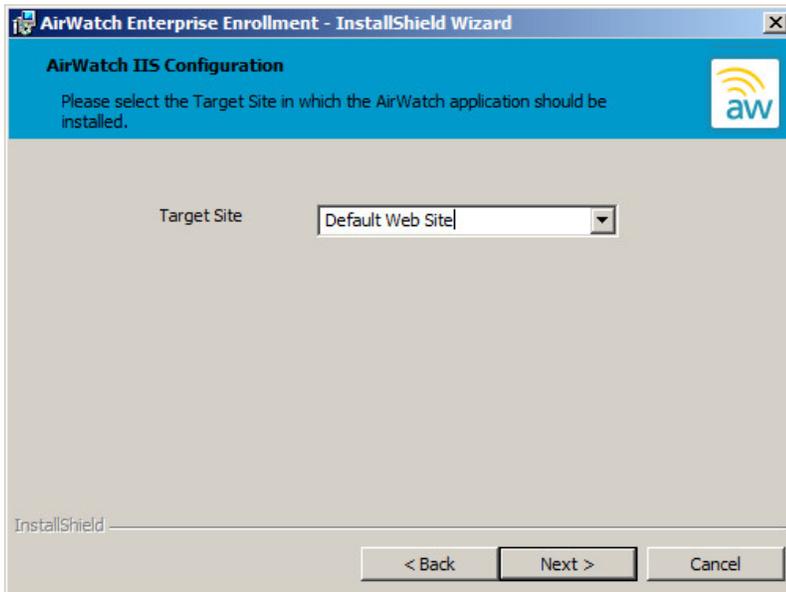
8. Choose your **Install** path then select **Next** to continue.



