

Email Notification Service 2 (ENS2)

VMware Workspace ONE UEM 1903



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

Copyright © 2019 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1 Introduction 4**
 - [Architecture Overview 5](#)
 - [Requirements 6](#)

- 2 Enabling and Securing Communication Between the Exchange Server and the Email Notification Server 9**

- 3 Email Notification Service for Cloud 10**
 - [Email Notification Service Endpoints 11](#)
 - [Verify VMware Boxer Settings 11](#)

- 4 Email Notification Service (ENS) for On-Premises 13**
 - [Upload Root CA Certificate 13](#)
 - [Configure CNS and Download Email Notification Service Configuration Files 13](#)
 - [Install Email Notification Service 2 14](#)
 - [Configure Workspace ONE Boxer for On-Premises 21](#)

- 5 ENS2 and SEG V2 Interaction 23**

- 6 Frequently Asked Questions 25**

Introduction

The 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
- No push notifications received for up to one hour when the device is actively used (Boxer in the background)
- 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.

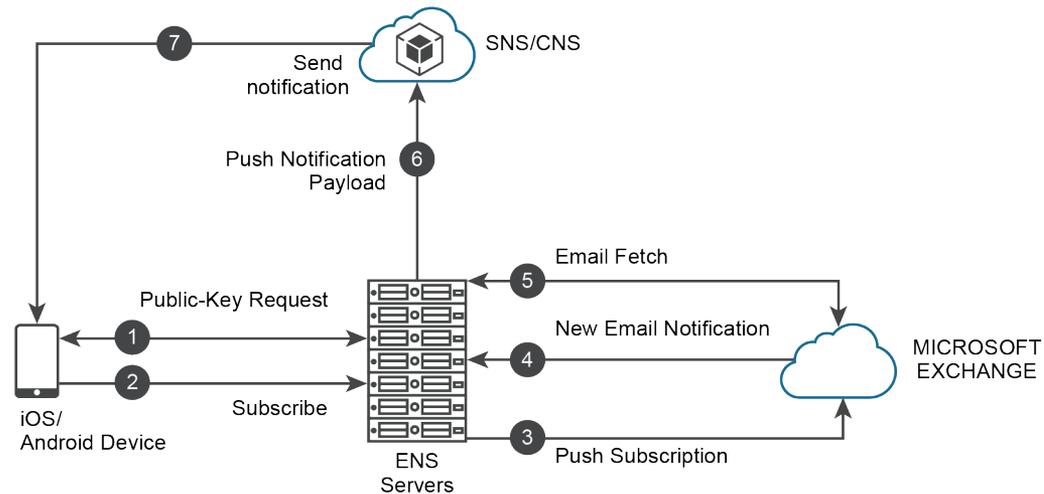
This chapter includes the following topics:

- [Architecture Overview](#)
- [Requirements](#)

Architecture Overview

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

ENS2 Architecture using SNS/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/CNS will send the notifications to iOS/Android devices.

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

Note Secure Email Gateway (SEG) cannot be used to proxy the traffic from ENS to Exchange with only NTLM authentication configured for Exchange EWS endpoint. However, it can function if basic authentication or Kerberos authentication is enabled. See the *Configure SEG V2 Compliance for Email Notification Service* section in the *Secure Email Gateway (SEG) V2* guide.

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 enabled on the SQL server user that is used for running the application

Requirement (On-Premises)	Notes
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
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	

Table 1-5. World Wide Web Services (Continued)

Component Name	Required Services
ISAPI Filters	
Server-Side Includes	
WebSocket Protocol	
Common HTTP Features	Default Document
Directory Browsing	
HTTP Errors	
Static Content	
Health and Diagnostics	HTTP Logging
Performance Features	Static Content Compression
Security	Request Filtering

SQL Server 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.

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.

Note the following considerations before the user's Exchange server can communicate with the ENS server:

- The root CA certificate must already be present on the Exchange server. Follow the steps below to upload the certificate on the Exchange server, if it is not already present:
 - a Download the SSL certificate from the ENS server. Access the ENS Alive endpoint in a browser and download the certificate from the address bar.
 - b Import this certificate on the Exchange Server into the **Trusted Root Certification Authorities** through MMC.

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.

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: <ul style="list-style-type: none">■ 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. For more information, see Email Notification Service Endpoints .
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: <ul style="list-style-type: none"> ■ 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.

