RoomWizard Exchange Connector

Complete Implementation/Upgrade Guide
Microsoft Exchange On-Premises
Microsoft Office 365

Steelcase

Table of Contents

RoomWizard Exchange Connector 1
Getting Started 4
Before installing and configuring the Exchange Connector, you will need the following: 4
What is autodiscovery and how does it work? 4
What is Impersonation and how does it work? 4
Exchange Connector Installation Prerequisites 5
Server Manager – IIS Install (See Appendix A) 5
Additional Requirements (See Appendix B) 5
Application Impersonation (See Appendix C) 5
Preparing your Environment 6
Configuring Basic Authentication(IIS) 6
Create a New Website Running on a .NET 4.0 Application Pool 9
Configuring the Exchange Connector 15
O365 Configuration 16
Exchange OnPrem Configuration 16
Generate a New Configuration 17
To use the demo for up to 90 days: 17
To update your configuration from a demo to a licensed version: 17
Test Connection Using Connector Test Tool 18
Configuring the RoomWizard 20
Appendix A (IIS) 22
Installing the IIS Role and additional Features (Server 2016) 22
Appendix B (Installing and Configuring ASP.NET MVC3 and Web Deploy 3.6) 30
Install ASP.NET MVC 3 30
Installing and Configuring Web Deploy 3.6 32
Appendix C (Application Impersonation) 36
Configuring Application Impersonation Via EAC 36
Appendix D (PowerShell Commands) 39
Establishing Remote Session with Outlook 39
Granting Application Impersonation Role Manually via PowerShell 39
Grant the Application Impersonation role: 39
Check if a user has the Application Impersonation role: 39
Configuring Room Mailbox 39
Configure every room's mailbox to auto-accept invitations: 39
Configure a specific room's mailbox to auto-accept invitations: 39
Viewing Attendee Response Status from RoomWizard 40
Find and grant all users and grants a service user full access: 40
Visit Steelcase.com 40

Getting Started

Before installing and configuring the Exchange Connector, you will need the following:

- Windows server on which to install the connector (details below)
- Connector package downloaded and unzipped, on the desktop of the Web Server
- Local domain service account that can be used to log in to the Web Server
- User account configured with Application Impersonation in Exchange/Office 365 that the connector will use to connect to Exchange (one Enterprise-type account, E1 and above) Microsoft link
- Resources mailboxes for calendars (one for each RoomWizard) configured to auto accept or decline meetings https://docs.microsoft.com/en-us/exchange/recipients/room-mailboxes
  Note: Newly created accounts and resources take three hours to replicate with Microsoft
- Exchange Web Services (EWS) server URL for the customer's Exchange service (not applicable in Exchange 2013 environments)
  - URL will be different for each hosting provider
  - Connector will use Exchange's autodiscovery to locate the EWS server, but some environments won't have autodiscovery configured.

What is autodiscovery and how does it work?

Autodiscovery is a process that Microsoft supports for locating Exchange Web Services servers based on an email address or domain. This is usually easier than specifying an EWS URL because most people know an email address but not the name of a server. To test Exchange Web Services connections, you can use Microsoft's Test Connectivity Analyzer: testconnectivity.microsoft.com

What is Impersonation and how does it work?

Exchange Impersonation is a mechanism that allows a single Windows Active Directory account (your RoomWizard Service account) to act on behalf of other users on a Microsoft Exchange mailbox (your RoomWizard Resource Mailboxes), as if they were performing the action themselves.

This greatly reduces the number of connections counted against the service account. Too many connections by any one account will result in Exchange throttling back access by that account through the EWS API. See Appendix D for configuring Exchange and Impersonation.

https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/impersonation-and-ews-in-exchange

Exchange Connector Installation Prerequisites

Please note: All Pre-requisites MUST be installed prior to installing and configuring the Exchange Connector.

- Server 2012 or Server 2016
- IIS Version 8, 9 or 10
- Port 8080 open in Server firewall; this will be used when configuring the Connector Website

Server Manager – IIS Install (See Appendix A)

- Internet Information Services (Features)
- .NET Framework 3.5, and 4.6

- Internet Information Services (Web Server Roles)
- Security | Basic Authentication
- Application Development (Full)
- Web Management Tools | IIS Web Management Console
- Web Management Tools | Management Service

Additional Requirements (See Appendix B)

- Web Deploy (Web Deployment Tool) in IIS https://www.iis.net/downloads/microsoft/web-deploy
- ASP.NET MVC3 Extension https://www.microsoft.com/en-us/download/details.aspx?id=1491

Application Impersonation (See Appendix C)