9. Confirm that your **Installation Path** then select **Next** to continue.

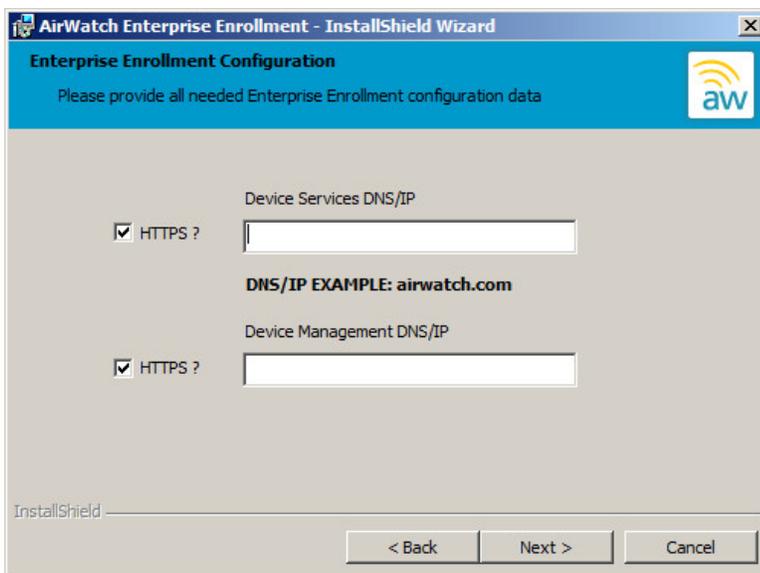


10. On the Workspace ONE UEM IIS Configuration screen, select the Web site being used.

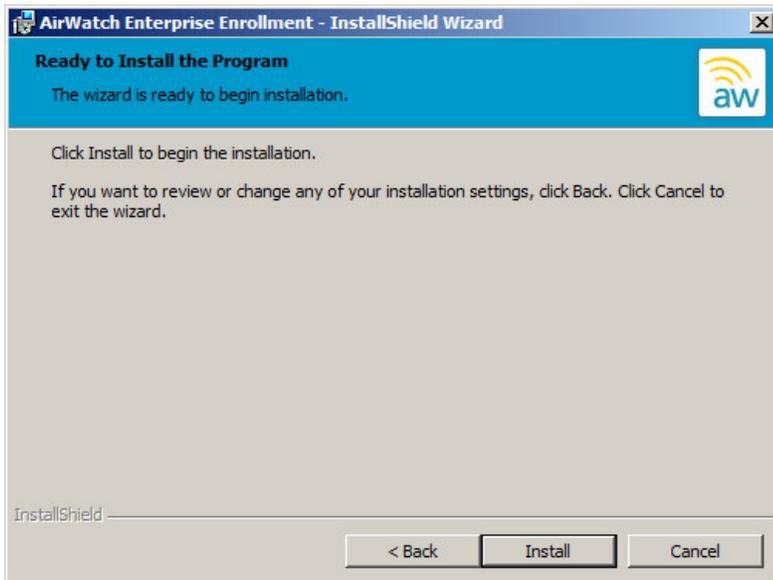


To use a Web site other than the Default Web site, type the Web site name in the text box. If you are planning on using multiple domains, enter the site name provided while configuring SNI. For more information, see [Use Server Name Indication for Multi Domain WADS](#).

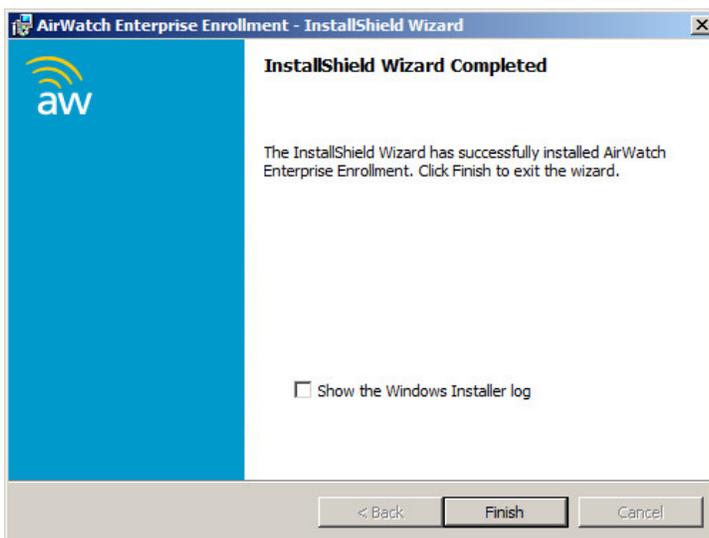
11. Enter the URL of the Device Services server. This URL can be found by navigating to Site URLs in the Console. **Groups and Settings > All Settings > System > Advanced > Site URLs**. Do not enter HTTPS:// in the installer text boxes. For example, if the Device Services URL listed in Site URLs is `https://ds16.airwatchportals.com/DeviceServices`, enter `ds16.airwatchportals.com` in the installer text boxes.



