Email Notification Service 2 (ENS2)

VMware Workspace ONE UEM 1907

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Introduction 1

Workspace ONE UEM powered by AirWatch Email Notification Service (ENS) adds Push Notification support to Exchange.

Workspace ONE Boxer provides notifications about your emails by running in the background. Due to platform limitations, Boxer can only run in the background for a limited time. Email Notification Service (ENS2) provides a solution to deliver notifications to user's device when Boxer is not running.

ENS2 supports notifications that includes the email subject and a badge icon (iOS only) to notify the number of unread emails in the Inbox on the server.

ENS2 can be configured with the Secure Email Gateway (SEG) V2 to secure your organization's email infrastructure. For more information about SEG, see the *Workspace ONE UEM Secure Email Gateway Guide (SEG) V2* guide.

This documentation provides the information required to install and configure the ENS2 as a cloud-hosted or On-Premises service.

ENS2 with Boxer

ENS2 uses Exchange Web Services (EWS) subscriptions to notify changes in users' mailboxes. The EWS subscriptions can go inactive due to different reasons and the systems involved should check to make sure that the subscriptions are active.

ENS2 uses a check-in mechanism within Boxer and also proactively checks the EWS subscription status to ensure the continuous delivery of notifications. The check-in mechanism used by ENS2 require intervention from Boxer to renew the EWS subscriptions. The functionality of ENS2 also depends on the Apple Push Notification Service (APNS) to deliver silent notifications to the device. ENS2 supports Certificate Based Authentication (CBA), Basic Auth, and OAuth on EWS.

The dependency of ENS2 on EWS and APNs can cause the following scenarios:

- No push notifications received when device notification is set to Do Not Disturb
- Inaccurate badge counts that is updated after receiving an email
- If Boxer is in a `killed` state, the device is not registered again for notifications. Due to this, the user will experience loss of ENS notifications. But when the device is active, and Boxer is activated, it will trigger the ENS subscription again, and the user will start receiving notifications.

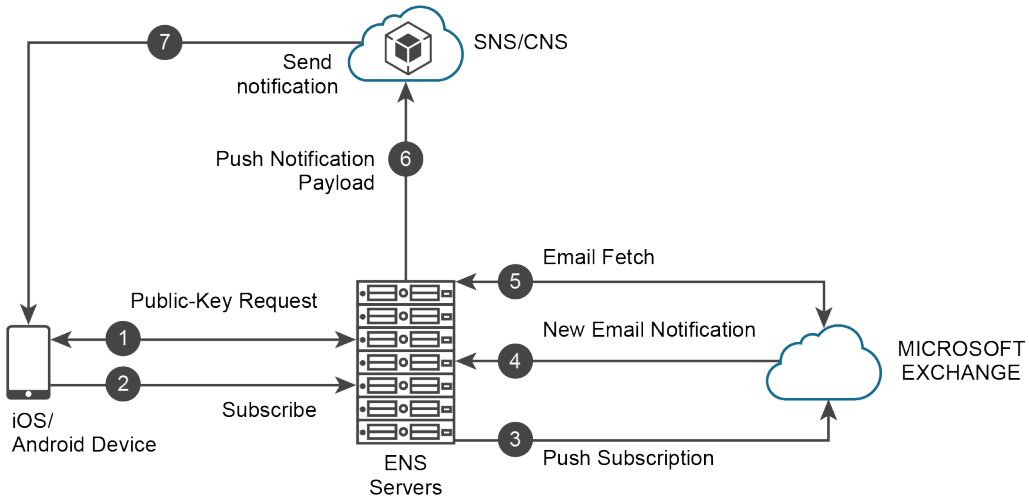
Bringing the Boxer app to the foreground enables the ENS2 to renew EWS subscriptions and solve the notification errors.

This chapter includes the following topics:

Architecture Overview

This section provides information about the architecture design and functionality of ENS2.

ENS2 Architecture using SNS or CNS



Architecture Flow Description

1 Public-Key Request - The device requests a public key to encrypt the account credentials.

2 Subscribe - The device sends an encrypted payload with credentials and all the necessary information to subscribe and get email notifications.

3 Push Subscription - ENS authenticates with EWS and subscribes for push notifications using a webhook URL. The webhook URL contains the encrypted credentials. The credentials are now kept encrypted on the Exchange server.

4 New Email Notification -

- Exchange sends notification about the mailbox changes to the provided webhook URL.
- ENS extracts and decrypts the credentials and prepares call to fetch emails.

5 Email Fetch - ENS performs a fetch for the email details (subject and sender) required for providing a notification.

6 Push Notification Payload - ENS pushes email details for delivery to all devices belonging to the user through SNS (ENS Cloud Deployments) or CNS (ENS On-Premises Deployments).

7 SNS or CNS sends notifications to iOS or Android devices. For iOS devices, SNS or CNS uses Apple Push Notification Service (APNs), and for android devices, SNS or CNS uses Firebase Cloud Messaging (FCM).

Requirements

This section explains the requirements for using the ENS2 with Workspace ONE UEM.

Email Server Integration Supported Versions

- Email Client - For Android support, you must have ENS2 1.3.0.4 or later and Workspace ONE Boxer 5.2 or later.
- Email Server - Exchange 2010 SP3, Exchange 2013 SP1, Exchange 2016, or Office 365

Workspace ONE UEM Requirements

- Cloud Deployment: Workspace ONE UEM console 8.4 or later
- On Premises Deployment: Workspace ONE UEM console 9.3 or later

Hardware Requirements (On-Premises Only)

Table 1-1. Web Server

CPU Core	RAM	Hard Disk Storage	Notes
2 (Intel processor)	16 GB (8GB minimum)	30 GB	Per 100,000 users.

Table 1-2. Database Server

CPU Core	RAM	Hard Disk Storage	Notes
2 (Intel processor)	16 GB (minimum)	Approx. 0.0477 MB per user to estimate the DB storage size.	Per 100,000 users.

Software Requirements

From ENS2 v1.3 , you must upgrade your CNS from CNS v1.0 to CNS v2.0 to support notifications.

Requirement (On-Premises)	Notes
Windows Server 2008 R2 or Windows Server 2012 R2 or Windows Server 2016	The servers should be externally accessible via https (SSL Cert) and with a Fully Qualified Domain Name (FQDN)
SQL Server 2012–2016 (Database Server)	The db_owner role and public role must be assigned to the SQL server user that is used for running the application
Basic Authentication for the Exchange environment	OAuth and Certificate Based Authentication (CBA) is supported for Exchange Web Services
CNS Certificate	
Secure Channel Certificate	
IIS 7 or later	Installed on Web Server
Requirement (Cloud)	Notes

Requirement (On-Premises)	Notes
Basic Authentication for the Exchange environment	OAuth and Certificate Based Authentication (CBA) is supported for Exchange Web Services
Autodiscovery enabled in Exchange environment and Internet-facing EWS environment. If autodiscovery is disabled, you can use the EWSUrl key value pair to configure ENS.	