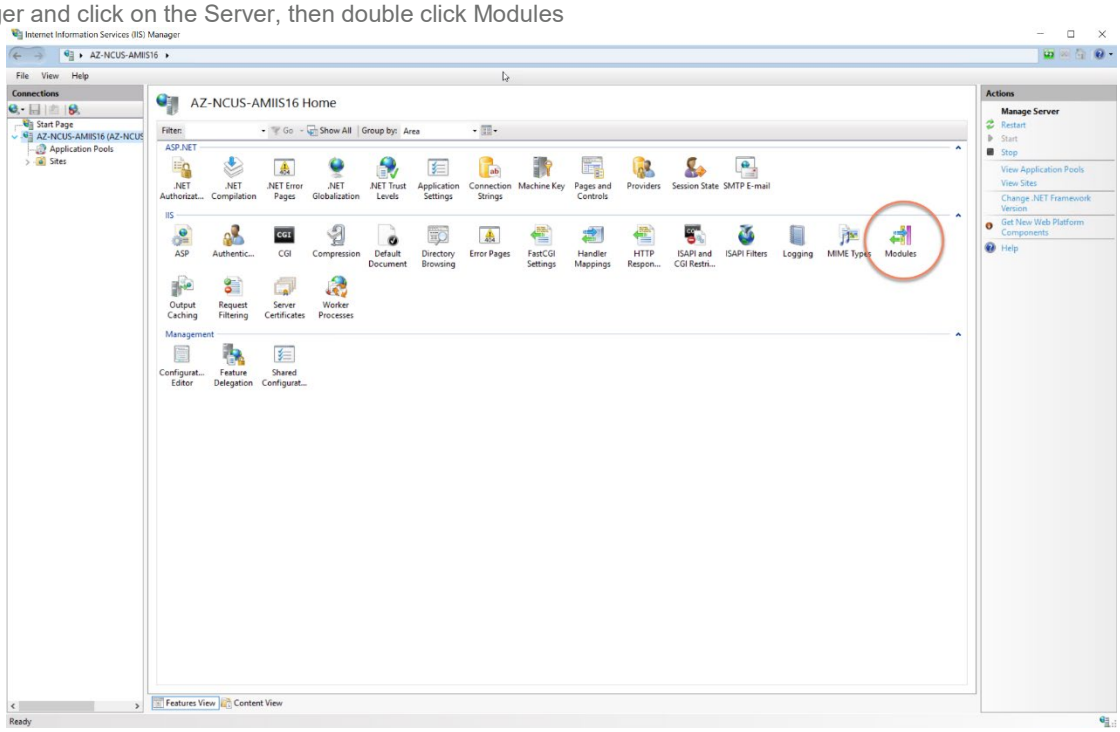
- https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/how-to-configure-impersonation
- https://kb.infobridge.com/hc/en-us/articles/202705692-How-to-set-Impersonation-in-Microsoft-Office-365-and-Microsoft-Exchange-2013

Preparing your Environment

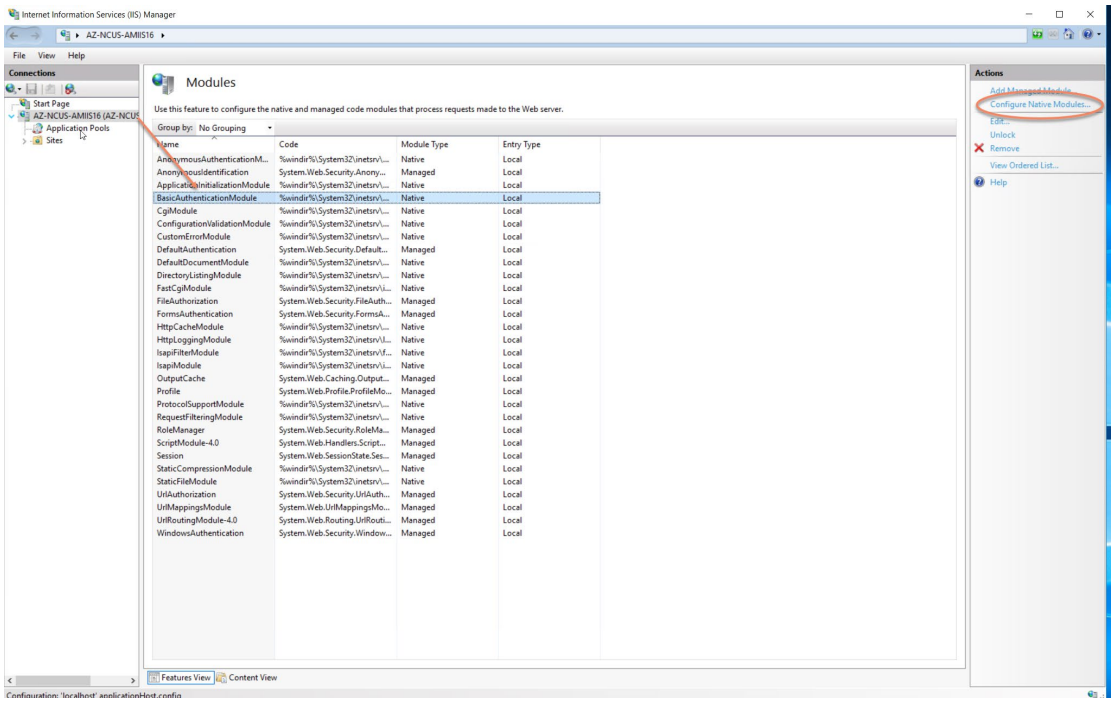
Configuring Basic Authentication(IIS)

These steps will be performed after the prerequisites in the above section have been completed.