12. Click **Install** to begin the installation.



13. Click **Finish**.



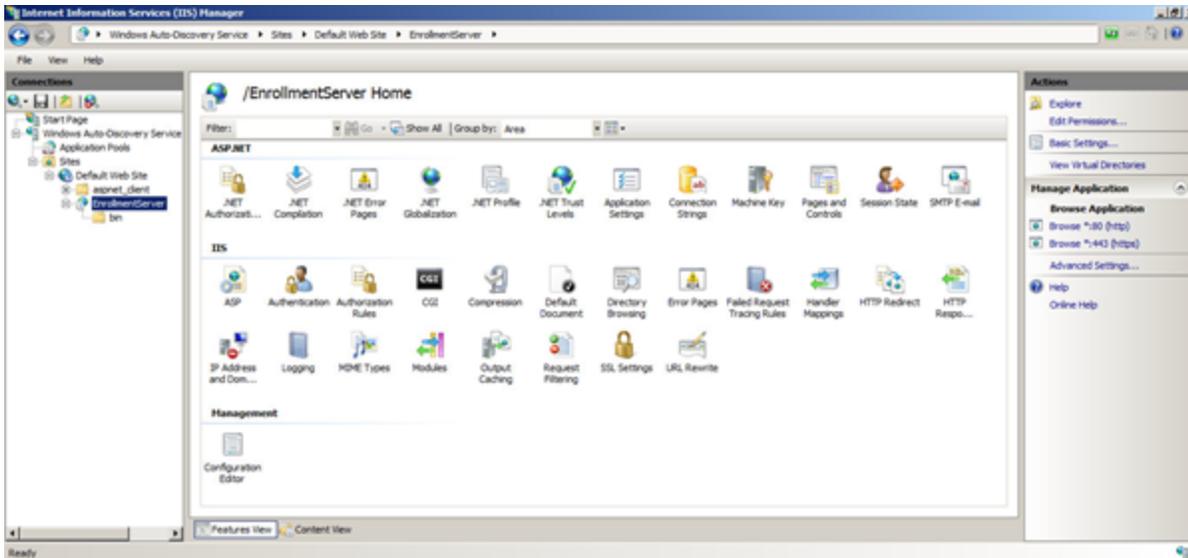
Note: Click Show the Windows Installer log to see detailed logs of the installation or to troubleshoot.

Bind the SSL Certificate

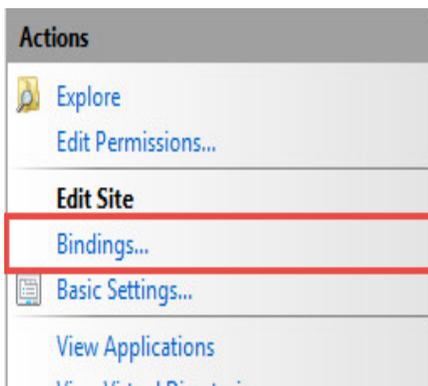
After obtaining the wildcard or domain-specific SSL certificate, bind the certificate to your site using IIS. Workplace on Windows 8.1 devices do not connect to any untrusted servers, so you must bind your SSL certificate to the site on port 443.

To bind the SSL certificate:

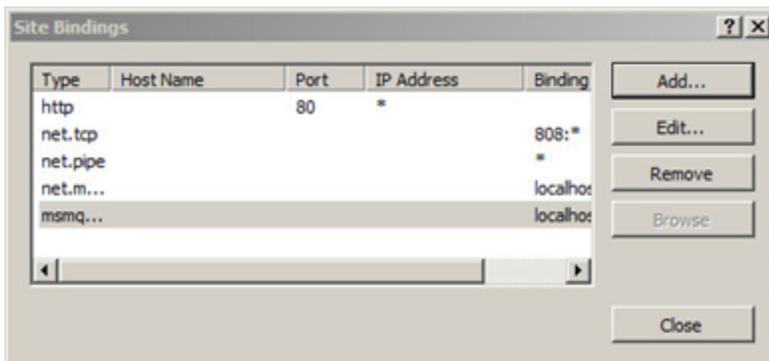
1. Open the Internet Information Services (IIS) Manager and navigate to the Default Web site.



2. Click **Bindings** on the right pane under **Actions**.



3. Click **Add** to create a binding.



4. Change the following settings:

- **Type** to **https**
- **Port** to **443**

- **SSL Certificate** to your wildcard or domain-specific certificate for the Windows Auto-Discovery Service.
- **IP Address** is optional.