Networking Requirements

Table 1-3. Network Ports

Source	Destination	Protocol (Port)
ENS	Exchange (EWS)	HTTPS (443)
Exchange (EWS)	ENS	HTTPS (443)
ENS	AirWatch Cloud Notification Service (CNS)	HTTPS (443)
ENS	SQL Server Instance	SQL (1433)
Internet (Devices)	ENS	HTTPS (443)

Table 1-4. IIS Services

Component Name	Required Services
Web Management Tools	IIS 6 Management Compatibility
IIS Management Console	
IIS Management Scripts and Tools	
IIS Management Service	

Table 1-5. World Wide Web Services

Component Name	Required Services
Application Development Features	.NET Extensibility 3.5
.NET Extensibility 4.6	
Application Initialization	
ASP	
ASP.NET 3.5	
ASP.NET 4.6	
ISAPI Extensions	
ISAPI Filters	
Server-Side Includes	
WebSocket Protocol	
Common HTTP Features	Default Document
Directory Browsing	

Component Name	Required Services
HTTP Errors	
Static Content	
Health and Diagnostics	HTTP Logging
Performance Features	Static Content Compression
Security	Request Filtering

SQL Server and High Availability Support

High availability configuration - ENS2 supports SQL Server AlwaysOn high availability configuration. Follow Microsoft guidelines to set up SQL Server AlwaysOn. If you are using AlwaysOn, point to the availability group when choosing the database server during ENS2 installation.

TLS Support for ENS

ENS supports TLS version 1.0 to TLS version 1.3. ENS does not choose any protocol, but allows the OS to choose the strongest available TLS version and the cipher suites. The following table lists the recommended cipher suites.

Cipher Suites	SSL Cipher Strength	TLS Protocol Version	Elliptic Curve Variants	Cryptographic Algorithm	Authenticated Encryption	Cryptographic Hash Algorithm
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	TLS 1.2	ECDH-ephemeral	ECDSA	AESGCM (128)	SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	TLS 1.2	ECDH-ephemeral	ECDSA	AESGCM (256)	SHA256 and SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	TLS 1.2	ECDH-ephemeral	ECDSA	AES (128)	SHA1
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	TLS 1.2	ECDH-ephemeral	ECDSA	AES (256)	SHA1
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	TLS 1.2	ECDH-ephemeral	ECDSA	AES (128)	SHA256

Cipher Suites	SSL Cipher Strength	TLS Protocol Version	Elliptic Curve Variants	Cryptographic Algorithm	Authenticated Encryption	Cryptographic Hash Algorithm
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384	TLS 1.2	ECDH-ephemeral	ECDSA	AES (256)	SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	TLS 1.2	ECDH-ephemeral	RSA	AESGCM (128)	SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	TLS 1.2	ECDH-ephemeral	RSA	AESGCM (256)	SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	TLS 1.2	ECDH-ephemeral	RSA	AES (128)	SHA1
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	TLS 1.2	ECDH-ephemeral	RSA	AES (256)	SHA1
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256	TLS 1.2	ECDH-ephemeral	RSA	AES (128)	SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	TLS 1.2	ECDH-ephemeral	RSA	AES (256)	

Enabling and Securing Communication Between the Exchange Server and the Email Notification Server

2

Enable and secure communication between the Exchange server and the ENS server.

To ensure a successful communication between the Exchange and the ENS servers, note the following points:

- Communication between ENS and Exchange servers should not have any SSL errors.
- `telnet` and `ping` commands should work seamlessly between ENS and Exchange CAS/Mailbox servers.
- SSL certificates used for ENS and Exchange servers should not have any errors when they are run through SLL checkers.

This chapter includes the following topics:

Upload Root CA Certificate

Upload the root CA certificate to the Exchange server.

Procedure

1. Download the SSL certificate from the ENS server. Access the ENS Alive endpoint in a browser and download the certificate from the address bar.

   You must only download the root certificate issued by a trusted authority and signed by an internal CA. For cloud deployment, you can download the root certificate from https://ens.getboxer.com/api/ens/alive, https://ens-eu.getboxer.com/api/ens/alive, or https://ens-apj.getboxer.com/api/ens/alive based on your region, issued by VMware for your account.

   For On-Premise deployment, download the root certificate and replace acme.com with the resolved name or IP address of your ENS server.
2. Import this certificate on the Exchange Server into the **Trusted Root Certification Authorities** through MMC.

Email Notification Service for Cloud

3

Use Workspace ONE UEM console to configure Workspace ONE Boxer for your cloud deployment.

Configure the Email Notification Service 2 (ENS2) related settings for Workspace ONE Boxer on the Workspace ONE UEM console.

Prerequisites

- An API token and ENS2 server URL received from VMware is required to activate the ENS service using the Workspace ONE UEM console.
- Ensure the ENS server certificate is available on the user's Exchange server. See Chapter 2 Enabling and Securing Communication Between the Exchange Server and the Email Notification Server.

Procedure

1. Select the required organization group.
2. Select **APPS & BOOKS** and then select the **Public** tab.
3. Select **VMware Boxer**.
4. Select **Edit** on the upper right corner of the page and then select the **Assignment** tab.
5. On the **Application Configuration (Optional)** section, add the required keys.

Configuration Key	Value Type	Configuration Value	Description
ENSLinkAddress	String	Supported format: https://ens.getboxer.com/api/ens Replace `ens.getboxer.com` with the resolved name or IP provided by VMware based on your region. Sample link address: ■ For AMER - https://ens.getboxer.com/api/ens ■ For APAC - https://ens-apj.getboxer.com/api/ens ■ For EMEA - https://ens-eu.getboxer.com/api/ens	Provide the address for the ENS2 system for your users to connect.
ENSAPIToken	String	Sample API Token: +eXaml3_AP1=	API Token provided by VMware AirWatch to activate the ENS service.

Configuration Key	Value Type	Configuration Value	Description
AccountNotifyPush	Boolean	False - disable (default) True - enable	Enables ENS for the account.
EWSUrl	String	Supported Format: https://[external_email_server_domain]/EWS/Exchange.asmx Sample EWS URL: ■ https://e.mail.com/EWS/Exchange.asmx ■ https://seg.dom.com/EWS/Exchange.asmx	Enables manual configuration of Exchange Web Services (EWS) endpoint when autodiscovery is disabled in your Exchange environment.

6 Select **Save & Publish** and then select **Publish** on the next page.

ENS Endpoints and IP Whitelist

The API endpoints supported by ENS2 are listed in this topic.

When using cloud ENS servers, you must ensure that the ENS is accessible from the Exchange or Office 365 environment. The inbound IP addresses must be whitelisted to allow the ENS traffic into Exchange or Office 365. Based on the security policies applied to the outgoing traffic from Exchange, it might be necessary to whitelist the outbound IP addresses. The IP address is selected based on the region the ENS is hosted in. The following table describes the Exchange server IP whitelisting requirements.

Table 3-1. Exchange Server IP Whitelisting Requirements

Location	API Endpoint	ENS Outbound to Exchange Inbound	Exchange Outbound to ENS Inbound
North America	https://ens.getboxer.com/api/ens	52.204.159.41 107.23.52.83	35.170.156.92 52.0.239.8 52.203.205.147
Asia Pacific	https://ens-apj.getboxer.com/api/ens	52.69.186.14 52.196.212.232	54.248.56.175 54.249.212.171 54.95.25.171
European Union (EU)	https://ens-eu.getboxer.com/api/ens	3.120.17.75 18.196.83.52	18.195.84.245 18.196.197.192 52.28.149.150

For information on architecture design and functionality of ENS2, see Architecture Overview .

Note The outbound IP addresses must be whitelisted from Microsoft Exchange client access rules (including Office 365) and any other firewall. This allows outbound communication from Exchange server into ENS server. You need not whitelist SEG IP addresses as all outbound connections from Exchange server is going to ENS server and not to SEG EWS proxy.