This chapter includes the following topics:

- [Email Notification Service Endpoints](#)
- [Verify VMware Boxer Settings](#)

Email Notification Service Endpoints

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

Table 3-1. Supported Endpoints

Location	API Endpoint	Service Outbound IP Addresses
North America	https://ens.getboxer.com/api/ens	35.170.156.92 52.0.239.8 52.203.205.147
Asia Pacific	https://ens-apj.getboxer.com/api/ens	54.248.56.175 54.249.212.171 54.95.25.171
European Union (EU)	https://ens-eu.getboxer.com/api/ens	18.195.84.245 18.196.197.192 52.28.149.150

Note The outbound IP addresses should be whitelisted from Exchange client access rules (including O365) and any other firewall. Only those IP Addresses from Exchange server to ENS should be whitelisted and ENS does not require you to whitelist the entire SEG server.

Verify VMware Boxer Settings

Use Workspace ONE Boxer to verify your email connectivity.

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.

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:

- [Upload Root CA Certificate](#)
- [Configure CNS and Download Email Notification Service Configuration Files](#)
- [Install Email Notification Service 2](#)
- [Configure Workspace ONE Boxer for On-Premises](#)

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.
- 2 Import this certificate on the Exchange Server into the **Trusted Root Certification Authorities** through MMC.

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 you 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**.

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.

Install Email Notification Service 2

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

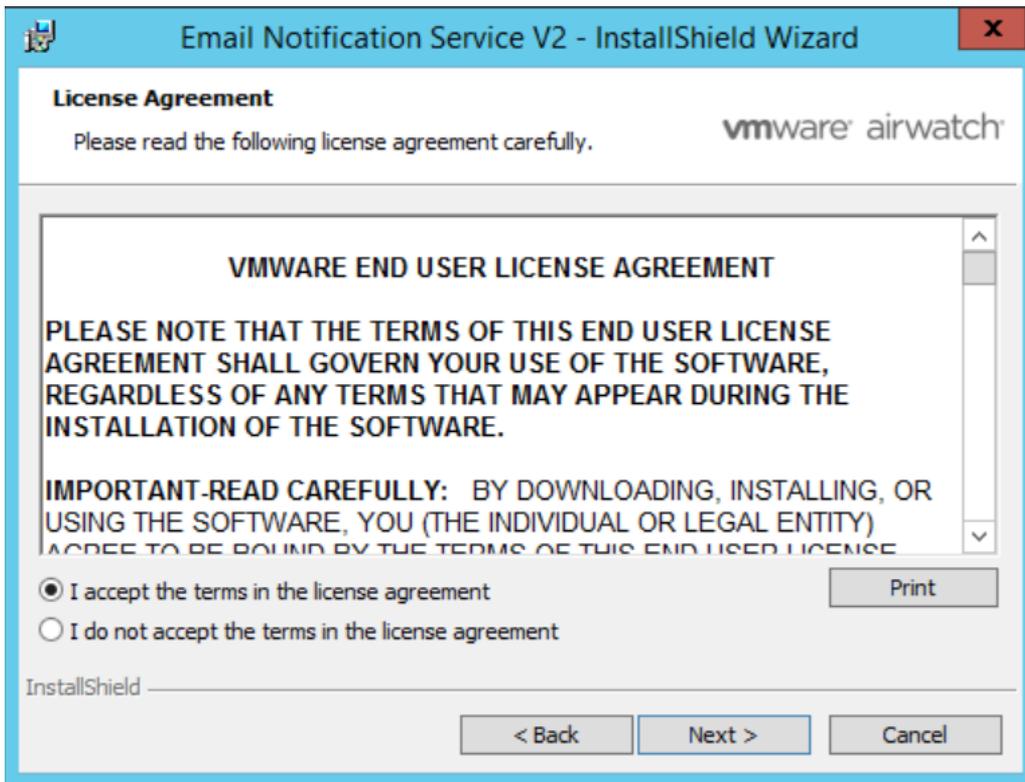
Prerequisites

Complete the following tasks before you install ENS2:

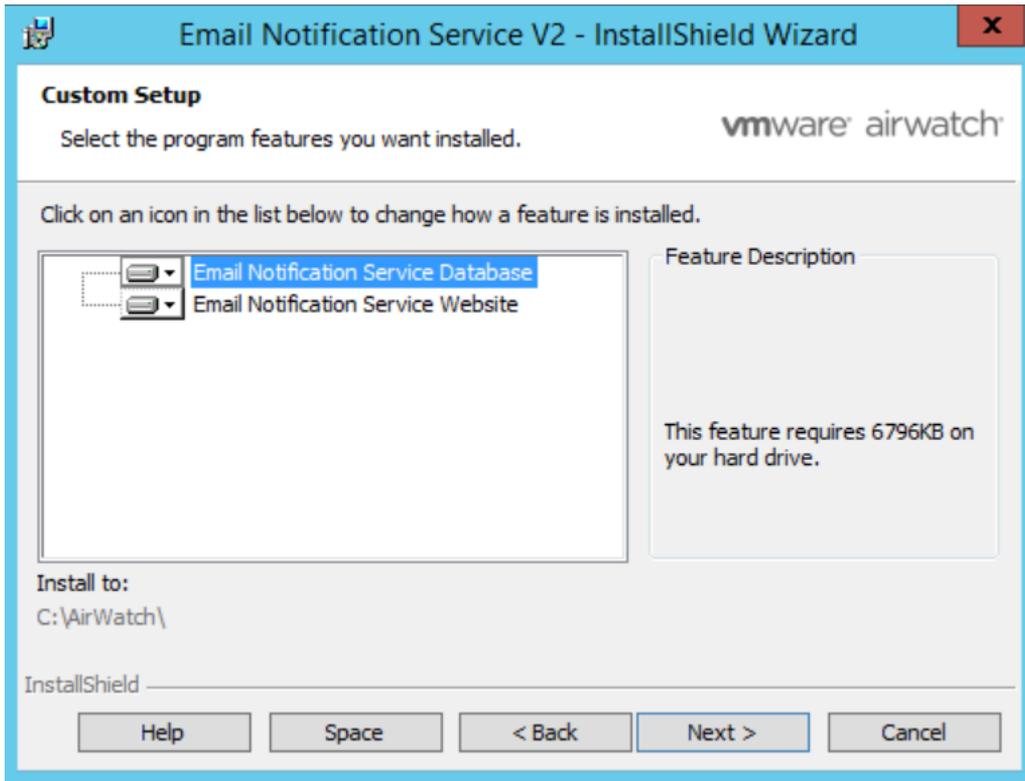
- Install IIS 7 or later on the Web Server
- Update ASP.Net to v 4.6.2
- Download the config.xml file from the Workspace ONE UEM console. See [Configure CNS and Download Email Notification Service Configuration Files](#).
- Ensure that an SSL certificate with a valid hostname is set up on the IIS server. 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

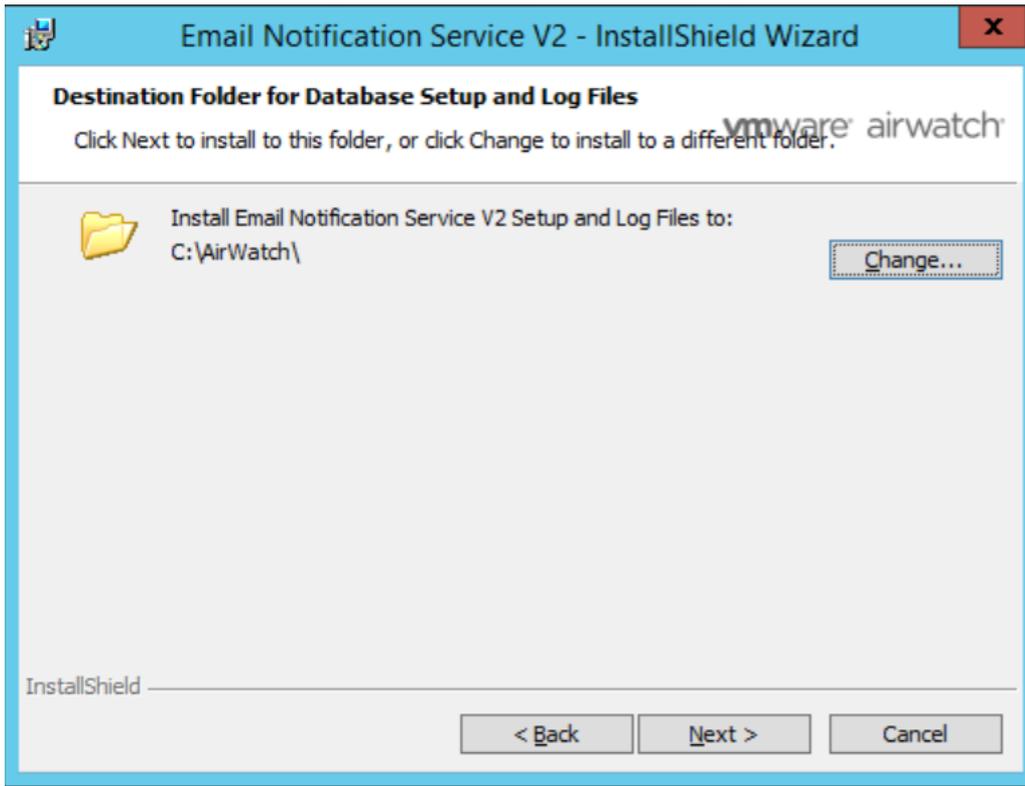
- 1 Download the latest version of ENS2 installer from the Software section of the [My Workspace ONE portal](#).
- 2 Run the installer. The InstallShield Wizard opens and displays the License Agreement.
- 3 Select the **I accept the terms in the license agreement** check box and then click **Next**.