5. Click **OK** to save settings.

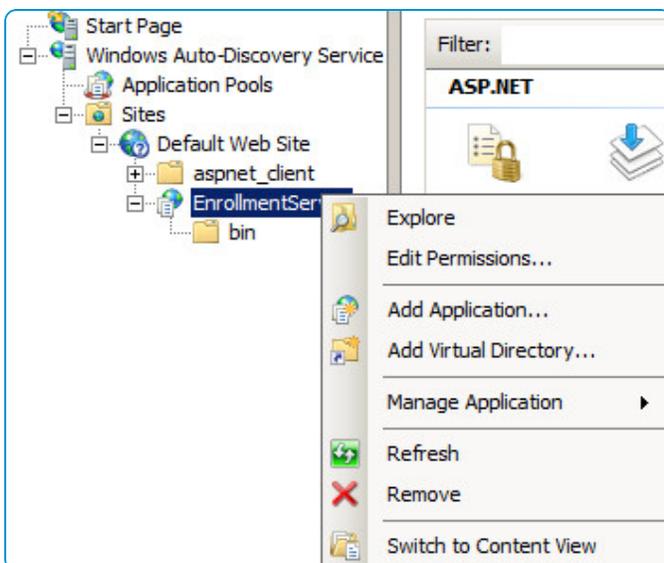
Enable WADS to use Workspace ONE UEM Auto-Discovery and Enrollment

Workspace ONE UEM Auto-Discovery provides the siouerver URL and group ID for end-users based on their email address. Configure WADS to query Workspace ONE UEM Auto-Discovery to simplify enrollment for your end users.

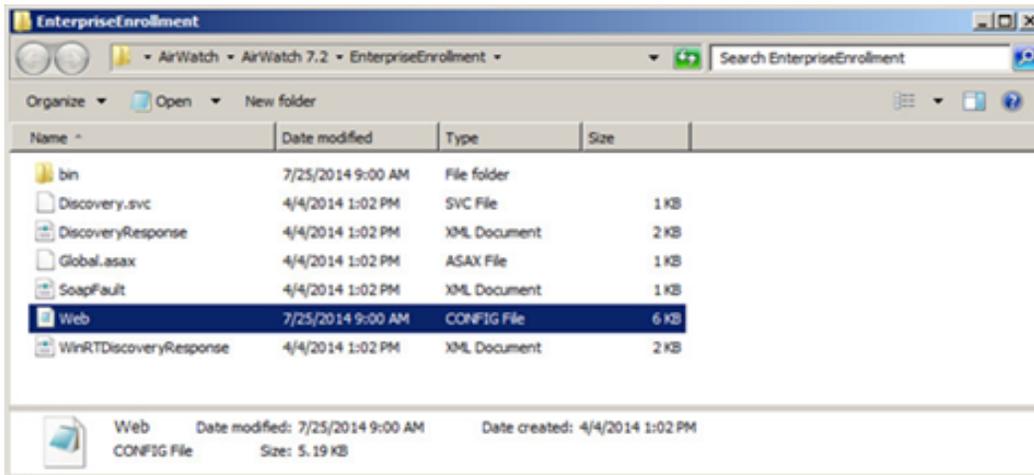
You can also enable the Windows Workplace Web enrollment method. This enrollment flow enables the ability to display the optional enrollment screens during workplace enrollment on Windows Phone and Windows Desktop devices. These screens include device ownership type, welcome messages, and asset number prompt. This flow allows for a similar enrollment experience across platforms while gathering additional information from the end user if needed.

To enable Workspace ONE UEM Auto-Discovery and Enrollment:

1. On the server hosting the Auto-Discovery Install, open Windows Explorer and navigate to **EnrollmentServer**.
2. Right click the **EnrollmentServer** virtual directory, then select **Explore**.



3. Open and edit the **Web.config** file to customize the settings.



4. Edit the following configuration file to customize your WADS setup to meet your enrollment needs.

Key	Value	Notes
WebEnrollmentEnabled	True	Enabling this option displays the optional enrollment screens, such as device ownership type, welcome messages, and asset number prompt, to the end user during workplace enrollment on Windows Phone 8.1 and above.
WebEnrollmentEnabled	False	Disabling this option prevents the optional enrollment screens during workplace enrollment on Windows Phone 8.1+ and only uses workplace for enrollment.
UseAirwatchAutoDiscovery	True	Enabling this option allows for the Windows Auto-Discovery Service to query Workspace ONE UEM Auto-Discovery for registered email domains and returns the server URL and group ID for the end user. This option eliminates the need for the end user to have to enter the Group ID. If enrolling Windows Phone 8, consider setting this value to true, otherwise this key is optional. WADS must reach discovery.awmdm.com on port 443.
UseAirwatchAutoDiscovery	False	End users are asked to enter group ID if set to false, unless enrolling Windows Phone 8.1 with Web enrollment enabled. Consider setting the option to true when possible to simplify enrollment for end users.

