VMware AirWatch PowerShell Integration Guide

Securing your email infrastructure

Workspace ONE UEM v9.6

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

Table of Contents

Chapter 1:
Overview

PowerShell Integration with VMware Workspace ONE UEM

The PowerShell integrated deployment is a direct model of integration that requires a simple setup with minimal infrastructure. In the PowerShell model, Workspace ONE UEM uses a PowerShell administrator role and issues commands to the Exchange ActiveSync (EAS) infrastructure to permit or deny mobile access based on the policies defined in the Workspace ONE UEM console. PowerShell deployments do not require a separate email proxy server and the configuration process is simple.

PowerShell Requirements

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

- A service account that has Remote Shell access to Exchange Server and the minimum roles to integrate with PowerShell:
  - Organization Client Access Role
  - Mail Recipients Role
  - Recipient Policies Role (only needed when managing Windows Phone 7 and BlackBerry devices)
- PowerShell minimum version of 3.0. Note, this minimum version of PowerShell is for the application servers and not the Exchange servers. To download an updated version of PowerShell, see Microsoft's download center. To know the command used to check the version of PowerShell installed, see Server-Side Session on page 19.

Note: Selecting the roles enables all required resources or permissions needed for Workspace ONE UEM to operate. Create a custom role group with these roles.

For Office 365 implementations, you must have an Exchange Admin role with the three relevant management roles mentioned earlier.

- Access to the server-side session for Workspace ONE UEM to run Exchange commands.

- Port 443 over which the PowerShell commands are issued from the UEM console directly to the Exchange server or through the VMware Enterprise Systems Connector.

Disclaimer: Integration with a third-party product is not guaranteed and dependent upon the proper functioning of those third-party solutions.

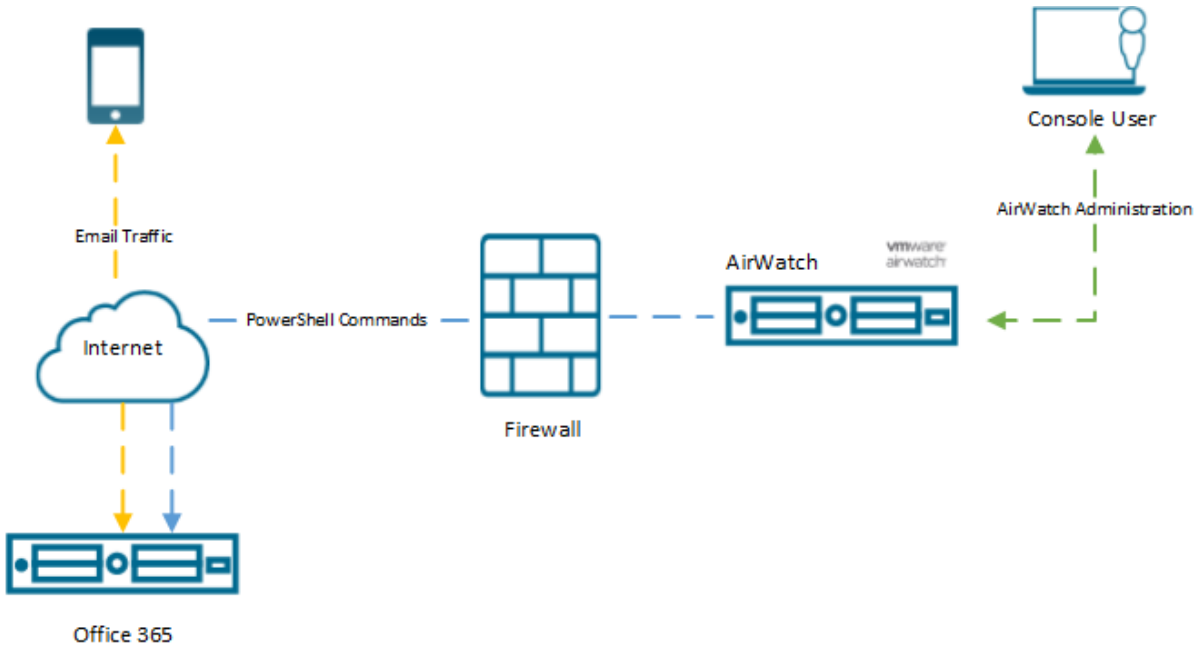
PowerShell Architecture

In the PowerShell model of deployment, Workspace ONE UEM adopts a PowerShell administrator role. Workspace ONE UEM issues commands to the Exchange ActiveSync (EAS) infrastructure to permit or deny email access based on the settings defined in the UEM console.

PowerShell deployments do not require a separate email proxy server, and the installation process is simple. Once installed, Workspace ONE UEM sends commands to PowerShell in accordance with the established email policies, and PowerShell runs the actions. The PowerShell model is for organizations using Microsoft Exchange 2010,2013, 2016, or Office 365 environments.

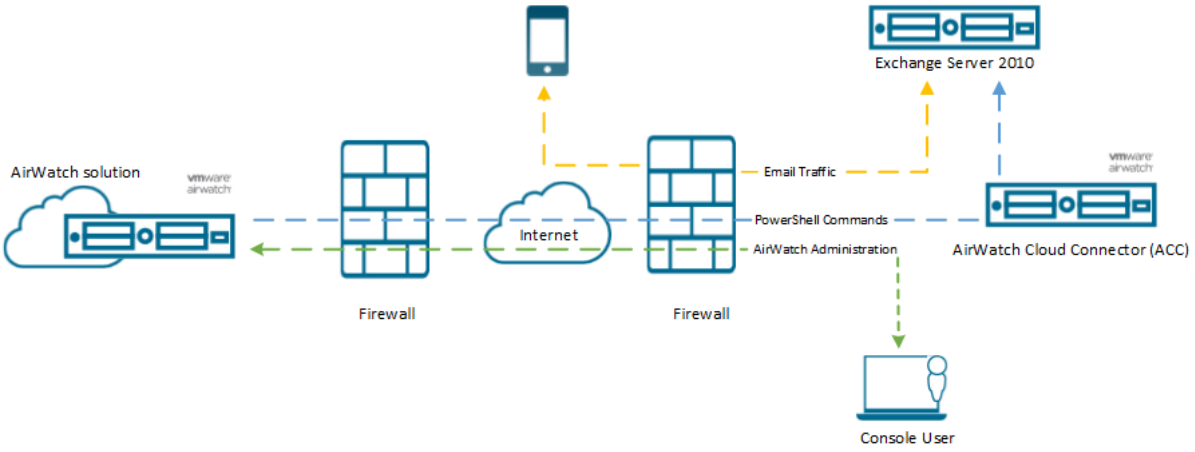
Office 365

The diagram highlights the communications flow for an implementation with Office 365. For Office 365 implementation, Workspace ONE UEM does not recommend routing the PowerShell traffic through the VMware Enterprise Systems Connector.