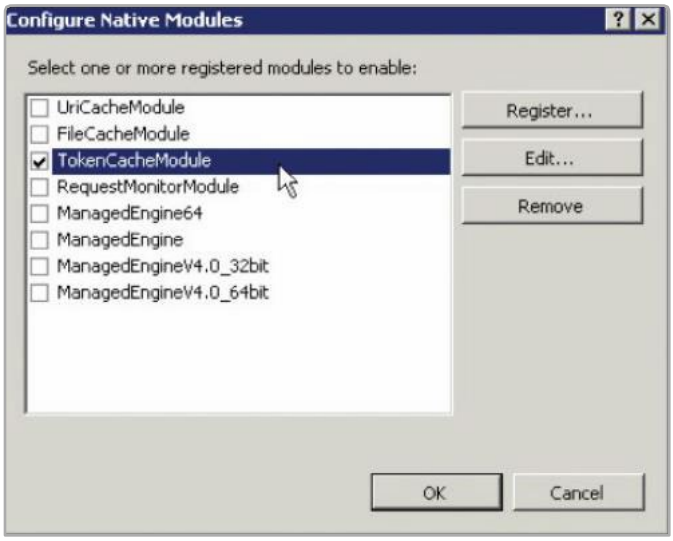
Start IIS Manager and click on the Server, then double click Modules



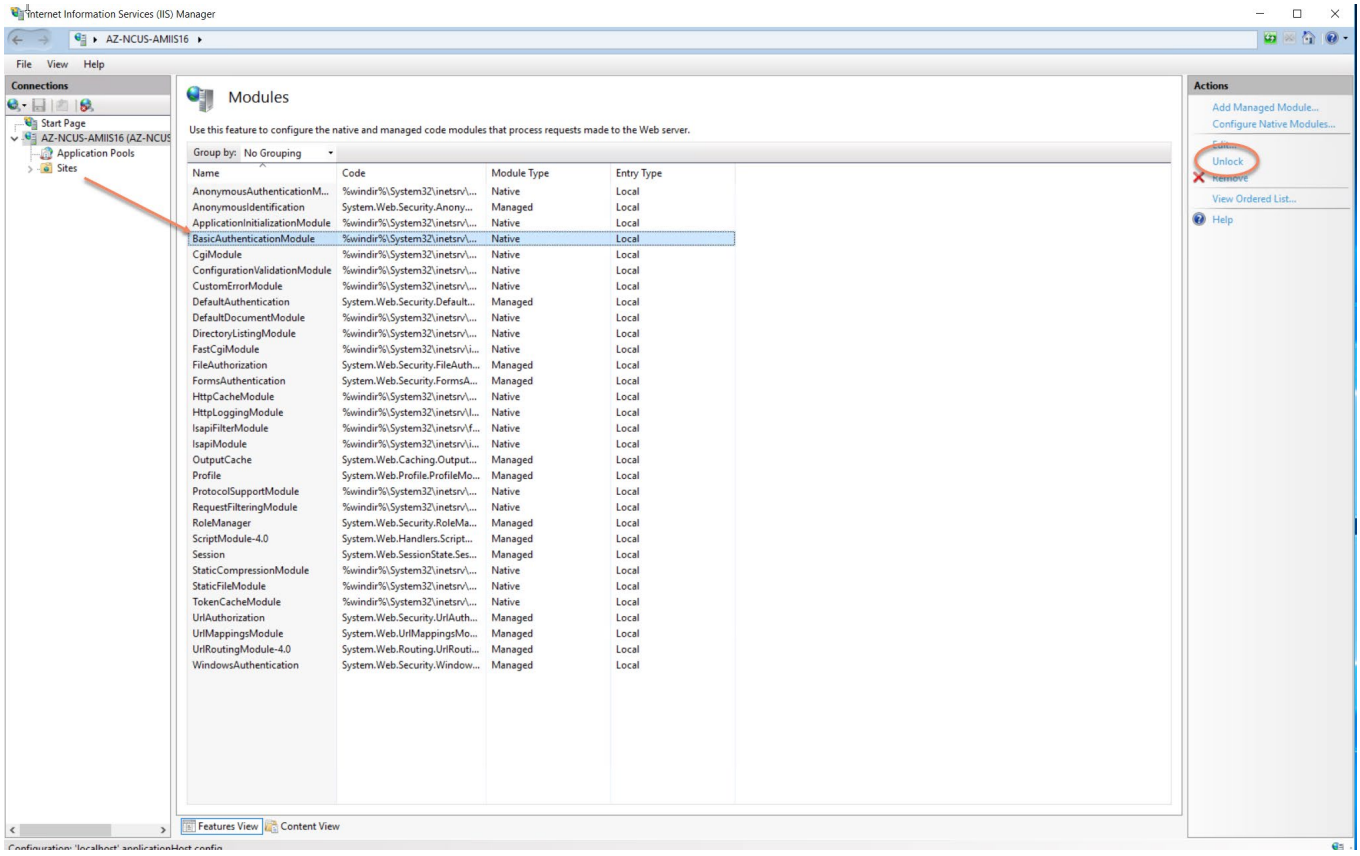
Single Click BasicAuthenticationModule and choose Configure Native Module