- 4 Select both the Email Notification Service Database and the Email Notification Service Website and click **Next**.

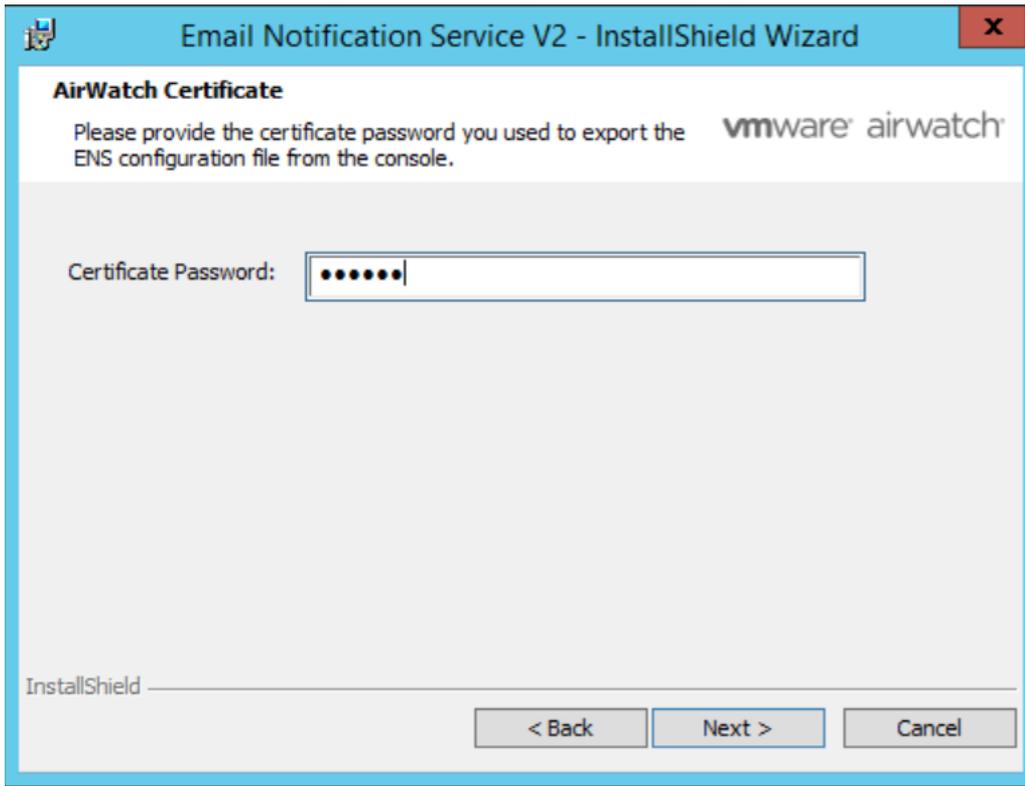


- 5 Click **Next** to install the components at the default location. If you want to install the components at a custom location, click **Change** and browse and select your location.