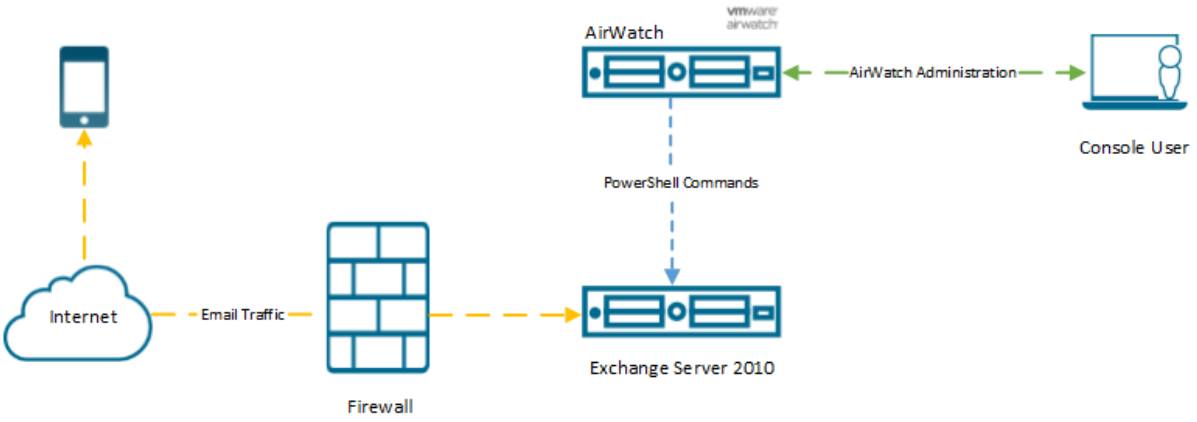
Exchange 2010/2013/2016 for Workspace ONE UEM Cloud-Based Deployments

The following diagram highlights the communications flow for a cloud-based implementation with hosted Exchange 2010/2013/2016 deployments. Workspace ONE UEM recommends installation of one VMware Enterprise Systems Connector per MEG Q server to avoid processing delays.



Exchange 2010/2013/2016 for Workspace ONE UEM On-Premises Deployments

The following diagram highlights the communications flow for an on-premises implementation with hosted Exchange 2010/2013/2016 deployments.



Note: If you want to enable PowerShell with an outbound proxy, then you must configure WinHTTP on the Workspace ONE UEM server to use the proxy. Workspace ONE UEM automatically uses WinHTTP proxy configuration to establish a PowerShell session.

Chapter 2:
PowerShell Implementation Prerequisites

Set up the PowerShell Admin User

For the Workspace ONE UEM server to start issuing the PowerShell commands, you must set up a PowerShell Admin User account on Office 365 or the Exchange Server. This user account is a service account that must also have specific roles associated to it for Workspace ONE UEM to operate.

Create an Office 365 Service Account

You must create the service account to associate with the service account all your user mailbox accounts that require protection.

Note: To create user mailboxes in Exchange 2016, refer https://technet.microsoft.com/en-us/library/jj991919(v=exchg.160).aspx.
To create user mailboxes in Exchange 2013, refer https://technet.microsoft.com/en-IN/library/jj991919(v=exchg.150).aspx.

To create a service account in Office 365:

1. Log in to your Office 365 as an administrator.
2. Navigate to **Office 365 admin center > USERS > Active Users**.
3. To add a new user, select the "**+**" icon. The **create new user account** page appears.
4. On the create new user account page:
    a. Enter the first name, last name, display name, user name, and your email domain.
    b. Select **Type password** and enter the password for the service account.
    c. Deselect the **Make this person change their password the next time they sign in** check box.
    d. Enter the email address of the recipient to whom the password must be sent. Select **Create**.
    e. Select **Close**.

An Office 365 license is assigned to the service account. The service account does not require an Office 365 license to be assigned to it. You can remove the assigned license by editing the license.

5. Select your service account from the Active users list.
6. Select **Edit** next to the Assigned License. The Assigned License page appears.
7. Deselect the check box for the assigned license. Select **Save**.

Assign Roles to the Office 365 Service Account

After you create a service account, use the Exchange Admin Center to create specialized roles for the service account. These roles provide Workspace ONE UEM all the permissions required to operate.

Note: You can also create custom roles for Exchange 2013 and Exchange 2016 service accounts using the Exchange Admin Center.

To assign roles to the service account:

1. Navigate to **Exchange Admin Center > Permissions> admin roles**.
2. To create a new role group, select the "**+**" icon. The new role group page appears.
3. Enter the details.

Settings	Descriptions
Name	Enter the name for the role.
Description	Enter the description for the role.
Write Scope	Select **Default** from the drop-down menu.
Members	Select the Service Account you have created.
Roles	Add **Mail recipients**, **Organization Client Access**, and **Recipient Policies**as the roles.

4. **Save** the settings.

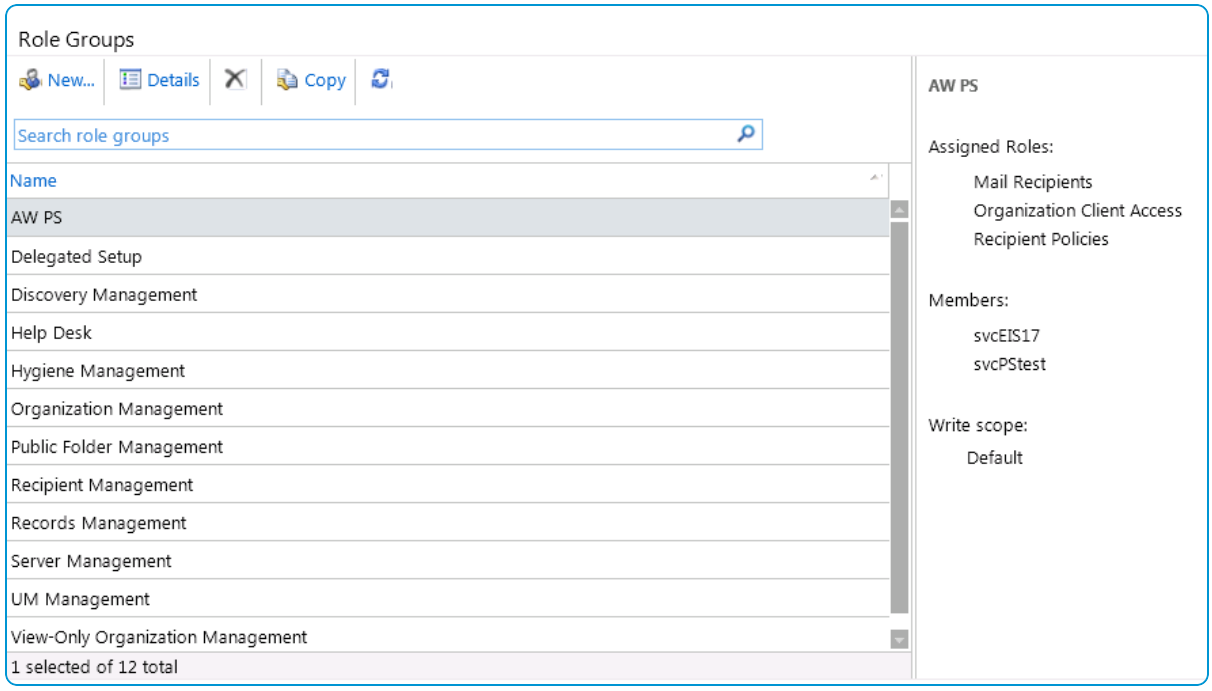
Note: If you are a Workspace ONE UEM SaaS and an Office 365 user, your configuration is complete. The remaining steps are applicable for on-premises Exchange and Workspace ONE UEM configurations.