Verify VMware Boxer Settings

Use Workspace ONE Boxer to verify your email connnectvity.

After you have added the ENS configuration keys to VMware Boxer in Workspace ONE UEM, check the Boxer settings on your device to confirm it has received these keys and that the ENS is activated.

Procedure

1 Open Boxer, tap the **Settings** icon and then select the appropriate email account.

2 In the email settings, verify the **Use Push Service** is enabled.

3 In the email settings, verify the **Notifications** display **Push** as the default selection.

If the **Use Push Service** is enabled and Notifications display **Push**, then the ENS is activated.

Air Watch Resource Library for architecture

These are conref targets for architecture, there is a section for each element type

ol Elements

1 Navigate to the `/opt/vmware/tunnel/_tunnel_installation/` directory.

```
cd /opt/vmware/tunnel/_tunnel_installation/
```

2 Execute **Uninstall_Tunnel**.

```
sudo ./Uninstall_Tunnel
```

3 Review installer logs at `/opt/vmware/tunnel/_tunnel_installation/Logs`, if necessary.

p Elements

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

*This port can be changed if needed based on your environment's restrictions.

For SaaS customers who need to whitelist outbound communication, refer to the following Knowledge Base article that lists up-to-date IP ranges that Workspace ONE currently owns: https://support.workspaceone.com/articles/115001662168-.

Ensure the Directory Sync Service and the Scheduler Service are running on the same server, since they write to and read from the same queues.

The Content Gateway, together with VMware Workspace ONE Content, lets your end users securely access content from an internal repository. This means that your users can remotely access their documentation, financial documents, board books, and more directly from content repositories or internal file shares. As files are added or updated within your existing content repository, the changes will

immediately be reflected in VMware Workspace ONE Content, and users will only be granted access to their approved files and folders based on the existing access control lists defined in your internal repository. Using the Content Gateway with VMware Workspace ONE Content allows you to provide unmatched levels of access to your corporate content without sacrificing security.

Configuration Key	Value Type	Configuration Value	Description
ENSLinkAddress	String	Supported format: https://ens.getboxer.com/api/ens Replace `ens.getboxer.com` with the resolved name or IP provided by VMware based on your region. Sample link address: ■ For AMER - https://ens.getboxer.com/api/ens ■ For APAC - https://ens-apj.getboxer.com/api/ens ■ For EMEA - https://ens-eu.getboxer.com/api/ens	Provide the address for the ENS2 system for your users to connect.
ENSAPIToken	String	Sample API Token: +eXaml3_AP1=	API Token provided by VMware AirWatch to activate the ENS service.
AccountNotifyPush	Boolean	False - disable (default) True - enable	Enables ENS for the account.
EWSUrl	String	Supported Format: https://[external_email_server_domain]/EWS/Exchange.asmx Sample EWS URL: ■ https://e.mail.com/EWS/Exchange.asmx ■ https://seg.dom.com/EWS/Exchange.asmx	Enables manual configuration of Exchange Web Services (EWS) endpoint when autodiscovery is disabled in your Exchange environment.

The Email Notification Service (ENS) adds Apple Push Notification support to Exchange. On iOS, this means the VMware Boxer email app can get notifications utilizing either Apple’s background app refresh or Apple Push Notification Service (APNs) technologies. Background app refresh is used by default, however iOS attempts to balance the needs of all apps and the system itself. This means that each app may provide notifications at irregular periods using this method. To provide notifications quickly and consistently, Apple also provides APNs. This allows a remote server to send notifications to the user for that application, however Exchange does not natively support this. ENS adds APNs support to your deployment to allow quick and consistent notifications about new items in your end users' email inboxes.

table Elements

Requirement	Notes
SSH access to Linux Servers and an admin account with full write permissions.	Root permissions, or sudo access with the same privileges as root required. Once installation completes, you can put restrictions into place for these account types.
yum Enabled	Enable to allow the installer to request and install any missing prerequisites.
CentOS 7.x SUSE 12.x RHEL 7.x	UI-less recommended. Basic infrastructure type recommended.

StatusChecklist	Requirement	Notes
	Windows Server 2008 R2 or Windows Server 2012 or Windows Server 2012 R2	
	Install PowerShell on the server	PowerShell version 3.0+ is required if you are deploying the PowerShell MEM-direct model for email. To check your version, open PowerShell and run the command $PSVersionTable.
	Install .NET Framework 4.6.2	The VMware Enterprise Systems Connector auto-update feature will not function correctly until your VMware Enterprise Systems Connector server is updated to .NET Framework 4.6.2. The VMware Enterprise Systems Connector auto-update feature will not update the .NET Framework automatically. Please install .NET 4.6.2 manually on the VMware Enterprise Systems Connector server before performing an upgrade.

StatusChecklist	Requirement	Notes
	Ensure that you have remote access to the servers that Workspace ONE UEM is installed on	Workspace ONE UEM recommends setting up Remote Desktop Connection Manager for multiple server management, you can download the installer from https://www.microsoft.com/en-us/download/details.aspx?id=44989 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 as well.
	Installation of Notepad++ (Recommended)	Workspace ONE UEM recommends setting up Notepad++.
	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.

Hard Disk Storage
10 GB

Email Notification Service (ENS) for On-Premises 4

Configuring ENS for your On-Premises deployment in a 3-step process.

You must first configure CNS and download the ENS configuration files, then install ENS2, and finally configure Boxer for On-Premises.

You must also ensure that the ENS server certificate is available on the user's Exchange server. See Chapter 2 Enabling and Securing Communication Between the Exchange Server and the Email Notification Server.

This chapter includes the following topics:

Configure CNS and Download Email Notification Service Configuration Files

Before you install ENS in an On-premises deployment, you must configure the Cloud Notification Service (CNS) and download the configuration `.xml` file using the Workspace ONE UEM console.

Prerequisites

- Download the CNS public certificate from https://resources.workspaceone.com/view/2hjxzvgkxyf8n738hy7x/en.
- If you have installed ENS2 v1.3, you must upgrade your CNS from CNS v1.0 to CNS v2.0 for supporting notifications.

Note To proceed with ENS2, your console version must be 9.3 or higher. If you see a **Download Installer** displayed when your are configuring and downloading the configuration files, then your console version is less than 9.3. This is the installer for the earlier version of ENS. See the *VMware Email Notification Service* installation guide for instructions and detailed information.

Procedure

1. Select the required Organization Group and navigate to **Groups & Settings** > **All Settings**.
2. From the System column, select **Advanced**, and then select **Site URLs**.

3 (On-premises only) From the Site URLs values page, select **Cloud Notification Service URL** and add `https://cns.awmdm.com/nws/notify/apns`.

4 (On-premises only) - If the Workspace ONE UEM console is deployed On-premises, then you must upload the CNS certificate.

   a From the left navigation pane, select **System > Security > SSL Pinning**.

   b Select **ADD HOST**. In the **Add Pinned Host** window, enter the host as `cns.awmdm.com`.

   c Select **Upload** to upload the CNS certificate you downloaded earlier.

5 If the UEM console is On-premises, navigate to **System > Advanced > Secure Channel Certificate** and select **Download CNS Secure Channel Certificate Installer**. You can also open a Zendesk ticket with **SaasOps** > **CNS Upload Request** category.

   Send a request the VMware Support Team to install the certificate on the CNS server.

6 From the Settings page, select **Email** and then select **Email Notification**.

7 To enable Email Notification, select **Yes** and then click **Save**.

   After the settings are saved, the Download Configuration option is displayed.