Key	Value	Notes
DeviceServicesUrl	N/A	Enter the URL of the Device Services server. This URL can be found by navigating to Site URLs in the Console. Groups and Settings > All Settings > System > Advanced > Site URL . Do not enter HTTPS:// in the installer text boxes. For example, if the Device Services URL listed in Site URL is https://ds16.airwatchportals.com/deviceservices, enter ds16.airwatchportals.com in the installer text boxes.
DeviceManagementUrl	N/A	Enter the URL of the Device Management server. This URL can be found by navigating to Site URLs in the Console. Groups and Settings > All Settings > System > Advanced > Site URL . Do not enter HTTPS:// in the installer text boxes. For example, if the Device Management URL listed in Site URL is https://ds16.airwatchportals.com/devicemanagement, enter ds16.airwatchportals.com in the installer text boxes.
Level	Error	Default value, catches all errors and information
Level	Verbose	Switch to Verbose when troubleshooting, provides more logs

Use Server Name Indication for Multi-Domain WADS

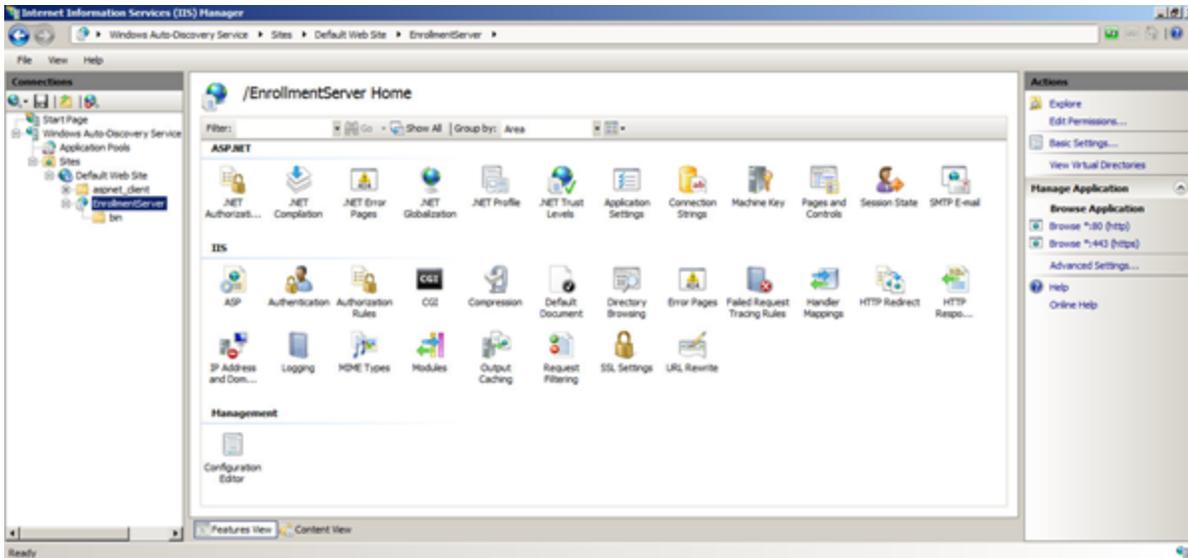
If you are using multiple domains for enrollment, use Server Name Indication to simplify installation and reduce the server overhead.

Multiple domains normally require multiple servers, SSL certificates, and IP addresses. To reduce issues and overhead, use Server Name Indication (SNI) to use only one server supported by multiple SSL certificates, and CNAME/ANAME records pointing to this SNI supported server.