Assign Roles to the Exchange 2010 Service Account

For Exchange 2010, you can set up a PowerShell Admin User on Exchange Management console through the **Administration** tab. Use permissions that can set up the PowerShell Admin user roles.

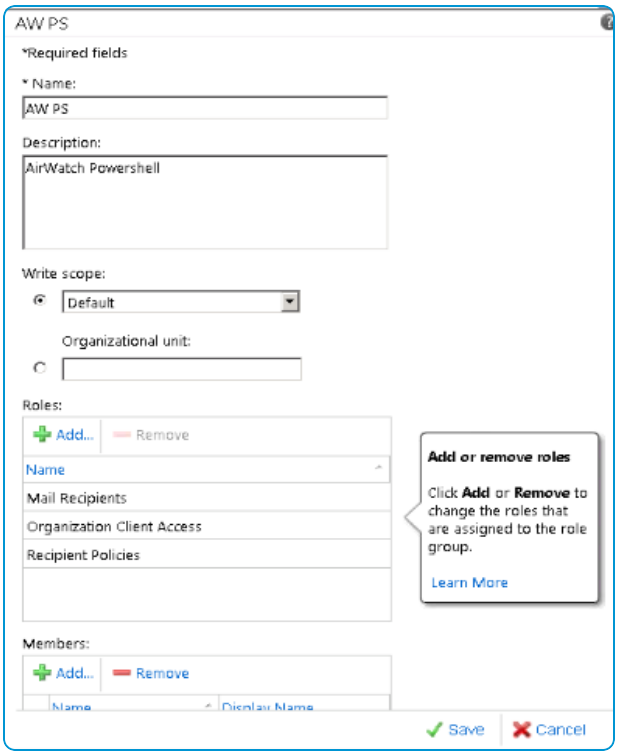
To configure the PowerShell admin user on Exchange console:

1. Navigate to **Toolbox** and access the **Role Based Access Control User Editor** in the Exchange Management console.
2. Once the Internet browser opens, enter in the credentials (domain or user and password) of the Exchange administrator with relevant permissions. Signing in as the Exchange administrator creates a test role group and the roles associated to this group.



3. Select **New** to create a new role group.
4. **Add** the relevant roles; Mail Recipients, Organization Client Access, and Recipient Policies. Add the Service Account you created under the Members section and then select **Save** to create a new role group specific to Workspace ONE

UEM PowerShell Integration.



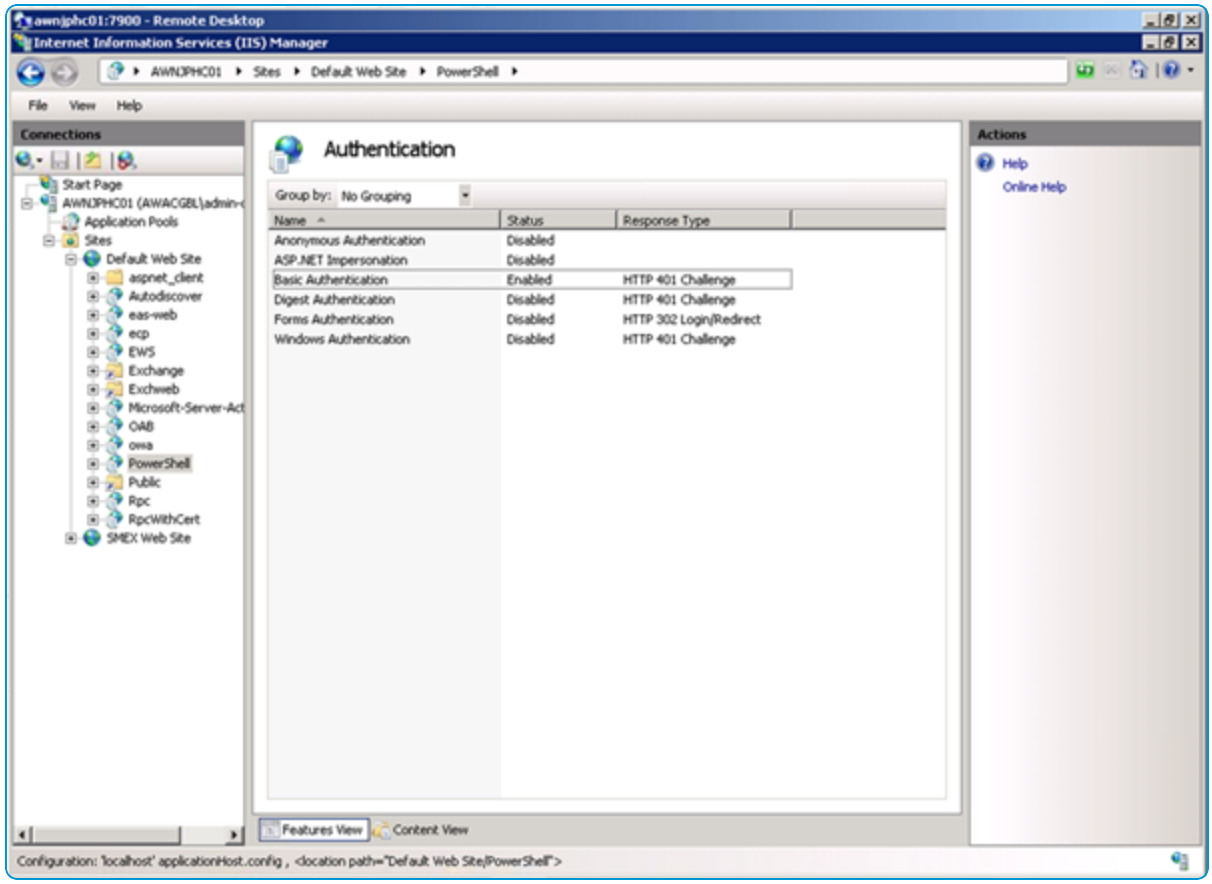
Configure PowerShell Endpoint in IIS

Ensure that the PowerShell endpoint in IIS on the Exchange Server is configured to accept either Basic Authentication or Windows Authentication credentials.

Note: Configuring of authentication details in the IIS manager is only for Exchange 2010, 2013, and 2016. For Office 365 implementations, the Office 365 support team configures the authentication settings.

To configure authentication details:

1. In the IIS manager, expand **Default Web Site** and select **PowerShell**.
2. Select either **Basic Authentication** or **Windows Authentication**.



3. To configure the PowerShell endpoint, enter the following command on the Exchange Management Shell on the Exchange Server and on the Remote Shell on the UEM console Server.