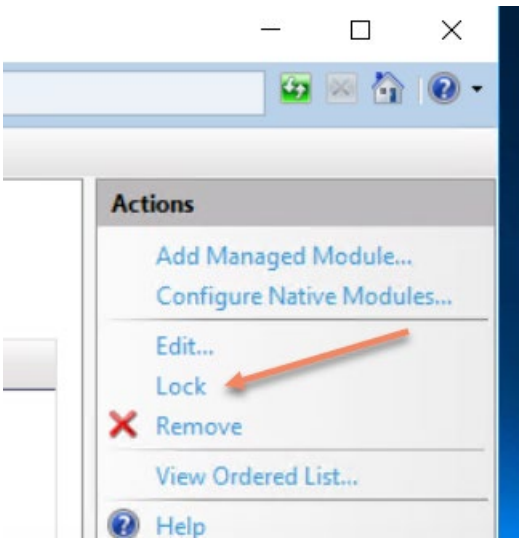


TokenCacheModule should be in the list that appears. Check the box next to it. (If TokenCacheModule does not show in the list, disregard this step.) Then clilck OK



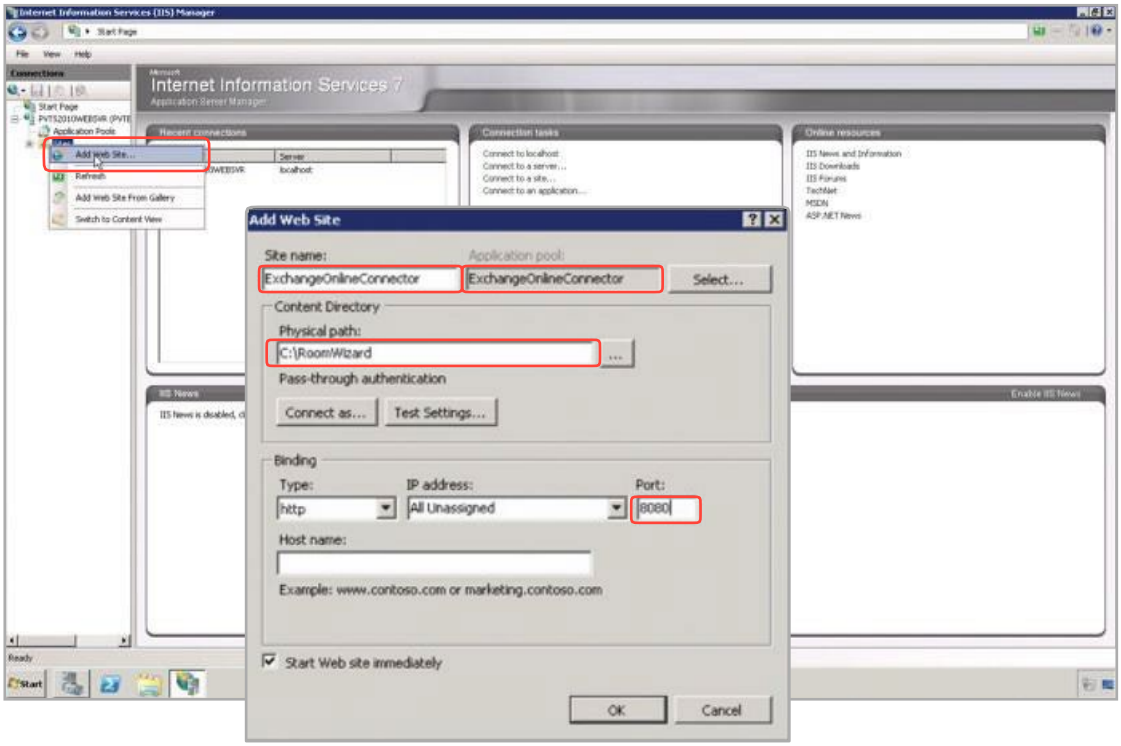
Single click on BasicAuthenticationModule again and click the Unlock so that it reads Lock




Actions
Add Managed Module...
Configure Native Modules...
Edit...
Lock
Remove
View Ordered List...
Help

Create a New Website Running on a .NET 4.0 Application Pool

Right-click on the **Sites** folder in the left pane of IIS Manager and select **Add Web Site** to begin. This will open the Add Web Site dialog box.