8 Select **Download Configuration**.

9 Enter a password in **Certificate Password**. to download the configuration.

   The password is required to download the configuration and must be provided again during ENS installation.

10 Select **Confirm Password**, reenter the password to confirm and click **Download**.

11 Save the archived `.xml` file to be accessible for upload during ENS installation.

Install Email Notification Service 2

To use the Email Notification Service 2 (ENS2), you must install the ENS on an IIS server.

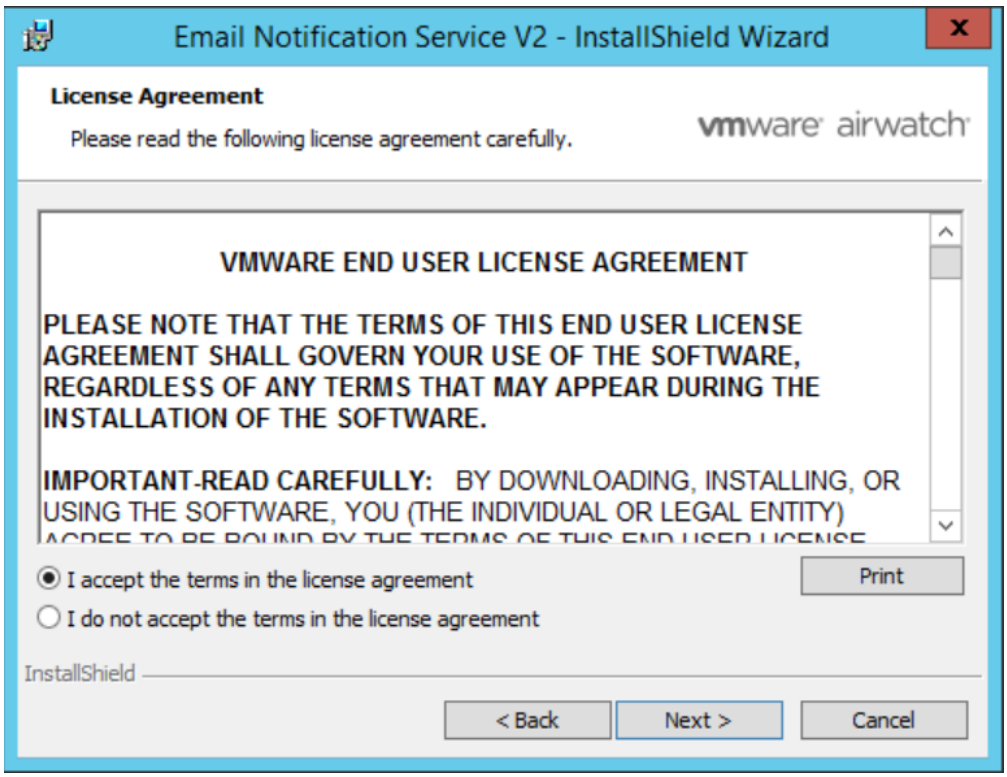
Prerequisites

Complete the following tasks before you install ENS2:

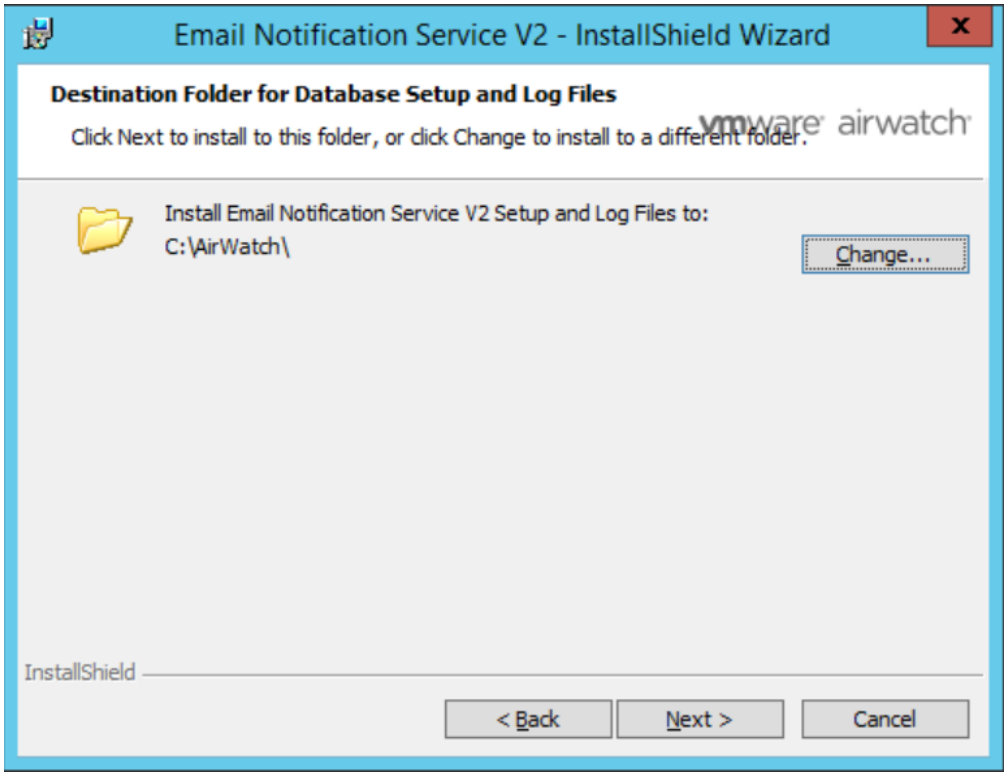
- Install IIS 7 or later on the Web Server
- Update ASP.Net to v 4.6.2
- Download the `config.xml` file from the Workspace ONE UEM console. See Configure CNS and Download Email Notification Service Configuration Files.
- Ensure that an SSL certificate with a valid hostname is set up on the IIS server. This server should be externally accessible via https (SSL cert) and with a Fully Qualified Domain Name (FQDN).
- Create a new database and name it appropriately. If you are using SQL Server AlwaysOn, you can create availability group and listeners.
- The database account user must have privileges to access and modify the database.

Procedure

1. Download the latest version of ENS2 installer from the Software section of the My Workspace ONE portal.
2. Run the installer. The InstallShield Wizard opens and displays the License Agreement.
3. Select the **I accept the terms in the license agreement** check box and then click **Next**.

