Email Notification Service 2 (ENS 2)

VMware Workspace ONE UEM 1902
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
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 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 at docs.vmware.com.

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) 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

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**

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.**

**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 Workspace ONE UEM SEG (V2) guide on docs.vmware.com.

Workspace ONE UEM Requirements

- Cloud Deployment: Workspace ONE UEM console 8.4 or later
- On Premises Deployment: Workspace ONE UEM console 9.2.3 or later

Hardware Requirements (On-Premises Only)

**Table 1-1. Web Server**

<table>
<thead>
<tr>
<th>CPU Core</th>
<th>RAM</th>
<th>Hard Disk Storage</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 (Intel processor)</td>
<td>16 GB (8GB minimum)</td>
<td>30 GB</td>
<td>Per 100,000 users.</td>
</tr>
</tbody>
</table>

**Table 1-2. Database Server**

<table>
<thead>
<tr>
<th>CPU Core</th>
<th>RAM</th>
<th>Hard Disk Storage</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 (Intel processor)</td>
<td>16 GB (minimum)</td>
<td>Approx. 0.0477 MB per user to estimate the DB storage size</td>
<td>Per 100,000 users.</td>
</tr>
</tbody>
</table>

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                      |
Basic Authentication for the Exchange environment                          | OAuth and Certificate Based Authentication (CBA) is supported for Exchange Web Services                                                |
CNS Certificate                                                             |                                                                                                                                       |
Table 1-3. Network Ports

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol (Port)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENS</td>
<td>Exchange (EWS)</td>
<td>HTTPS (443)</td>
</tr>
<tr>
<td>Exchange (EWS)</td>
<td>ENS</td>
<td>HTTPS (443)</td>
</tr>
<tr>
<td>ENS</td>
<td>AirWatch Cloud Notification Service (CNS)</td>
<td>HTTPS (443)</td>
</tr>
<tr>
<td>ENS</td>
<td>SQL Server Instance</td>
<td>SQL (1433)</td>
</tr>
<tr>
<td>Internet (Devices)</td>
<td>ENS</td>
<td>HTTPS (443)</td>
</tr>
</tbody>
</table>

Table 1-4. IIS Services

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Required Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Management Tools</td>
<td>IIS 6 Management Compatibility</td>
</tr>
<tr>
<td>IIS Management Console</td>
<td></td>
</tr>
<tr>
<td>IIS Management Scripts and Tools</td>
<td></td>
</tr>
<tr>
<td>IIS Management Service</td>
<td></td>
</tr>
</tbody>
</table>

Table 1-5. World Wide Web Services

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Required Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Development Features</td>
<td>.NET Extensibility 3.5</td>
</tr>
<tr>
<td>.NET Extensibility 4.6</td>
<td></td>
</tr>
<tr>
<td>Application Initialization</td>
<td></td>
</tr>
<tr>
<td>ASP</td>
<td></td>
</tr>
<tr>
<td>ASP.NET 3.5</td>
<td></td>
</tr>
<tr>
<td>ASP.NET 4.6</td>
<td></td>
</tr>
<tr>
<td>ISAPI Extensions</td>
<td></td>
</tr>
<tr>
<td>ISAPI Filters</td>
<td></td>
</tr>
<tr>
<td>Server-Side Includes</td>
<td></td>
</tr>
</tbody>
</table>
### Table 1-5. World Wide Web Services (Continued)

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Required Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebSocket Protocol</td>
<td></td>
</tr>
<tr>
<td>Common HTTP Features</td>
<td>Default Document</td>
</tr>
<tr>
<td>Directory Browsing</td>
<td></td>
</tr>
<tr>
<td>HTTP Errors</td>
<td></td>
</tr>
<tr>
<td>Static Content</td>
<td></td>
</tr>
<tr>
<td>Health and Diagnostics</td>
<td>HTTP Logging</td>
</tr>
<tr>
<td>Performance Features</td>
<td>Static Content Compression</td>
</tr>
<tr>
<td>Security</td>
<td>Request Filtering</td>
</tr>
</tbody>
</table>
Enabling and Securing Communication Between the Exchange Server and the Email Notification Server

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 SSL checkers.
Upload Root CA Certificate

Before the user’s Exchange server can communicate with the ENS server, the root CA certificate must already be present on 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.
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.