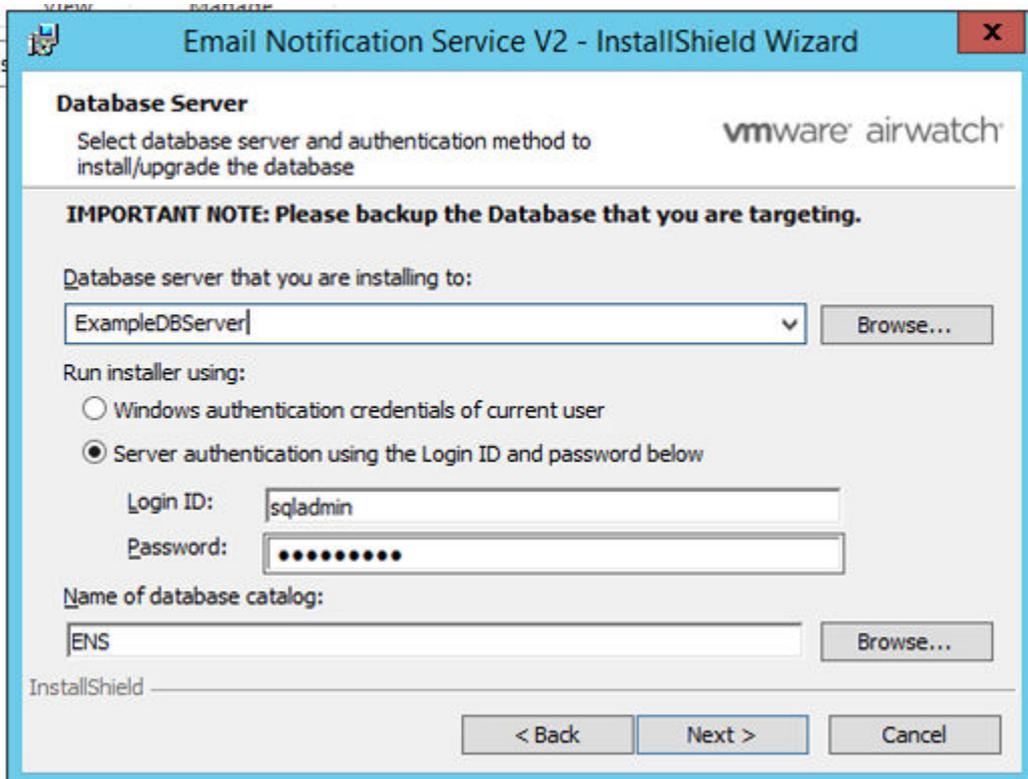
- 6 Click **Browse** and locate the **config.xml** file and then click **Next**.

- 7 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**.



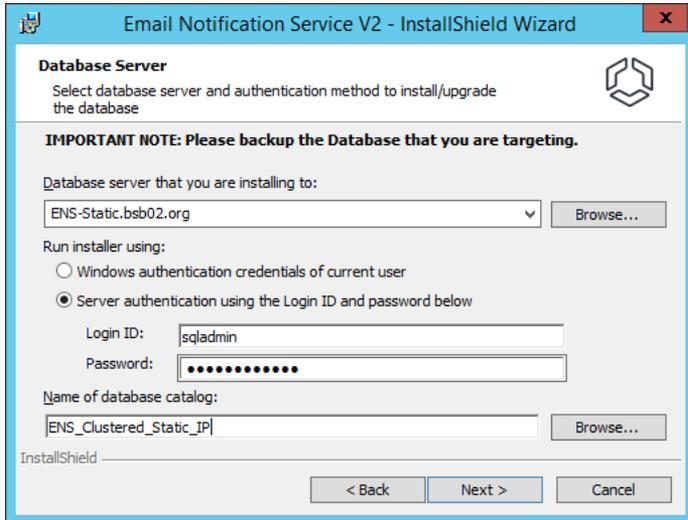
- 8 (Optional) On the **AirWatch CNS Email Proxy Configuration** window, provide the following information:
 - a Check **Enable CNS Proxy** to configure the CNS proxy. Enter the hostname/IP address and the proxy port of the the server.
 - b Select the authentication type:
 - Anonymous - user name and password is not required
 - Basic/Windows - Enter user name and password.

- 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.