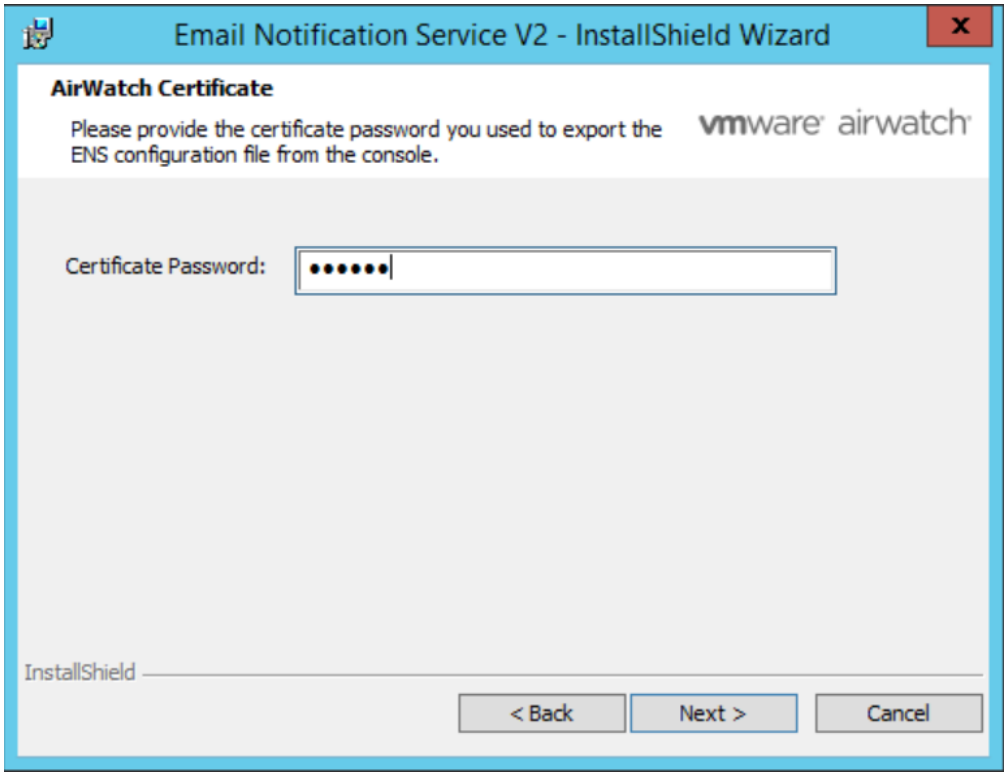


4 Click **Next** to install the components at the default location. If you want to install the components at a custom location, click **Change** and browse and select your location.



5 Click **Browse** and locate the **config.xml** file and then click **Next**.

6 Click **Certificate Password** text box and enter the certificate password you provided when you downloaded the configuration file from the Workspace ONE UEM console, and then click **Next**.



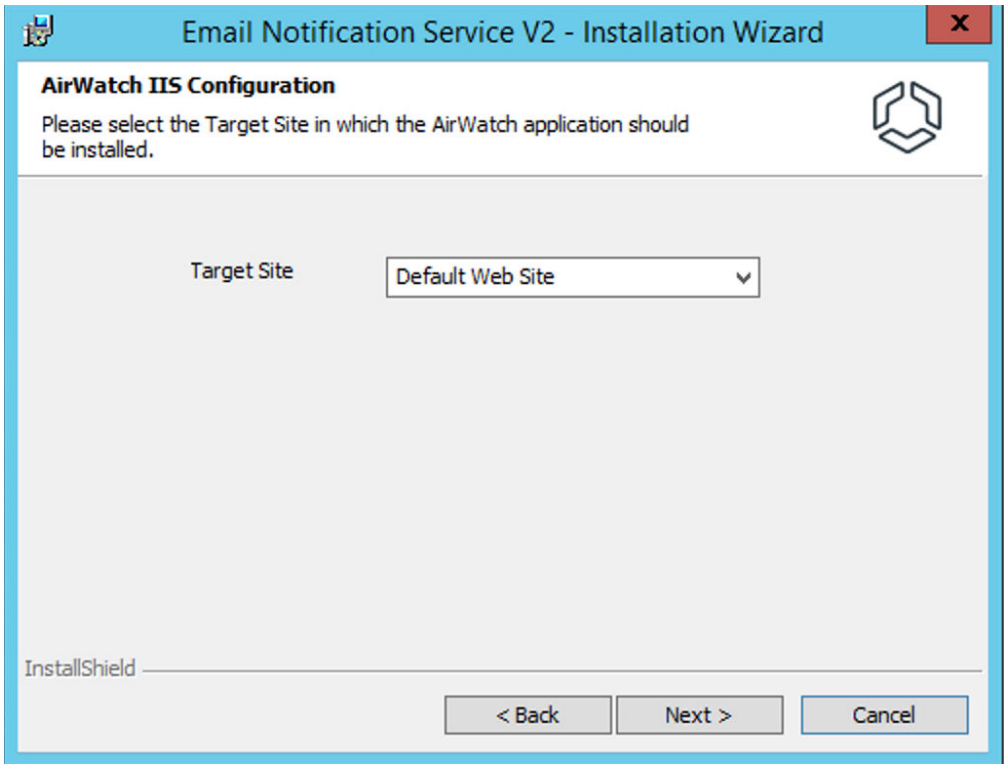
7 (Optional) On the **AirWatch CNS Email Proxy Configuration** window, provide the following information:

a Check **Enable CNS Proxy** to configure the CNS proxy. Enter the hostname/IP address and the proxy port of the the server.

b Select the authentication type:

- Anonymous - user name and password is not required
- Basic/Windows - Enter user name and password.

8 Select the target site on the Airwatch IIS configuration window.



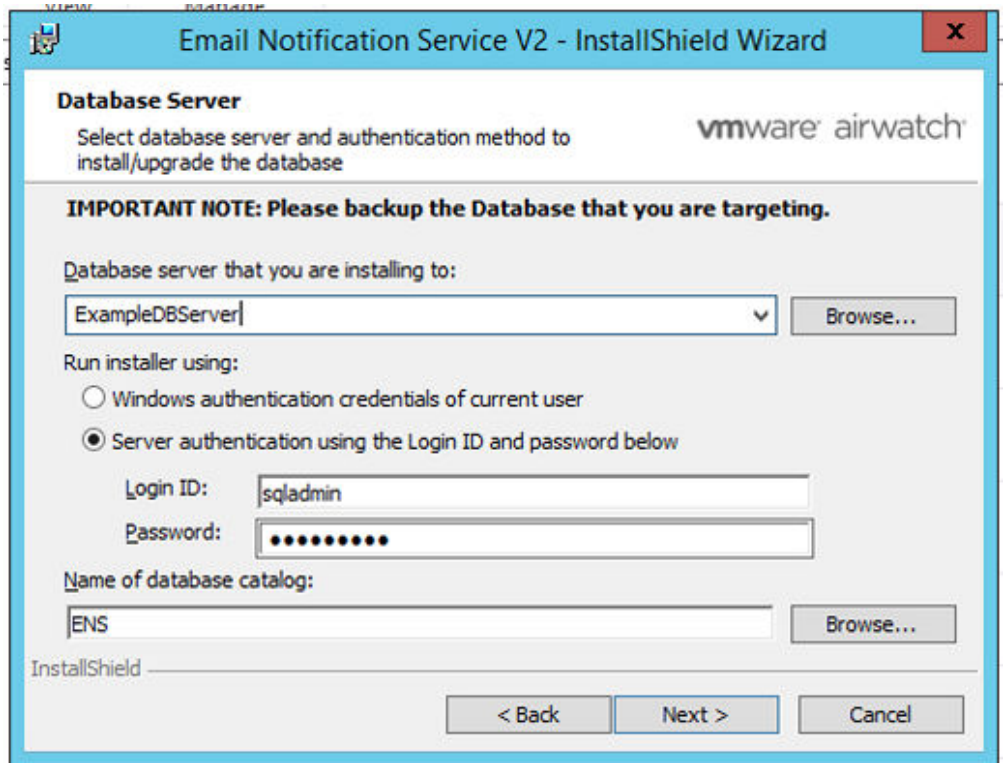
9 On the Database Server window, enter the following information:

a Browse to select the database server where the database is located. Enter the IP address or host name of the server if the server is not listed.

b Select Windows authentication or server authentication based on your authentication configuration. If you choose server authentication, enter the login ID and password.