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
```

Configure Windows PowerShell On Workspace ONE UEM Server

To issue remote Shell commands from the UEM Console server, Windows environment must be installed and configured with PowerShell. By default the execution policy on Windows 2008 is set to the **Restricted**script execution mode.

Note: If your deployment consists of an on-premises Workspace ONE UEM server with Office 365, you must configure the Set-ExecutionPolicy on the Workspace ONE UEM server.

To configure PowerShell on the Workspace ONE server:

1. Change the script execution mode from **Restricted** to **RemoteSigned** using the following **Set-ExecutionPolicy** command.

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
```

2. Test the configured PowerShell by connecting to the server-side session. For more information on connecting to the server-side session, see Server-Side Session on page 19.

Note if VMware Enterprise Systems Connector is not in use, then, both the UEM console and the Device Services server requires PowerShell connectivity to the Exchange server.

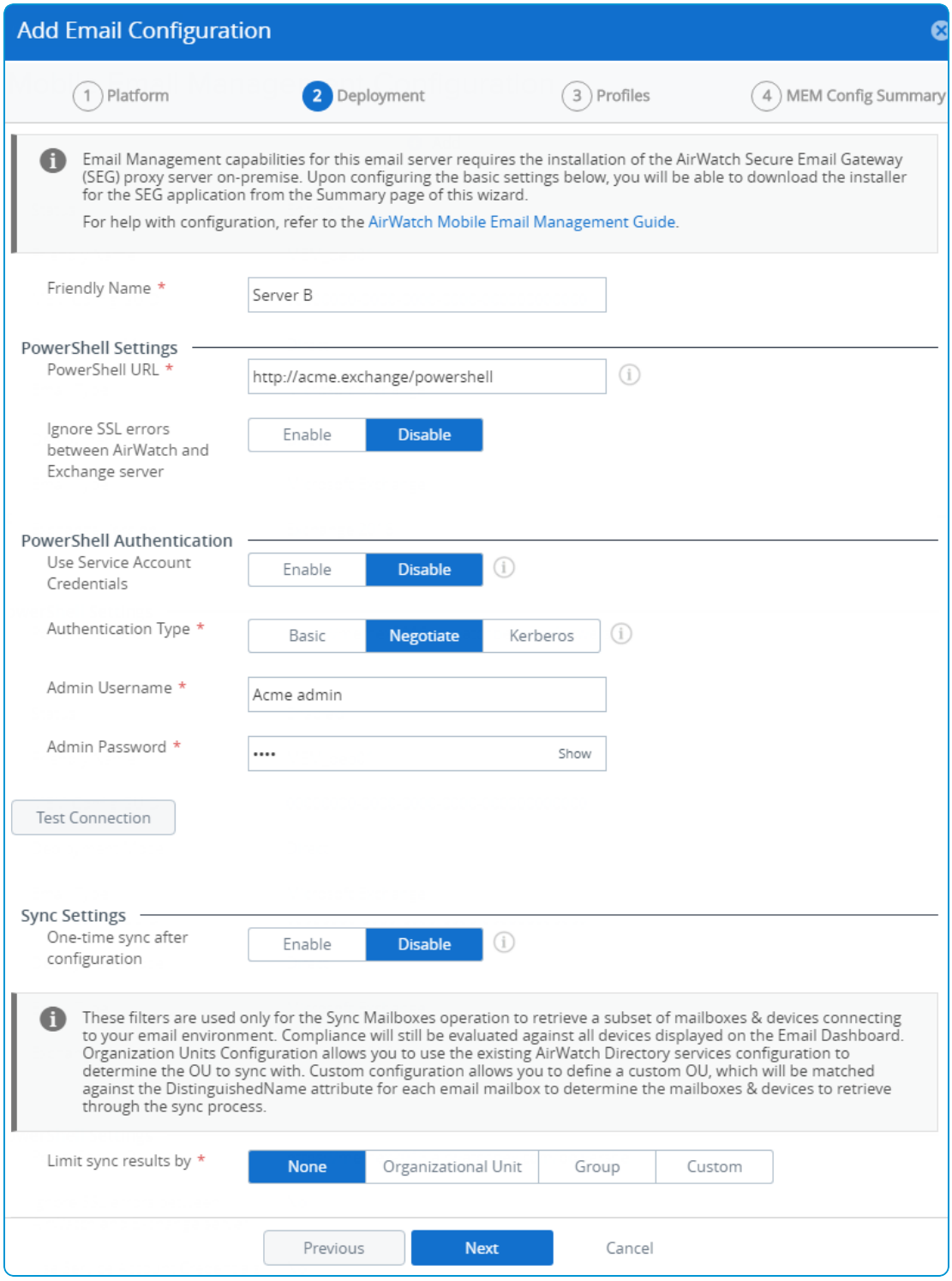
Chapter 3:
PowerShell Implementation

Enable PowerShell Integration in Workspace ONE UEM

To control and manage a remote Exchange instance, enable PowerShell integration through MEM on the UEM console after configuring the PowerShell on the Workspace ONE UEM server.

To enable PowerShell integration:

1. Navigate to **Email** > **Settings**in the UEM console and select **Configure**. The Add Email Configuration wizard form displays.
2. In the Platform wizard form:
   - Select **Direct** as the **Deployment Model**.
   - Select **Exchange** as the Email Type and Exchange 2010/2013/2016 or Office 365 as the Exchange Version. Select **Next**.
3. In the **Deployment** wizard form:

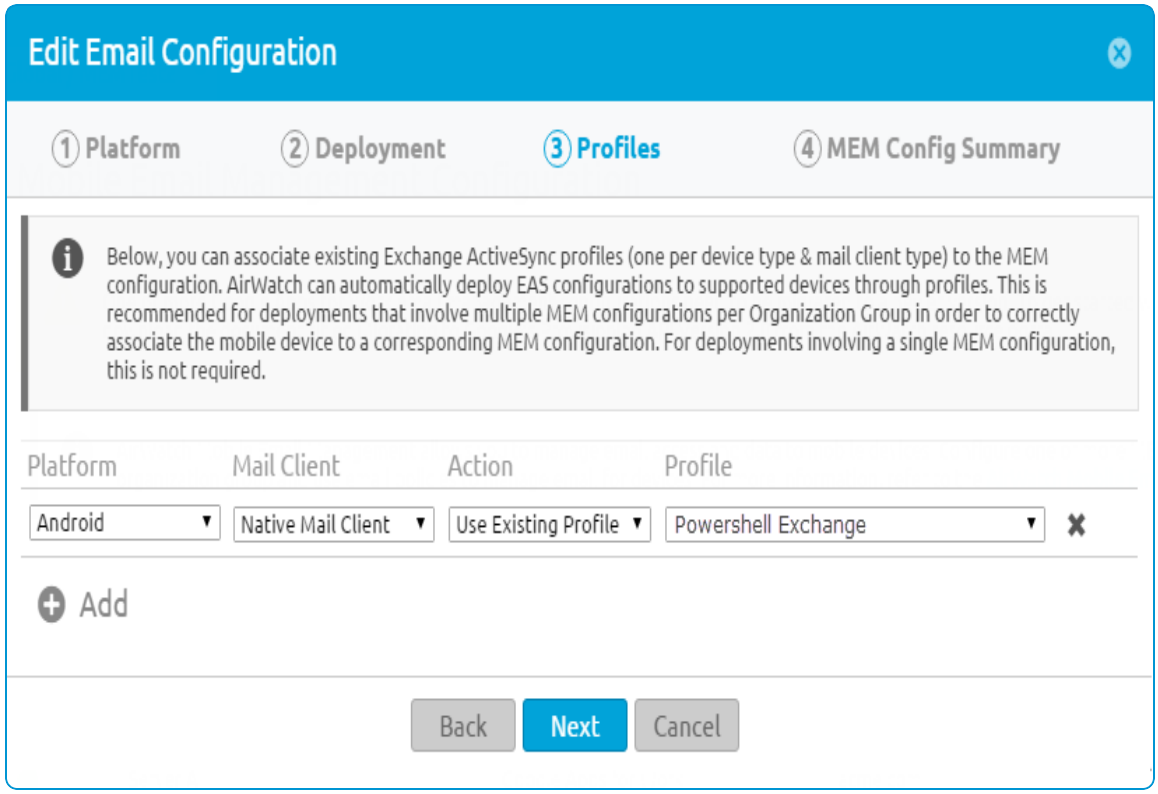


Setting	Description
Friendly name	Enter a friendly name for the PowerShell deployment. This name gets displayed on the MEM dashboard screen for devices managed by PowerShell.
PowerShell Settings	

Setting	Description
PowerShell URL	Enter the PowerShell URL which is the PowerShell instance on the email server in relation to the Workspace ONE UEM Server. Typically, the PowerShell URL is in the form of https://<emailserver>/powershell.
Ignore SSL errors between AirWatch and Exchange server	To Ignore SSL Errors to allow devices to ignore Secure Socket Layer (SSL) certificate errors between Workspace ONE UEM and Exchange server, select **Enable**. **Note:** A valid SSL trust must always be established between Workspace ONE UEM and Exchange server using valid certificates.
PowerShell Authentication	
Use Service Account Credentials	Select **Enable** to use the credentials from the Cloud Connector Application Pool as the Service Account for PowerShell connections.
Authentication Type	Select the authentication type based on the Exchange Server settings. The options available are: • **Basic** – Workspace ONE UEM connects to the remote PowerShell endpoint using the basic authentication type. • **NTLM (Negotiate)** – Workspace ONE UEM connects to the remote PowerShell endpoint using the negotiate authentication type. • **Kerberos** – The email server uses Kerberos to authenticate a domain account and NTLM for a local computer account.
Admin Username	Enter the user name of the PowerShell Service Account if the Use Service Account Credentials option is not enabled. • Domain users must specify the user name in the form of domain\username. • Local users on a server computer must specify the user name in the form of servername\username.
Admin Password	Enter the password of the PowerShell Service Account if the Use Service Account Credentials option is not enabled.
Sync Settings	
One time sync after configuration	Select **Enable** to enable this option to sync with PowerShell soon after configuration.

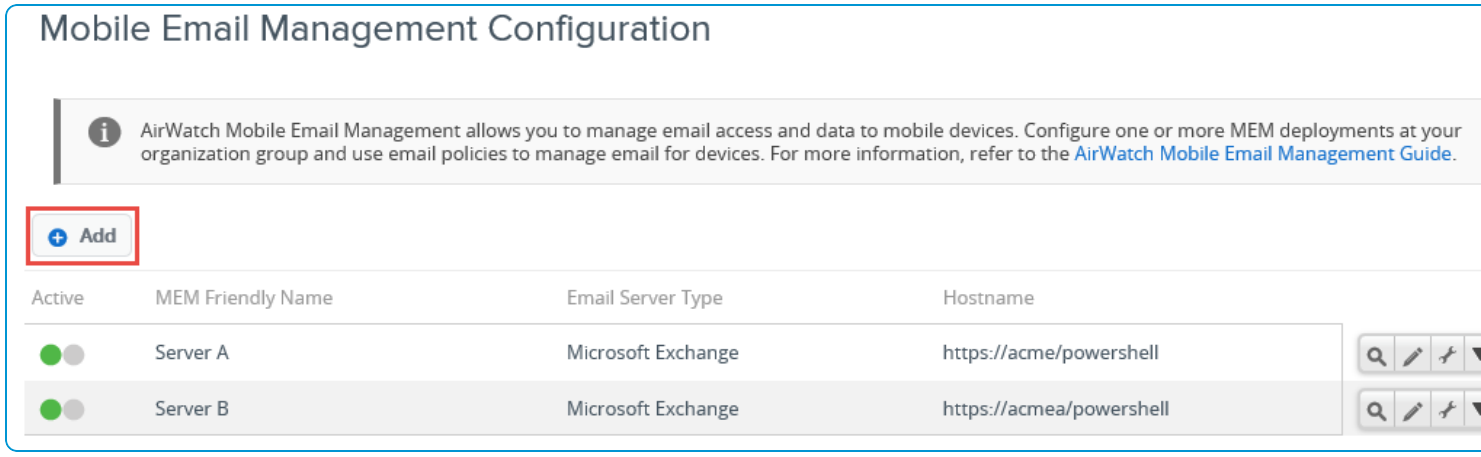
Setting	Description
Limit sync results by	You can restrict the sync action to certain filtered groups by selecting the options: • **None** – Syncs the devices retrieved by the PowerShell queries. • **Organization Unit Configuration** – Organization Unit Configuration limits the sync results to devices whose users are in the selected Organization Unit in Active Directory. The Organization Unit Base DN is fetched from the Directory Services configuration and the Group Search Filter is the Organization Unit name. • **Group** – Group configuration limits the sync results to specific groups defined in Office 365. You can define these groups by navigating to **Exchange Control Panel > Recipients > Groups**. **Note:** The Group sync option is available only for Office 365 implementations. The service account must have the privileges to the Get-Group cmdlet. • **Custom** – Custom configuration limits the sync results to devices whose users belong to the specified Custom DN. The Custom DN can be an Organization Unit or specific users' Distinguished Name. Custom configuration is useful for piloting PowerShell integration against a small subset of users.

4. Select **Next**. The Profiles wizard form displays.
5. (Optional) If you plan to migrate the users from an existing MEM configuration, then associate a profile with the MEM configuration.



6. Select **Next**. The MEM Config Summary form provides a quick overview of the basic configuration you have just created for the PowerShell deployment. **Save** the settings.

7. You can select the **Add** option from the **Mobile Email Management Configuration** main page to configure more deployments.



8. Optionally, you can configure the Advanced Settings. To configure, navigate to **Email** > **Settings**page and then select the  icon.

Setting	Description
PowerShell Sync Batch Size	The batch size determines the number of CasMailbox and ActiveSyncDevice/MobileDevice objects returned per PowerShell session when using the Sync Mailboxes or Run Compliance features. The batch size depends on whether VMware Enterprise Systems Connector or Enterprise Integration Service (EIS) is being used. For VMware Enterprise Systems Connector and direct connection, the number of devices is 25000 and for EIS 2500 devices. The PowerShell MEM config detects these conditions and sets the batch size accordingly.
Manage Active Sync for Mailbox	Select to enable control of Active Sync at the Mailbox Identity level. In proper deployments, it is not necessary as a Global Access State of Block or Quarantine is in use.
Remove ActiveSync Partnership on Unenroll	Select to remove partnership of the unenrolled device from Exchange. This setting removes unenrolled devices from Exchange when they are removed from AirWatch.
Sync with entire forest in AD	Select to add the viewEntireForest option to the PowerShell session. This option might be helpful depending on how your company's Organization Groups are structured.