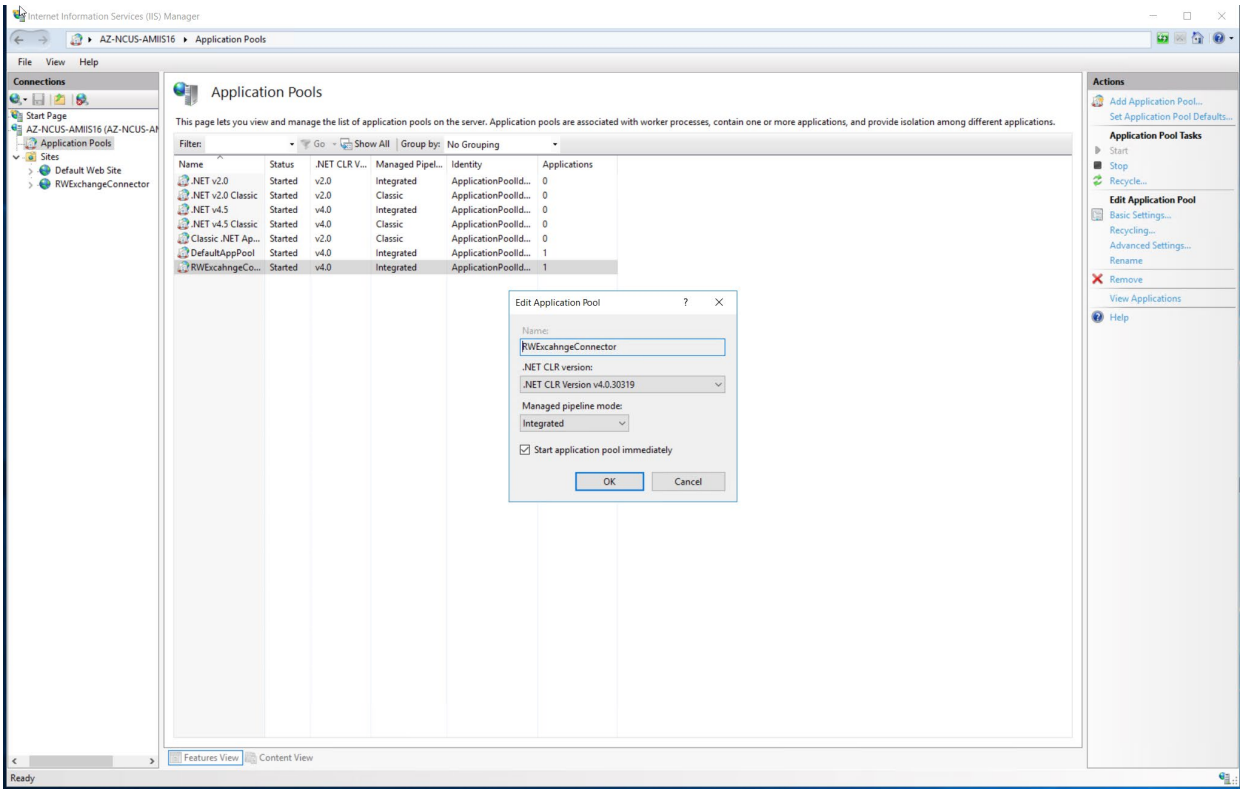
In the Add Web Site dialog box, enter information for these fields:

- **Site name:** Enter a name for your website
- **Application pool:** Note what Application pool your website is going to use; you will configure that in the next step
- **Physical path:** Choose where on the server drive the connector application files will reside. You may need to create a new empty folder for this, such as C:\RoomWizard
- **Binding:** Configure the Port section so that it will not conflict with other sites running on the Web Server. “8080” is used in the example above. *Note: Make sure you use a port open within your environment.*

Click **OK** to create the site.