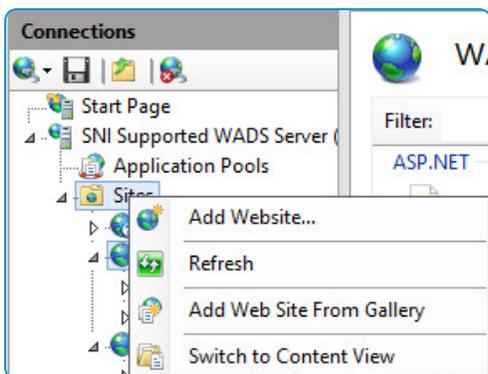
Note: For SNI, you need Windows Server 2012 R2 with IIS 8.0+.

To configure SNI:

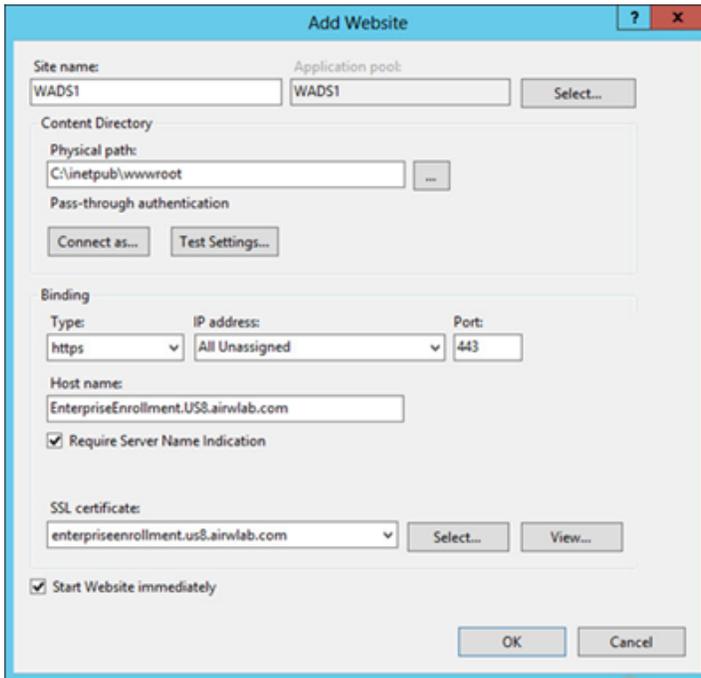
1. Open the Internet Information Services (IIS) Manager.



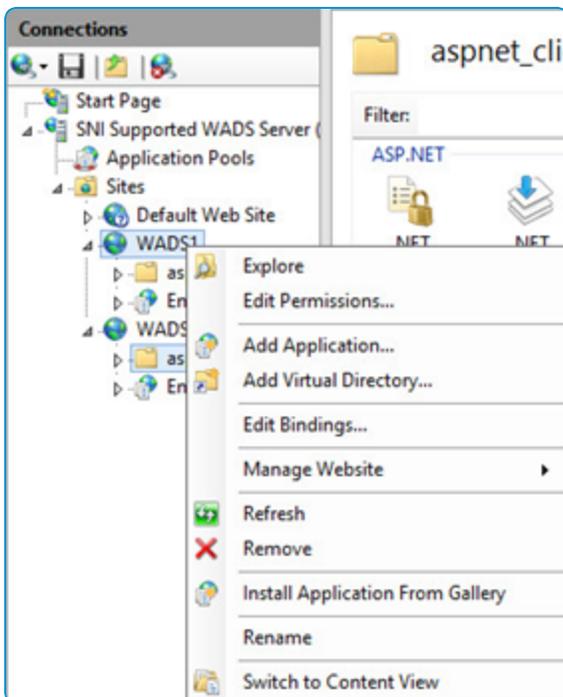
2. Right click **Sites**, then select **Add Website**.