Configure Exchange to Block or Quarantine Devices

To manage new devices trying to connect to email for the first time, configure Exchange to either Block or Quarantine devices from an organizational level. Exchange can be configured through either an Exchange PowerShell session or web interface. For Office 365 and Microsoft Exchange 2010/2013/2016 users, access the web UI through an administrator's Outlook Web Access (OWA) portal.

To configure Exchange through PowerShell:

1. Configure your organizational settings so that they block or quarantine devices. Blocking devices blocks the device outright while quarantining provides you more visibility to unknown devices. However, quarantining also uses more processing power.
2. Open the Exchange PowerShell command window from the Exchange Server and enter the following command to:
   a. Quarantine devices

```
PS C:\Windows\system32> Set-ActiveSyncOrganizationSettings –DefaultAccessLevel
quarantine
```

   b. Block devices

```
PS C:\Windows\system32> Set-ActiveSyncOrganizationSettings –DefaultAccessLevel
Block
```

Caution: The preceding instructions block or quarantine new devices until they enroll in the UEM console, at which point, Workspace ONE UEM issues relevant PowerShell cmdlets to allow email access for the newly enrolled devices. Use caution while enforcing device block or quarantine at the Global level on the Exchange server. While using this setting in a production environment, ensure that all your devices are enrolled. Typically, this setting is not used during a trial or evaluation. The cmdlet might also temporarily block or quarantine enrolled devices until they check into AirWatch. Quarantining or blocking devices from accessing email over ActiveSync allows organizations to ensure that only approved (that is, Workspace ONE UEM managed) devices are allowed for email access. Without this enforcement, there is the possibility that unmanaged devices might gain temporary access to corporate email. The temporary access is until the next PowerShell sync process discovers and blocks them. Define a custom email message for users with blocked devices. Microsoft Exchange can then automatically send users a notification to enroll, when their blocked device attempts to access email.
For further information, refer http://blogs.technet.com/b/exchange/archive/2010/11/15/3411539.aspx.

Chapter 4:
Server-Side Session

Server-Side Session Commands

After configuring the Windows PowerShell session on your UEM console server for issuing remote commands to Exchange 2010/2013/2016 or the cloud-based Office 365 service, connect to the server environment to begin the server-side session.

Following contains the commands to control the Exchange mailbox properties:

- Command to connect to the server-side session and to establish a new session.

```
PS C:\Windows\system32> $cred = Get-Credential
PS C:\Windows\system32> $session = New-PSSession -ConfigurationName
Microsoft.Exchange -ConnectionUri "https://Exchange.Server.URL.com/powershell/" -Credential $cred -
Authentication Basic -AllowRedirection
```

  Press enter after authentication to run the $session command.

- Command to import the server-side session. Issue this command after successfully connecting to the server.

```
PS C:\Windows\system32> Import-PSSession $session
PS C:\Windows\system32>
```

- Command to perform mailbox queries – During the device enrollment in AirWatch, devices can be configured for the exchange through the profile distribution. When properly configured, the UEM console issues commands to enable the Exchange ActiveSync for a user's mailbox on Exchange. The Workspace ONE UEM console also issues a command to whitelist the device ID being enrolled. To see what devices are whitelisted for a mailbox, use the command **Get-CASMailbox** to select the allowed devices.

Command:

```
PS C:\Windows\system32> get-casmailbox -Identity "user.name@mail.com" | select
{$_.ActiveSyncAllowedDeviceIDs}
```

Result:

```
$_.ActiveSyncAllowedDeviceIDs
-----------------------------
{ApplDLXGL5FGDJHF, B058C150E57CC4004DA6B2E1BE4EE572}
```

Likewise, query a user's mailbox to view the blacklisted or blocked device IDs as shown in the following example.

Command:

```
PS C:\Windows\system32> get-casmailbox -Identity "user.name@mail.com" | select
{$_.ActiveSyncBlockedDeviceIDs}
```

Result:

```
$_.ActiveSyncBlockedDeviceIDs
-----------------------------
{Appl87049106A4S, DT095F898778SDF2E1B3453445DG56}
```

- Command to close the Server-side session – Always close the console-server session when troubleshooting is complete. To remove the server-side session, use the ***remove-PSSession*** command.

```
PS C:\Windows\system32> remove-pssession $session
PS C:\Windows\system32>
```

- Command to display the PowerShell version – To know the version of the PowerShell installed, enter **$PSVersionTable** on the PowerShell command window.

```
PS C:\Windows\system32> $PSVersionTable
```

Chapter 5:
Email Management

Manage Emails Through PowerShell

Email management through PowerShell involves syncing of mailboxes and applying email policies for enrolled devices.

To begin managing emails for mobile devices connected to the Exchange server, follow the outlined process:

1. To pull in all devices having an EAS partnership, sync all mailboxes (from the Workspace ONE UEM Email Dashboard) with Exchange.
2. Allow devices to begin enrollments and continue to sync daily to check for devices that convert from Unmanaged to Managed status.
3. At any point, choose to create and apply a Workspace ONE UEM Email Policy (refer Email Security Policies) to block unmanaged devices.

> **Note:** For migration from SEG deployments to PowerShell deployments, work with your Workspace ONE UEM contact to identify an optimum solution for your enterprise.

Email Security Policies for PowerShell Integration

Email policies enhance security by restricting email access to non-compliant, unencrypted, inactive, or unmanaged devices. These policies allow you to provide email access to only the required and approved devices. Email policies also restrict email access based on the device model and the operating systems.

These policies are available from **Email** > **Compliance Policies** in the UEM console. Activate or deactivate the policies using the colored buttons under the **Active** column. Use the edit policy icon under the **Actions** column to allow or block a policy.

To restrict access to unmanaged devices even when there are no compliance policies set, Workspace ONE UEM issues allow and block commands upon device enrollment and unenrollment. If you want to prevent Workspace ONE UEM from issuing these automatic commands, you can select **Disable Compliance** on the **Email > Compliance Policies** page of the UEM console.

General Email Policies

Email Policy	Description
Managed Device	Restrict email access only to managed devices.
Mail Client	Restrict email access to a set of mail clients.
User	Restrict email access to a set of users.
EAS Device Type	Allow or block devices based on the EAS Device Type attribute reported by the end-user device.

Managed Device Policies

Managed Device Policy	Description
Inactivity	Allows you to prevent inactive, managed devices from accessing email. You can specify the number of days a device shows up as inactive (that is. does not check in to AirWatch), before email access is cut off.
Device Compromised	Allows you to prevent compromised devices from accessing email. Note, this policy does not block email access for devices that have not reported compromised status to AirWatch.
Encryption	Allows you to prevent email access for unencrypted devices. Note, this policy is applicable only to devices that have reported data protection status to AirWatch.
Model	Allows you to restrict email access based on the Platform and Model of the device.
Operating System	Allows you to restrict email access to a set of operating systems for specific platforms.
Require ActiveSync Profile	Allows you to restrict email access to devices whose email is managed through an Exchange ActiveSync profile.