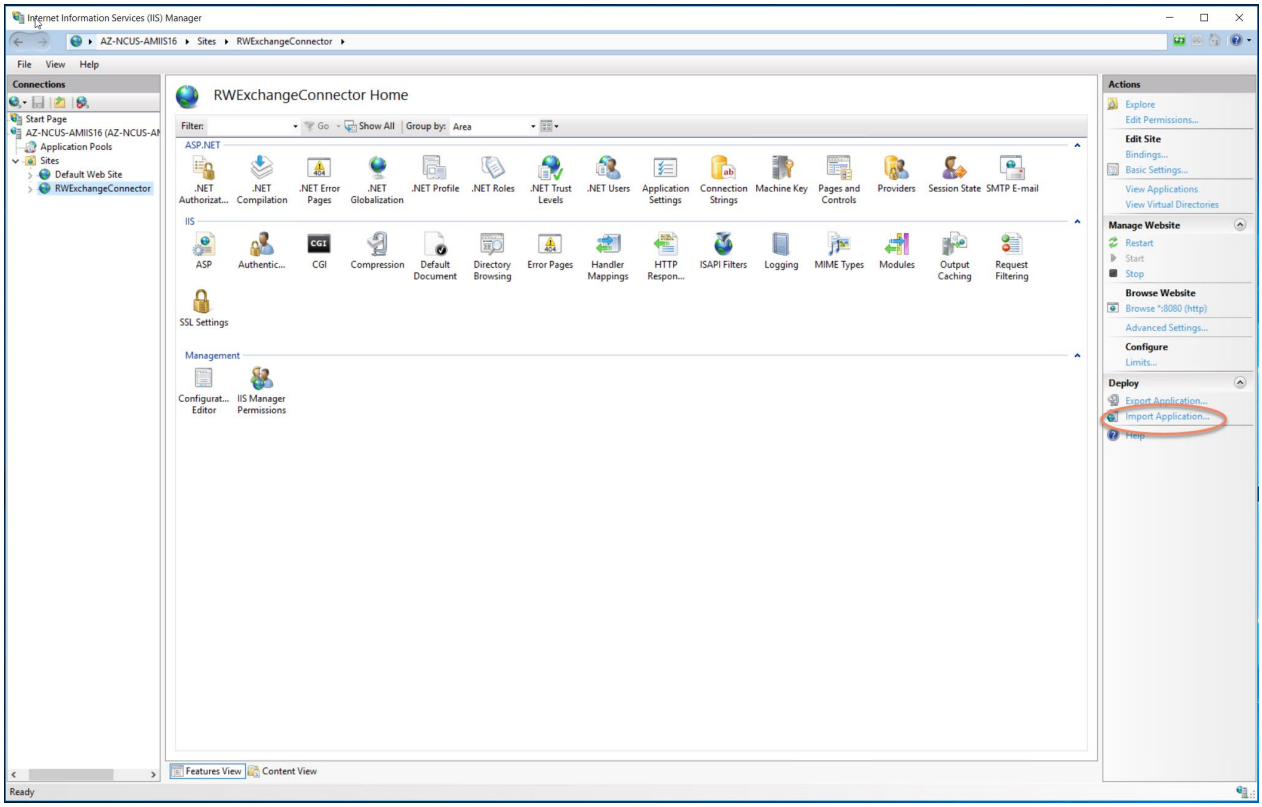
To configure the Application pool, click **Application Pools** in the left pane to bring up the list of current application pools on the server.

Double-click the Application pool you configured for the new site to use. This will bring up the Edit Application Pool dialog box.