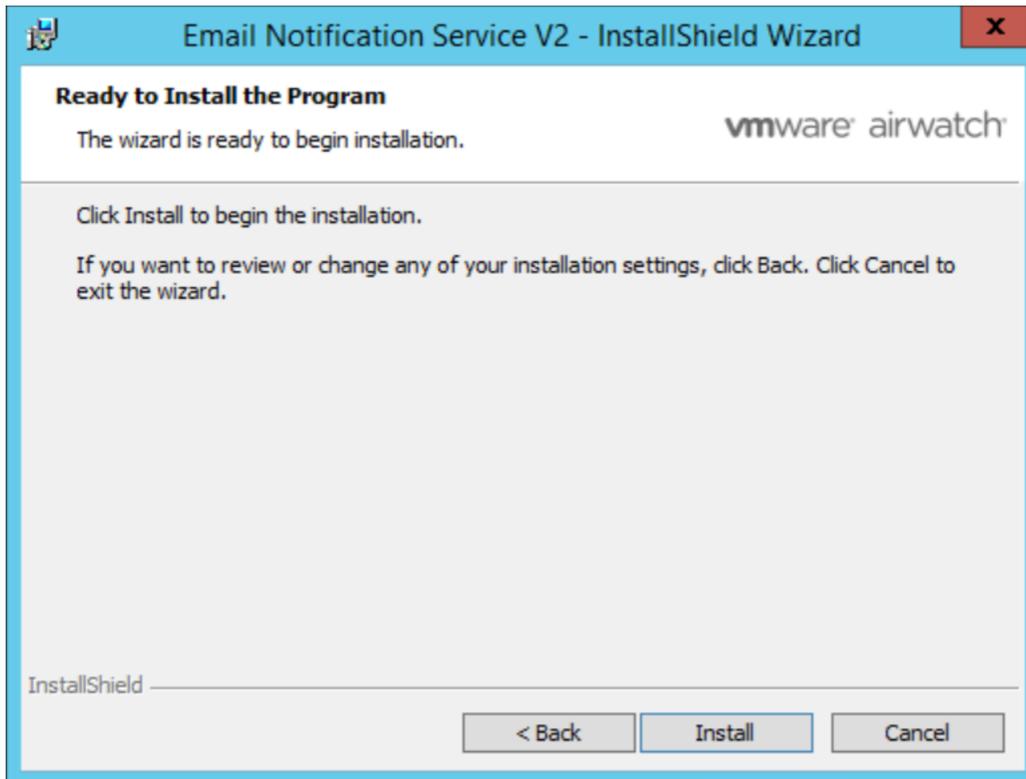


The below diagram shows the configuration using SQL Server AlwaysOn.

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.

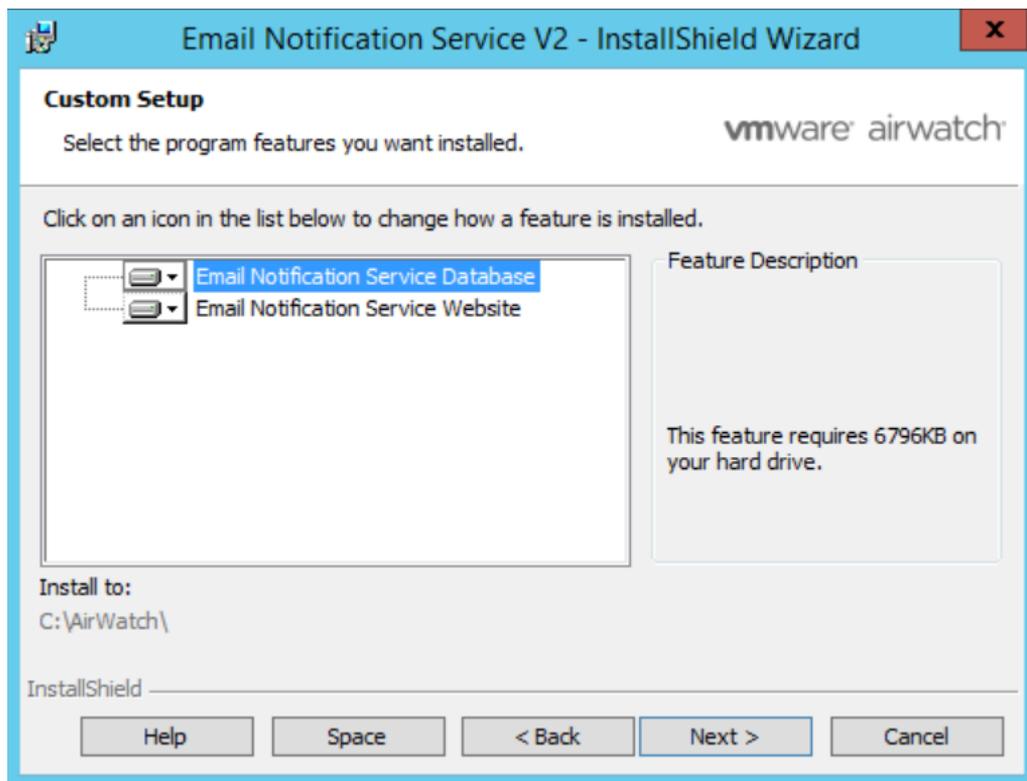
Upgrade ENS2

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](#).