Important: Mail Client, EAS Device Type, and Inactivity policies require a PowerShell sync before they can be used, as the data is obtained only from Exchange. Except for populating the EAS Device type of AirWatch Inbox on iOS and Android, and the native client of iOS devices, all other device-client combination require a sync.

Testing Email Policies

Testing the email policies before deploying on the devices is a good practice. Use the following method to test the capabilities of these policies before applying them on the devices.

- Disable the **Compliance** option available on the **Email Policies** page during the testing phase. Use a separate organization group to test out policies against a subset user using the user group filter available in the configuration wizard.

Note the compliance option when disabled prevents Workspace ONE UEM from running any automatic PowerShell Cmdlets based on the compliance status in AirWatch. If the default access state for a mailbox is set to Blocked or Quarantined, then that status does not change for devices upon enrollment to Workspace ONE UEM if compliance is disabled.

Device Discovery

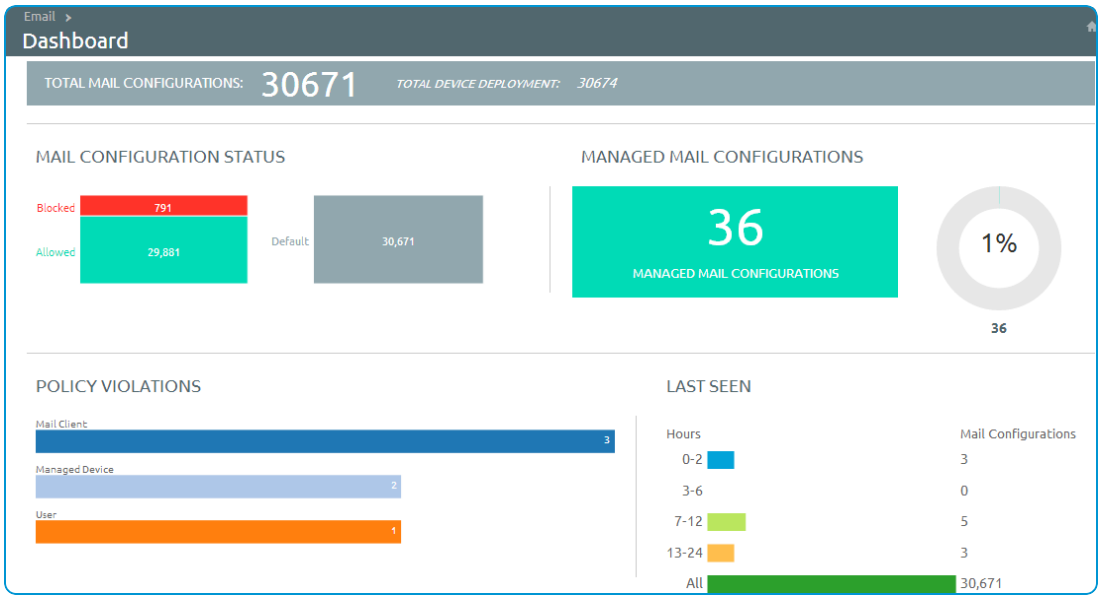
Before you can begin managing the devices from the Email Dashboard, the configured MEM must discover the devices enrolled to the organization group. Based on whether an EAS profile is present on the devices or not, either a command or a broadcast message is sent to discover the devices.

The configured MEM discovers the devices enrolled to the organization group in two ways:

- **With the EAS profile** – Workspace ONE UEM sends an allow command to the relevant EAS profile associated PowerShell environment when you perform **Sync Mailboxes** action from the **List View** page.
- **Without the EAS profile** – Workspace ONE UEM sends an 'Allow' command to all the PowerShell integrated environments. For the environment that the command succeeds against, Workspace ONE UEM automatically associates the device to the corresponding memConfigID.

Email Dashboard

Gain visibility into the email traffic and monitor the devices through the AirWatch **Email Dashboard**. **Email Dashboard** gives you a real-time summary of the status of the devices connected to the email traffic.



You can access the dashboard from **Email > Dashboard**. The email dashboard enables you to:

- Allow or deny access to email by whitelisting or blacklisting a device.
- View the devices which are managed, unmanaged, compliant, non- compliant, blocked, or allowed.
- View the device details such as OS, Model, Platform, Phone Number, IMEI, and IP address.
- Use the available graphs to filter your search.

Email List View

You can view all the real-time updates of your end-user devices that you are managing with VMware AirWatch MEM. Access the **List View** from **Email** > **List View**. You can view the device or user-specific information by switching between the two tabs: **Device** and **User**. You can change the **Layout** to either view the summary or the detailed list of the information based on your requirement.

Device and User Details

The List View screen provides detailed information on device and device users.

List View Screen Fields	Description
Last Request	Displays the last state change of the device either from Workspace ONE UEM or from Exchange.

User	The user account name.
Friendly Name	The friendly name of the device.
MEM Config	The configured MEM deployment that is managing the device.
Email Address	The email address of the user account.
Identifier	The unique alpha-numeric identification code associated with the device.
Mail Client	The email client syncing the emails on the device.
Last Command	The last command sent to email server to manage the device. It populates the **Last Request** column.
Status	The real-time status of the device and whether email is blocked or allowed on it as per the defined policy.
Reason	The reason code for allowing or blocking email on a device. The reason code displays 'Global' and 'Individual' only when an entity other than AirWatch (for example, an external administrator) changes the access state of the email.
Platform, Model, OS, IMEI, EAS Device Type, IP Address	The device information displays in these columns.
Mailbox Identity	The location of the user mailbox in the Active Directory.

Filters for Quick Search

Using the **Filter** option, you can narrow-down your device search based on the following parameters.

Device Search Parameter	Description
Last Seen	All, less than 24 hours, 12 hours, 6 hours, 2 hours.
Managed	All, Managed, Unmanaged.
Allowed	All, Allowed, Blocked.
Policy Override	All, Blacklisted, Whitelisted, Default.
Policy Violation	Compromised, Device Inactive, Not data Protected/Enrolled/MDM Compliant, Unapproved EAS Device Type/Email Account/Mail Client/Model/OS.
MEM Config	Filter devices based on the configured MEM deployments.

Additional Actions

The **Override**, **Actions**, and **Administration** drop-down menu provides a single location to perform multiple actions on a device.

Override

Option	Description

Whitelist	Allows a device to receive emails.
Blacklist	Blocks a device from receiving emails.
Default	Allows or blocks a device based on whether the device is compliant or non compliant.

Actions

Option	Description
Sync mailboxes	• Syncs the mobile device records from the Exchange with the managed mail clients on enrolled devices. • The Sync Mailboxes Confirmation page allows you to sync quickly the devices from a set of mailboxes without having to edit your MEM configuration's existing filter. • You can restrict the sync action at a user, organizational unit, group, or custom level by selecting the options; User, Organizational Unit, Group, or Custom. • If you have set a persistent filter in your MEM configuration, you can select the Use pre-configured settings check box. • Workspace ONE UEM offers the Email Sync option within the Self Service Portal so that end users can sync their devices with the mail server and also run preconfigured compliance policies for all their devices. This process is typically much faster than the bulk sync performed on all the devices.
Run Compliance	Triggers the compliance engine to run for the selected MEM configuration.