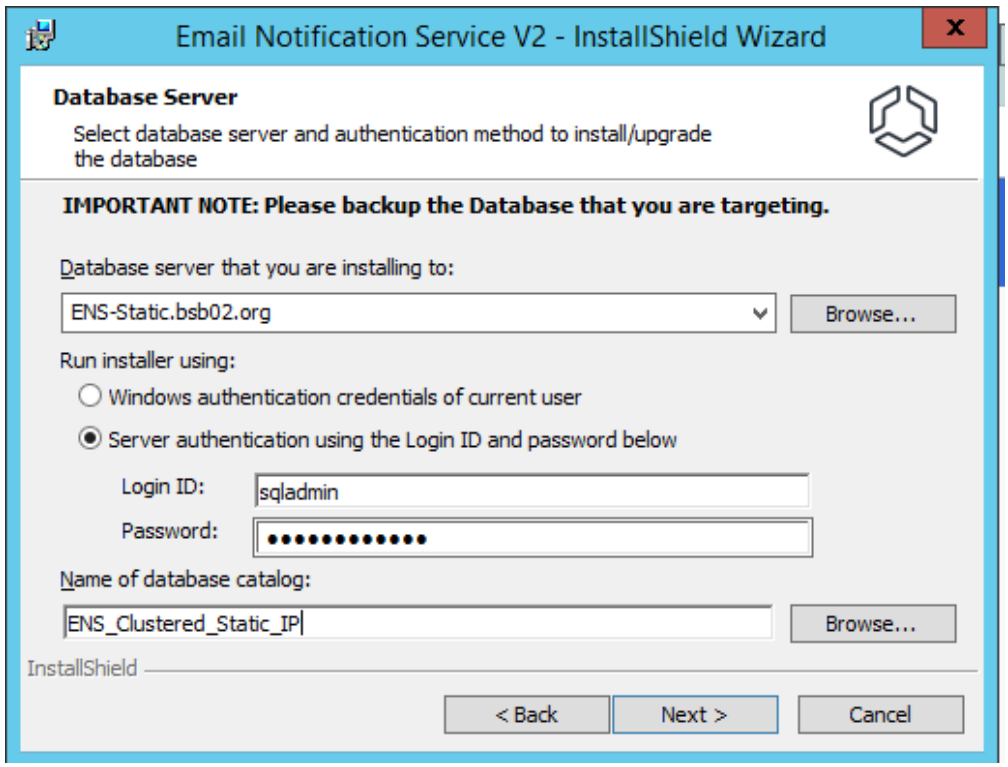
c Enter the name of the database in the **Name of the database catalog** text box and click **Next**.

- If the database has already been created, browse and select the existing database.
- If there is no existing database, enter a name for the new database, and the installer will create and publish the database.
- You can configure using a single database configuration or with SQL AlwaysOn. The below figure shows the the single database configuration.

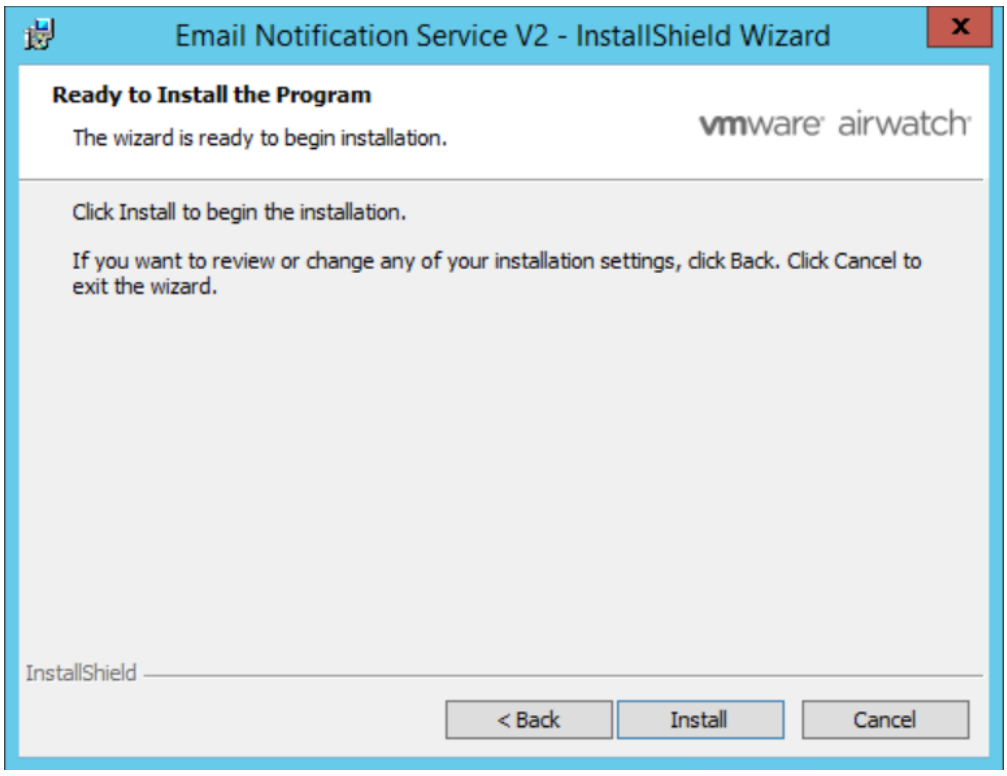


The below diagram shows the configuration using SQL Server AlwaysOn.

Note If you are using SQL Server AlwaysOn, you can configure the availability group Listener URL here.



10 Click **OK** to confirm and then click **Install** to start the installation.



11 Click **Finish** to complete the installation.

After the installation is complete, an API token is displayed in a text file.

12 Copy the API token.

Note This API token is required when configuring the Boxer application UEM console. Use this value for the *ENSAPIToken* field.

Upgrade ENS2

You can upgrade from an older version of ENS2 to the latest version.

You must have the latest version of the installer on your system. Download the latest version of ENS2 installer from the Software section of the My Workspace ONE portal.

The instructions to upgrade to the latest version of ENS2 are the same as the ENS2 installation instructions. See Install Email Notification Service 2.

Configure Workspace ONE Boxer for On-Premises

After you have installed the ENS2, you must configure the ENS2 related settings for Workspace ONE Boxer on the Workspace ONE UEM console.

Prerequisites

The API token and ENS2 server URL are required to activate the ENS service using Workspace ONE UEM console.

Procedure

1 Select the required organization group.

2 Select **APPS & BOOKS** and then select the **Public** tab.

3 Select **VMware Boxer**.

4 Select **Edit** on the upper right corner of the page and then select the **Assignment** tab.

5 In the **Application Configuration (Optional)** section, add the following keys.

Configuration Key	Value Type	Configuration Value	Description
ENSLinkAddress	String	Supported format: `https://acme.com/MailNotificationService/api/ens`. Replace *acme.com* with the resolved name or IP of your ENS Server.	Provide the address for the ENS2 system for your users to connect. See ENS Endpoints and IP Whitelist .
ENSAPIToken	String	Sample API Token: +eXaml3_AP1=	This token is generated at the end of your ENS installation and is provided by VMware AirWatch to activate the ENS service. SaaS customers can request this token by sending a request to the SaaS support team.