Note During the upgrade, when you run the installer, and are selecting the program features to be installed, ensure that you select both the Email Notification Service Database (even if an older version of the database is already installed and available) along with the Email Notification Service Website. Selecting the database component is especially important when you are upgrading multiple servers which have the ENS2 application installed on them, and is connected to a single database.



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 <i>acme.com</i> with the resolved name or IP of your ENS Server.	Provide the address for the ENS2 system for your users to connect. See Email Notification Service Endpoints .
ENSAPIToken	String	Sample API Token: +eXaml3_AP1=	API Token provided by VMware AirWatch to activate the ENS service.
AccountNotifyPush	Boolean	<ul style="list-style-type: none"> ▪ 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: <ul style="list-style-type: none"> ▪ 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

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

Background

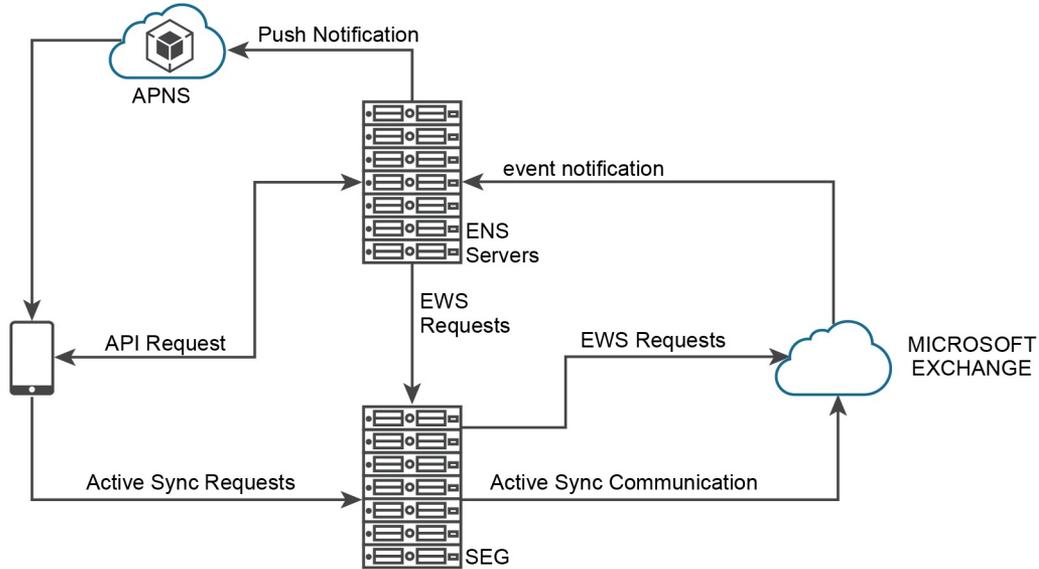
Currently, when a mobile device is wiped clean, the client deregisters from the ENS2 environment. For example, when a wipe command is received to the Boxer iOS, the device keeps trying to unregister until it is successful.

Additionally, when the device stops the required hourly checkins with ENS2, and that Exchange subscriptions need to be periodically redone, even if a device fails to unregister from ENSv2, eventually the device stops receiving notifications.

However this is not an ideal scenario, since there is dependency on the device to deregister from the ENS2 environment.

Integration with SEG V2

The VMware AirWatch Secure Email Gateway V2 (SEG V2) helps protect clients' email configuration and enables Mobile Email Management (MEM) functionality by monitoring the device's compliance against the setup on Workspace ONE UEM console. With the integration of ENS2 and SEG V2, we can enforce immediate blocking of requests for a device based on compliance criteria specified via console and completely take control off the client. Below is a high-level diagram showing the interaction between ENS2 and Exchange with SEG V2 as the proxy.



Frequently Asked Questions

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.