Note: When the Direct PowerShell Model is configured, Workspace ONE UEM communicates directly to the CAS array through remote signed PowerShell sessions established from the console server or VMware Enterprise Systems Connector (depending on the deployment architecture). Using remote signed sessions, commands are sent to blacklist (block) and whitelist (allow) device IDs on a given user's CAS mailbox in Exchange 2010, 2013, 2016, and Office 365. Blacklisting and whitelisting are based on the device's compliance status in AirWatch.
The 'DefaultAccessLevel' on the Exchange server does not change on running compliance. This setting applies only to known devices and overrides the access controls defined by 'DefaultAccessLevel'. If 'DefaultAccessLevel' is set to allow, then new unmanaged devices can access email. Devices can be manually blocked through the UEM console. It is a best practice to test the expected PowerShell integration behavior without enforcing device blocking across the enterprise.

Administration

Option	Description
Enrollment Email	Sends an email to the user with all the details required for enrollment.
Delete Unmanaged Devices	Deletes the selected unmanaged device records from the dashboard. Note, this record might reappear after the next sync.

Remote Wipe	Resets the device to factory settings.
Sync Selected Mailbox	Syncs the selected device mailbox. Only one device mailbox at a time can be synced.

Note: These additional actions once performed cannot be undone.

Chapter 6:
Cmdlets Executed by Workspace ONE UEM

Cmdlets

The Exchange Management Shell includes various cmdlets commands to configure everything from mailbox quotas to SMTP relay settings. Cmdlets are typically named with a <verb> - <noun> convention, such as in Get-CASMailbox. Workspace ONE UEM uses the PowerShell cmdlets to establish the remote PowerShell session.

New-PSSession

- Creates a persistent PowerShell connection to a local or remote host. Once the session is open, the client can perform any number of PowerShell commands.
- Performs Set-CASMailbox and updates three distinct parameters for a mailbox when Workspace ONE UEM uses this connection: ActiveSyncAllowedDeviceIDs, ActiveSyncBlockedDeviceIDs, and ActiveSyncEnabled.

  For example:

  - New-PSSessionOption -SkipRevocationCheck -SkipCACheck -SkipCNCheck–ProxyAccessType WinHttpConfig
  - New-PSSession –ConfigurationName $configurationName -ConnectionUri $connectionUri -Credential $cred -Authentication $authentication-AllowRedirection -SessionOption $proxyOption

Import-PSSession

Helps to import PowerShell commands from one PowerShell session to another. For example:

- Import-PSSession –AllowClobber -CommandName $commandToImport -FormatTypeName

Set-ExecutionPolicy

Allows the client to modify its preferences for the PowerShell execution policy. **Set-ExecutionPolicy** also helps to determine if the client has the permissions necessary to perform certain PowerShell commands.

Set-CASMailbox

Helps to block or allow client access to specific user's mailboxes over several client applications, including ActiveSync. Using this cmdlet, Workspace ONE UEM can block particular devices or users from accessing ActiveSync based on the device compliance and user compliance to MDM policies. Workspace ONE UEM specifically uses the following arguments to this cmdlet. For example:

- Set-CASMailbox "acmeuser" - ActiveSyncAllowedDeviceIDs{Appl123456ABCD78} - ActiveSyncBlockedDeviceIDs $null - ActiveSyncEnabled $true

> **Note:** The Set-CASMailbox cmdlet operates on one mailbox at a time and can configure properties for Exchange ActiveSync. You can configure a single property or multiple properties by using one statement.

- ActiveSyncAllowedDeviceIDs - Helps to whitelist particular device IDs that can access the mailbox through ActiveSync. The ActiveSyncAllowedDeviceIDs parameter accepts a list of device IDs that are allowed to synchronize with the mailbox.
- ActiveSyncBlockedDeviceIDs - Helps to blacklist particular device IDs that cannot access the mailbox using ActiveSync. The ActiveSyncBlockedDeviceIDs parameter accepts a list of device IDs that are not allowed to synchronize with the mailbox.
- ActiveSyncEnabled - Helps to enable or disable ActiveSync access for a particular mailbox. TheActiveSyncEnabled parameter specifies whether to enable Exchange ActiveSync.

Get-CASMailbox

Returns the list of attributes of a mailbox. This cmdlet is also used for performing one time sync of mailbox. For example:

- Get-CASMailbox "acmeuser" | Select ActiveSyncAllowedDeviceIDs,ActiveSyncBlockedDeviceIDs
- Get-CASMailbox –Filter $filter $–ResultSize Unlimited
- Get-CasMailbox –Identity $identity

Set-ADServer Settings

- Set-AdServerSettings –ViewEntireForest $true/$false

Get-ActiveSyncDevice

Retrieves a list of devices in your organization that have active Microsoft Exchange ActiveSync partnerships. This cmdlet is also used for performing one time sync of mailbox. Administrators must now select the Exchange 2010 MEMconfig option for 'Get-ActiveSyncDevice', and the Exchange 2013/Office 365 option for 'Get-MobileDevice'.

For Exchange 2010:

- Get - ActiveSyncDevice –Mailbox "acmeuser"
- Get-ActiveSyncDevice –ResultSize Unlimited
- Get-ActiveSyncDevice –Mailbox $mailbox

For Exchange 2013/2016/Office 365:

- Get-MobileDevice –Mailbox "acmeuser"
- Get-MobileDevice –ResultSize Unlimited
- Get-MobileDevice –Mailbox $mailbox

AW-Get-ADGroups

The Get-ADGroup cmdlet gets a group or performs a search to retrieve multiple groups from an Active Directory. For example:

- Get-OrganizationalUnit

Clear-ActiveSyncDevice

Deletes all user data from a mobile phone the next time that the device receives data from the server (for example, syncs with Microsoft Exchange Server 2010). Sets the ***DeviceWipeStatus*** parameter to $true in Exchange. For example:

- Clear-ActiveSyncDevice –Identity $identity –Confirm $true/$false

Remove-PSSession

Closes or ends the Windows PowerShell session.

Chapter 7:
Multiple PowerShell Deployments

Workspace ONE UEM provides you the flexibility of integrating multiple PowerShell deployments with a specific VMware Enterprise Systems Connector server from a list of VMware Enterprise Systems Connector servers that have been configured for the child organization groups. This integration allows you to connect to multiple domains seamlessly. Multiple VMware Enterprise Systems Connector is enabled by default. This option is available for Workspace ONE UEM administrators and system administrators only. Also, this option is available only if you have child organization groups configured for a particular organization group.

By default, PowerShell integrations use an VMware Enterprise Systems Connector configuration that is available at the current organization group or inherited from a parent organization group. In the PowerShell configuration wizard, you can select a specific configured VMware Enterprise Systems Connector to integrate with that PowerShell deployment. From the **VMware Enterprise Systems Connector Configuration for PowerShell integration** drop-down, you can select from the listed configured VMware Enterprise Systems Connector.