Configuration Key	Value Type	Configuration Value	Description
AccountNotifyPush	Boolean	■ False - disable (default) ■ True - enable	Enables ENS for the account
EWSUrl	String	Supported Format: `https://[external_email_server_domain]/EWS/Exchange.asmx` Sample EWS URL: ■ `https://e.mail.com/EWS/Exchange.asmx` ■ `https://seg.dom.com/EWS/Exchange.asmx`	Enables manual configuration of Exchange Web Services (EWS) endpoint when autodiscovery is disabled in your Exchange environment.

6 Select **Save & Publish** and then select **Publish** on the next page. To verify the settings, see Verify VMware Boxer Settings.

ENS2 and SEG V2 Interaction 5

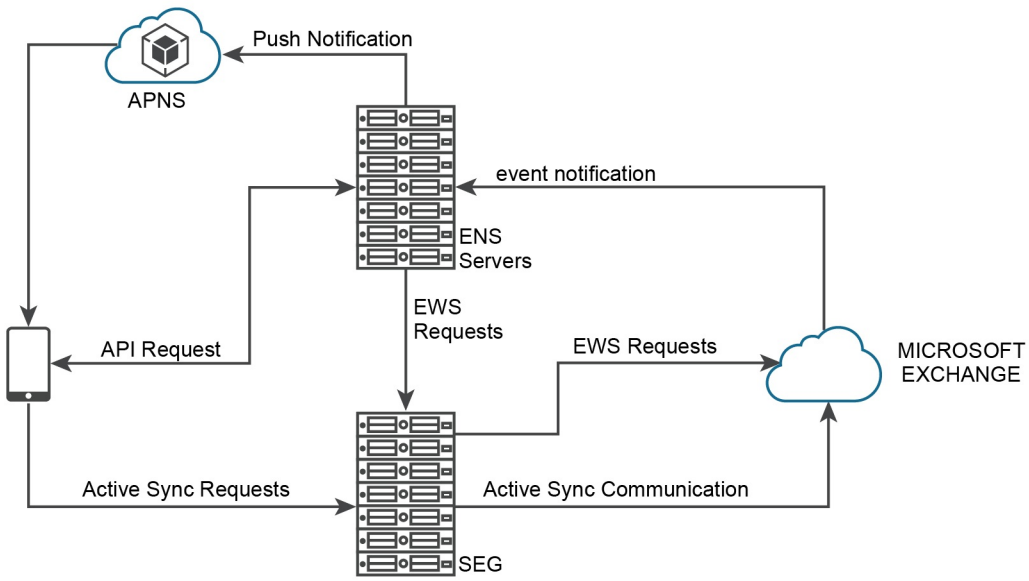
Monitor compliance of the client with the ENS2 environment so that ENS2 together with SEG V2 can block or unblock a client depending on the compliance criteria of the client.

Background

Currently, when a mobile device is enterprise wiped or removed from the Workspace ONE UEM console, the client unregisters from the ENS2 environment. For example, when an enterprise wipe command is sent to iOS Boxer the device tries to unregister until it is successful. However, this is not an ideal scenario as there is a dependency on the device to unregister from the ENS2 environment.

Integration with SEG V2

The SEG V2 protects the email configuration of the client and enables MEM functionality by monitoring the compliance of the device against the configuration in the Workspace ONE UEM console. With the integration of ENS2 and SEG V2, you can block request to a device and control the client, based on the compliance criteria specified in the Workspace ONE UEM console. The following is a high-level diagram showing the interaction between ENS2 and Exchange with SEG V2 as the proxy.



In addition to the compliance scenario, you can use SEG V2 as a proxy when the Exchange Web Service (EWS) endpoint is not publicly available. The EWS proxy allows devices to subscribe to the EWS subscriptions through the SEG V2 server instead of publicly exposing the EWS endpoint.

SEG V2 supports both cloud and on-premises ENS deployments. SEG V2 listens to the EWS traffic from ENS using the EWS endpoints. SEG applies the MEM compliance policies on the incoming requests and proxies the requests to Exchange. See, Configure ENS2 with SEG.

Supported Exchange Web Service Authentication Methods for SEG Proxy

The Exchange Active Sync (EAS) authentication method used with Boxer must match the EWS authentication method as ENS implicitly uses the authentication method used by Boxer. SEG as EWS proxy supports basic authentication, certificate-based authentication (CBA) with KCD, and modern authentcation (OAuth) types and does not support the New Technology LAN Manager (NTLM) authentication type.

Certificate-based authentication using KCD is supported. If your deployment utilizes CBA using KCD, SEG accquires the Kerberos token (from KCD) required for the Exchange authentication. The authentication method for EAS and Exchange Web Service (EWS) protocol must match for SEG to work correctly.

For more information, see the *Configure SEG V2 Compliance for Email Notification Service* topic in the *Secure Email Gateway (SEG) V2* guide.

Supported Servers for Exchange Web Service and ActiveSync

If you have different fully qualified domain name (FQDN) for Exchange Web Service (EWS) and ActiveSync endpoints, it is recommended you upgrade to SEG version 2.12 or later. In this SEG version, you can provide a different hostname and uncomment the ews.email.server.host.and.port=https://example.com:443 property for EWS flows.

Note If you provide a different hostname, SEG still uses the `server timeout`, `ignoreSslErrorsWithExch`, and other settings from the EAS email server configuration provided in the MEM configuration for the email server client. If the EWS server is using self-signed certificate then you need to add the self-signed certificate in the Java trustStore before the SEG installation or you need to rerun the SEG installer.

For SEG versions before 2.12, the only option available is to have two different MEM configuration and two different SEG servers to proxy traffic. One SEG can serve one email server address or FQDN. However, if EWS and ActiveSync endpoints are hosted on the same email server address or FQDN, same SEG server can proxy both EWS and ActiveSync traffic.

This chapter includes the following topics:

Configure ENS2 with SEG

The following procedure describes the steps to configure ENS2 with SEG.

Procedure

1. Navigate to **SEG > Configuration**.
2. Select the `application.properties` file and edit the file.
3. Select the `enable.boxer.ens.ews.proxy` value and update the value to `enable.boxer.ens.ews.proxy=true`.
4. Restart the SEG service. SEG receives the /EWS and /ews endpoints for traffic from the ENS.

Configure SEG for Authentication

If you are using basic authentication only, and the EWS endpoint is configured to allow NTLM authentication, ensure the SEG version is 2.9.0.1 and validate the `remove.unsupported.auth` configuration in SEG using the following procedure:

Procedure

1. Navigate to **SEG > Configuration** folder using file explorer.
2. Select the `application.properties` file and edit the file.
3. Check if the `remove.unsupported.auth.for.ews` value is true if NTLM authentication is enabled on Exchange, as SEG does not support NTLM connection persistence. If you do not see an entry for `remove.unsupported.auth.for.ews` then the SEG version is not 2.9.0.1. Ensure the SEG version is 2.9.0.1.
4. Verify the SEG version and save the file.

In the SEG `application.properties`, flag the `remove.unsupported.auth.for.ews=true` value to remove the unsupported www-authentication header from the EWS response to the ENS through SEG. The NTLM and the Negotiate headers are removed from the EWS response. The NTLM header as a persistent connection is not supported by SEG. The Negotiate www-authenticate header is removed in the absence of a valid client certificate, that is, when the userPrincipalname (UPN) is null. In the absence of Kerberos authentication, the Negotiate header can be considered as NTLM authentication.

Note If you enable both basic and Kerberos authentication and the client fails to present a valid client certificate, then the SEG removes the Negotiate header and requests you to authenticate using basic authentictaion. In such scenarios, the client is enforced to use basic authentication only. If the client does not have the basic authentication configured then the client fails to receive a successful response. When the client presents a valid certificate, the SEG generates a Kerberos token and proceeds with the Negotiate authentication.