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

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

API endpoints supported by ENS2.

### Table 4-1. Supported Endpoints

<table>
<thead>
<tr>
<th>Location</th>
<th>API Endpoint</th>
<th>Service Outbound IP Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td><a href="https://ens.getboxer.com/api/ens">https://ens.getboxer.com/api/ens</a></td>
<td>35.170.156.92</td>
</tr>
<tr>
<td></td>
<td></td>
<td>52.0.239.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>52.203.205.147</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td><a href="https://ens-apj.getboxer.com/api/ens">https://ens-apj.getboxer.com/api/ens</a></td>
<td>54.248.56.175</td>
</tr>
<tr>
<td></td>
<td></td>
<td>54.249.212.171</td>
</tr>
<tr>
<td></td>
<td></td>
<td>54.95.25.171</td>
</tr>
<tr>
<td>European Union (EU)</td>
<td><a href="https://ens-eu.getboxer.com/api/ens">https://ens-eu.getboxer.com/api/ens</a></td>
<td>18.195.84.245</td>
</tr>
<tr>
<td></td>
<td></td>
<td>18.196.197.192</td>
</tr>
<tr>
<td></td>
<td></td>
<td>52.28.149.150</td>
</tr>
</tbody>
</table>

## 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

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 ENS 2, 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
- Install Email Notification Service 2
- Configure Workspace ONE Boxer for On-Premises

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 ENS V2, your console version must be 9.2.3 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 9.2.3. 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 (ENS 2), you must install the ENS on an IIS server.

**Prerequisites**

Complete the following tasks before you install ENS 2:

- Install IIS 7 or later on the Web Server
- Update ASP.Net to v4.6.2
- Download the **config.xml** file from the Workspace ONE UEM console.
- 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 ceert) and with a Fully Qualified Domain Name (FQDN).
- Create a new database and name it appropriately.
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 select Next.

4. Select the ENS components you want to install and select Next.

   You can install both components on the same server. If you have separate database server, you can install the components on different servers.

5. Choose a location to install the selected components and select Next. If you want to install the components at a custom location, select Change.

6. From the ENS Configurations wizard window, select Browse and locate the config.xml file and then select Next.

7. Select 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 select Next.

8. From the Database Server window, select the Database server you are installing to text box and provide the database path and account credentials for installing the database components.

   The database account provided must have access and modifying privileges.

9. Select the Name of the database catalog text box and enter the name of the database and select Next.

10. Select OK to confirm and then select Install to start the installation.

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

11. Copy the API token. The API token is required when deploying Boxer application with ENS2.

12. Select Finish to exit the wizard.

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.

<table>
<thead>
<tr>
<th>Configuration Key</th>
<th>Value Type</th>
<th>Configuration Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENSLinkAddress</td>
<td>String</td>
<td>Supported format: <a href="https://acme.com/MailNotificationService/api/ens">https://acme.com/MailNotificationService/api/ens</a>. Replace acme.com with the resolved name or IP of your ENS Server.</td>
<td>Provide the address for the ENS2 system for your users to connect. See Email Notification Service Endpoints.</td>
</tr>
<tr>
<td>ENSAPIToken</td>
<td>String</td>
<td>Sample API Token: +eXaml3_AP1=</td>
<td>API Token provided by VMware AirWatch to activate the ENS service.</td>
</tr>
<tr>
<td>AccountNotifyPush</td>
<td>Boolean</td>
<td>False - disable (default)</td>
<td>Enables ENS for the account</td>
</tr>
<tr>
<td>EWSUrl</td>
<td>String</td>
<td>Supported Format: https://[external_email_server_domain]/EWS/Exchange.asmx</td>
<td>Enables manual configuration of Exchange Web Services (EWS) endpoint when autodiscovery is disabled in your Exchange environment.</td>
</tr>
</tbody>
</table>

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