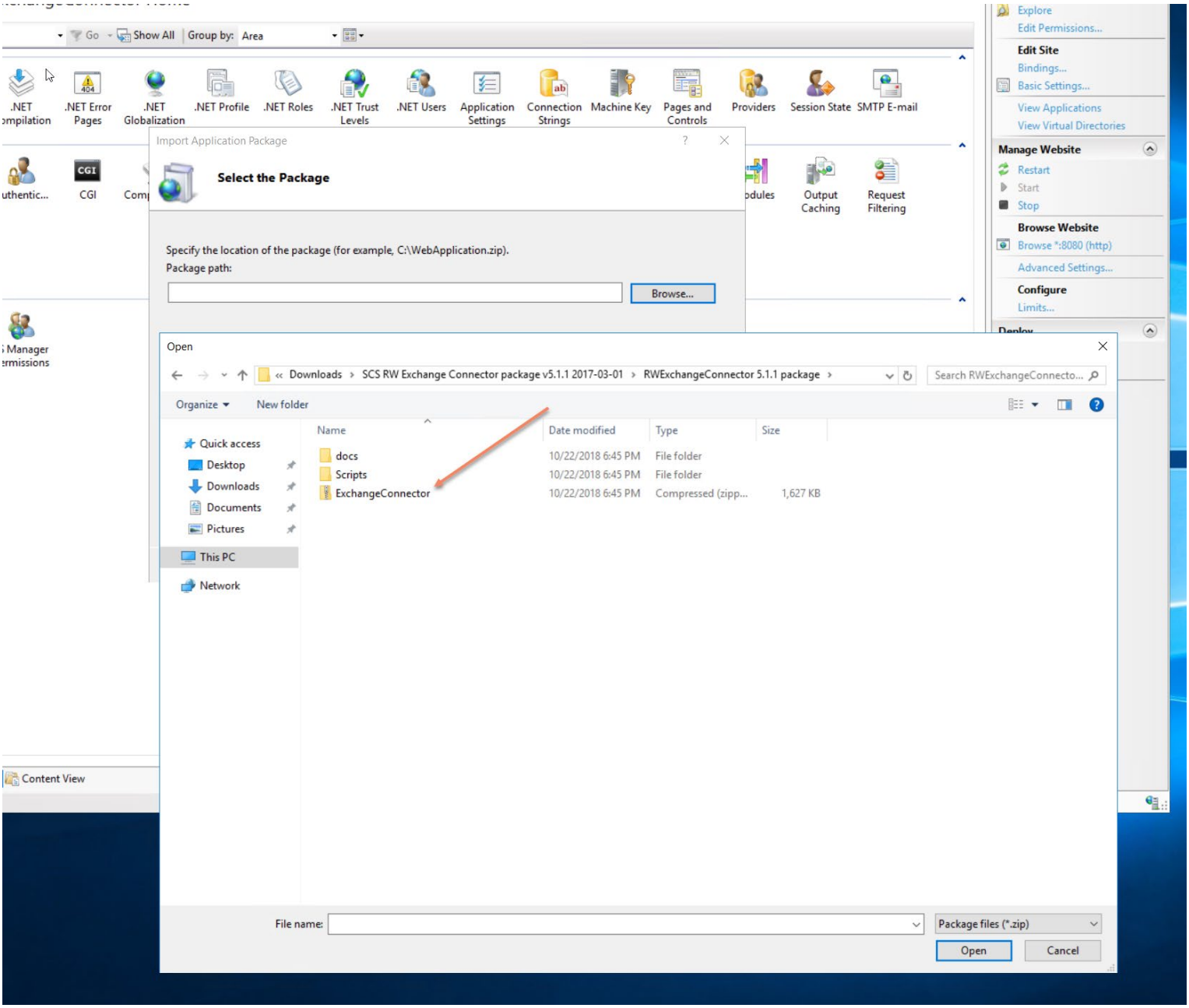


Select **.NET Framework v4.0.xxxxx** from the list. If it doesn't appear in the list, make sure you have the .NET framework version 4 installed. Click **OK** to save the changes.

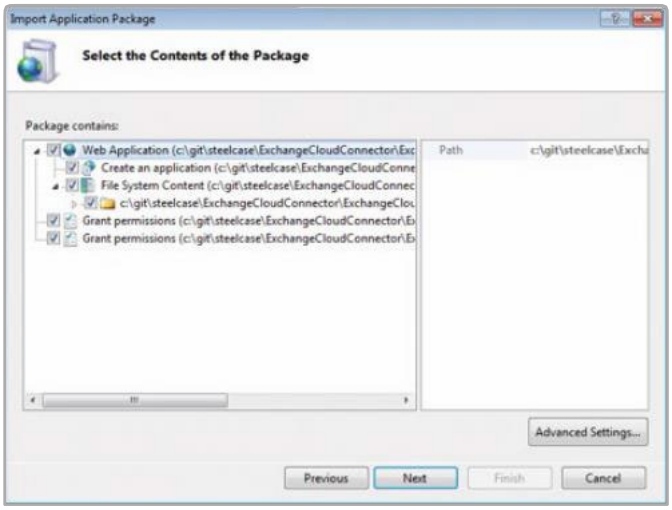
Now click back on the new website you created. Next, in the right-hand pane click on **Import Application**. This will let you import a zipped application bundle into the website.