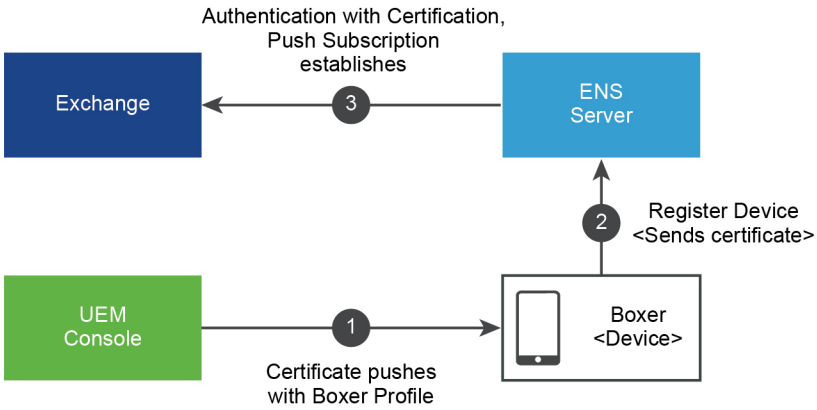
Enable Certificate-Based Authentication for ENS

6

ENS supports certificate-based authentication (CBA) and dual authentication. The dual authentication is a combination of basic authentication and certificate-based authentication. For ENS, you must configure the Boxer application with certificate-based authentication for Exchange server and enable certificate-based authentication for the EWS endpoint. ENS uses the same certificate that the Boxer application receives for the authentication purpose. ENS must ensure that the EWS endpoint can validate the certificates used by the Boxer application.

Prerequisites

Configure Boxer application with CBA and enable CBA for the EWS endpoint. For more information about configuring CBA for Workspace ONE Boxer, see the *Workspace ONE Boxer Admin Guide* documentation.



Procedure

1. Push the certificate with Boxer profile from the Workspace ONE UEM console to the Workspace ONE Boxer.
2. Register your device with the ENS server and send the certificate from Workspace ONE Boxer.
3. Send certificate from ENS to the Exchange server and establish the push subscription.

Configure ENS2 for Certificate-Based Authentication

When you configure ENS2 for Workspace ONE Boxer and want to use Certificate-Based Authentication (CBA) for authentication, you must follow the steps listed in this section for ENS2 to work with CBA.

1 Configure Workspace ONE Boxer to use CBA. See Configure Certificate-Based Authentication on the Exchange Server.

2 Change the appropriate settings to ensure that CBA is supported for the EWS endpoint and for EAS on the on-premise Exchange Server. See Using Office 365 with ENS2 and Certificate-Based Authentication and Configure Certificate-Based Authentication on the Exchange Server.

3 If you are using Secure Email Gateway V2 (SEG V2), see the *Secure Email Gateway V2 guide* for information on the changes that are required on the SEG server.

Configure Certificate-Based Authentication on the Exchange Server

You can enable certificate-based authentication (CBA) for Exchange Active Sync (EAS) on the Exchange Server (for TLS testing) by modifying specific values on the IIS server. Office 365 or Exchange online does not directly support certificate-based authentication. You must set up dual authentication, that is, modern authentication and CBA, to setup certificate-based authentication for Office 365. You must have Active Directory Federation Service (ADFS) setup to do certificate-based authentication. Office 365 authenticates through the modern authentication, and certificate is presented to the ADFS for authentication. On the Boxer profile, modern authentication and certificate-based authentication needs to be enabled that is, AccountUseOauth must be enabled. See the *Workspace ONE Boxer Admin Guide* documentation for more details.

Procedure

1 From the IIS console, navigate to **Sites > Default Sites > Microsoft-Server-ActiveSync** virtual directory.

2 Select and modify the following settings:

Setting	Description
Authentication	■ **Disable** Basic Authentication. ■ **Enable** Windows Authetication.
SSL Settings	Ensure that the **Require SSL** option is selected. Under Client Certificates, select **Require**.
Configuration Editor	Change the value of *system.webServer/security/authentication/clientCertificateMappingAuthentication)* from **False** to **True**.

Using Office 365 with ENS2 and Certificate-Based Authentication

If you are using Office 365 and want to perform certificate-based authentication (CBA), you must enable certain settings in the Workspace ONE Boxer profile.

Office 365 or Exchange online does not directly support certificate-based authentication. You must set up dual authentication, that is, modern authentication and CBA, to set up certificate-based authentication for Office 365. You must have Active Directory Federation Service (ADFS) set up to perform certificate-based authentication. Office 365 authenticates through the modern authentication and certificate is presented to ADFS for authentication.

You must also enable modern authentication and certificate-based authentication using the *AccountUseOauth* setting in the Workspace ONE Boxer profile. See the *Workspace ONE Boxer Admin Guide* documentation for more details.

Supported EWS Authentication Methods with Office 365

The following EWS authentication methods are supported with Office 365:

- OAuth 2.0 (Exchange Online only)
- NTLM (Exchange On-premises only)
- Basic (no longer recommended)

Refer to the relevant Microsoft Office 365 documentation for more details.

Frequently Asked Questions

7

This section lists and describes some of the frequently asked questions about ENS2 functionality.

How are credentials or authentication tokens handled?

Although the client shares the credentials or tokens with the ENS2 environment upon registration, they are not saved on Workspace ONE UEM servers. The Exchange server sends the encrypted authentication information back to Workspace ONE UEM as part of a notification whenever a new email is available. From that notification (Exchange to ENS2), the credentials are decrypted and used to make any requests necessary to the Exchange server. The credentials are discarded after performing the necessary requests.

If credentials are not saved, what data is saved by ENS? How secure is ENS?

- Workspace ONE stores a list of devices and a list of public private key pairs used to decrypt the credentials when the notifications are sent from Exchange. The database is saved on a Virtual Private Cloud (private sub-net) secured using firewall. There is no direct access from the internet to this sub-net. All access is controlled using VPC and Firewall rules and only web servers with a single account have access to the database.
- Workspace ONE saves the log files to help debug issues and monitor the system. The log does not contain any private information (PI) of the customers and access is secured using account permissions.

Where is ENS hosted? Are there instances configured to serve each region based on data sovereignty laws?

ENS is hosted in multiple regions. We have various environments spanning the US, Europe, and Asia regions that permit us to abide by data sovereignty rules.

What data is transmitted through the ENS server without being saved? How is it secured?

- User credentials that are encrypted with RSA encryption.
- Email subject and sender (sent using HTTPS).
- Future functionality: The functionality to control what data (if any) is sent or fetched for the notification. You can also control the data from an email that is used in the notification payload.
- All communication is made through HTTPS.

What is the dependency of ENS on cloud services?

- AWS Simple Notification Service (SNS) is used for managing push notification in AWS Cloud deployment.

- Cloud Notification Service (CNS) is mandatory for passing notifications to Apple/Android devices for On-Premises deployments.
- AWS Relational Database Service (RDS) is used for data persistence.

What is the user agent utilized by ENS2 when sending requests to Exchange?

MailNotificationService/v2 (ExchangeServicesClient/15.00.0913.015). The value '15.00.0913.015' will change as new libraries from Microsoft are released and are updated for using ENS2.

What email folders does ENS2 monitor for incoming messages and actions?

ENS2 only monitors each user’s Inbox folder.