3. Fill in your **site name**, **physical path**, and **host name**. Change type to **https** and to check **Require Server Name Indication**, and selecting the matching **SSL certificate**.



4. Right-click your Web site and select **Add Application**.



5. If you have not already, you must run the WADS installer. Change the Web site from **Default Web Site** to the **site name** provided in the previous steps. Once completed, the first domain has been successfully configured. To add more domains, repeat steps 2–4 and continue to step 6.
6. Fill in **Alias** as **EnrollmentServer** and update the **Application Pool** to point to **EnrollmentServer**. Click the contextual dots (...) to browse for the **EnterpriseEnrollment** directory created after the WADS setup was run.

The screenshot shows the 'Add Application' dialog box with the following configuration:

- Site name: WADS1
- Path: /
- Alias: EnrollmentServer
- Application pool: EnrollmentServer
- Example: sales
- Physical path: C:\AirWatch\AirWatch 7.1\EnterpriseEnrollment
- Pass-through authentication: Connect as... and Test Settings...
- Enable Preload:

WADS Installation Verification

After you configure the Windows Auto-Discovery Service, use a REST client to issue a POST request to your WADS endpoint.

The POST request must connect to the correct endpoint URL:

`https://EnterpriseEnrollment.{DOMAIN}/EnrollmentServer/Discovery.svc`

Note: Make sure that the device can reach `https://EnterpriseEnrollment.{DOMAIN}` without any SSL errors.

Example of a Request Body

```
<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <a:Action
      s:mustUnderstand="1">http://schemas.microsoft.com/windows/management/
      2012/01/enrollment/IDiscoveryService/Discover
    </a:Action>
    <a:MessageID>urn:uuid:748132ec-a575-4329-b01b-6171a9cf8478</a:MessageID>
    <a:ReplyTo>
      <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
    </a:ReplyTo>
    <a:To s:mustUnderstand="1">https://EnterpriseEnrollment.
      {DOMAIN}:443/EnrollmentServer/Discovery.svc
    </a:To>
```

```

</s:Header>
<s:Body>
  <Discover xmlns= "http://schemas.microsoft.com/windows/management/
  2012/01/enrollment">
    <request xmlns:i= "http://www.w3.org/2001/XMLSchema-instance">
      <EmailAddress>{EMAIL ADDRESS}</EmailAddress>
      <RequestVersion>1.0</RequestVersion>
    </request>
  </Discover>
</s:Body>
</s:Envelope>

```

Example of an Expected Response

```

<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <a:Action
      s:mustUnderstand="1">http://schemas.microsoft.com/windows/management/201
      2/01/enrollment/IDiscoveryService/DiscoverResponse
    </a:Action>
    <ActivityId
      xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics"
      CorrelationId="48915517-66c6-4ab7-8f77-c8277e45b3cf=">
      a4067bc9-ce15-446b-a3f7-5ea1006256f5</ActivityId>
    <a:RelatesTo>urn:uuid:748132ec-a575-4329-b01b-6171a9cf8478</a:RelatesTo>
  </s:Header>
  <s:Body>
    <DiscoverResponse
      xmlns="http://schemas.microsoft.com/windows/management/2012/01/enrollmen
      t">
      <DiscoverResult xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
        <AuthPolicy>Federated</AuthPolicy>
        <AuthUrl>prod</AuthUrl>
        <AuthenticationServiceUrl>https://{DS
        HOSTNAME}/DeviceManagement/Enrollment</AuthenticationServiceUrl>
        <EnrollmentPolicyServiceUrl>https://{DS
        HOSTNAME}/DeviceServices/Policy.svc</EnrollmentPolicyServiceUrl>
        <EnrollmentServiceUrl>https://{DS
        HOSTNAME}/DeviceServices/Enrollment.svc</EnrollmentServiceUrl>
      </DiscoverResult>
    </DiscoverResponse>
  </s:Body>
</s:Envelope>

```