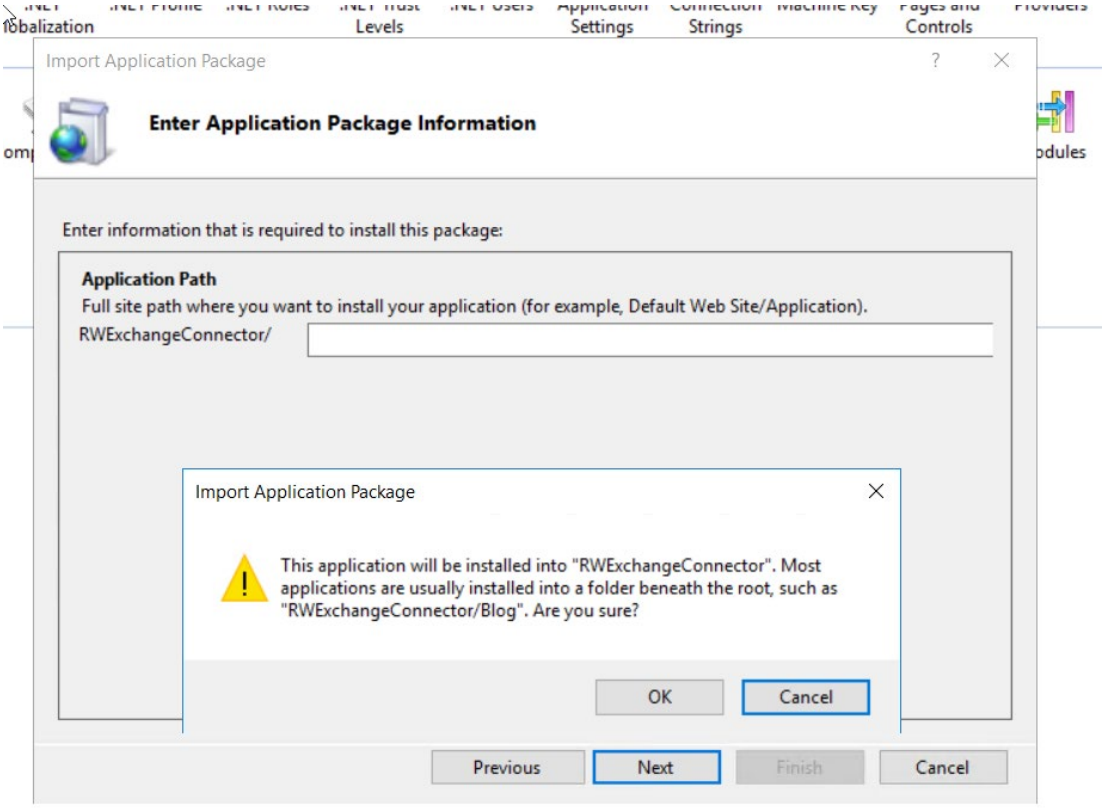
Click **Browse** and locate the zip file containing the **Exchange Connector** (this is in the Connector package you downloaded and unzipped on the Desktop of Web Server). Click **Next** to continue.



The defaults are correct below. Copy all of the contents of the zip file and click **Next** to continue.

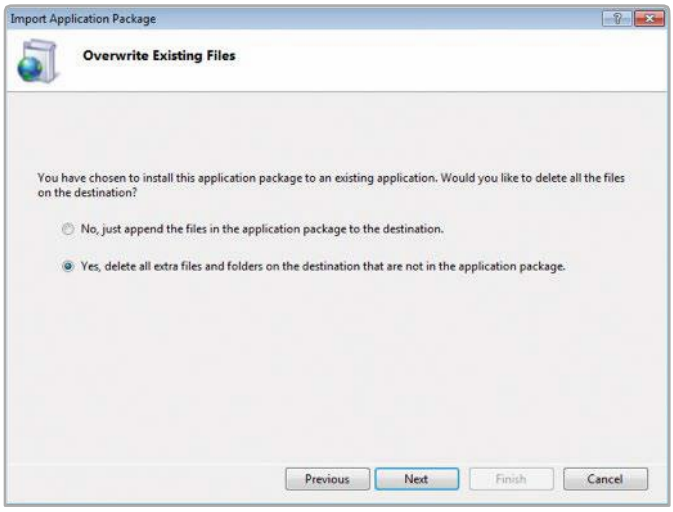


Clear the text in the Application Path box to install it in the root of the site. A dialog box will appear confirming your choice to install the application at the root of the site instead of in a folder beneath the root. Click **OK**, then click **Next** to continue.

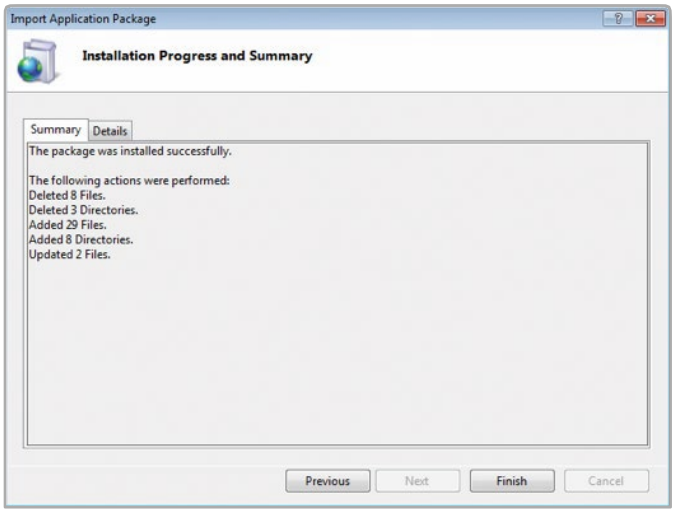


On the Overwrite Existing Files page:

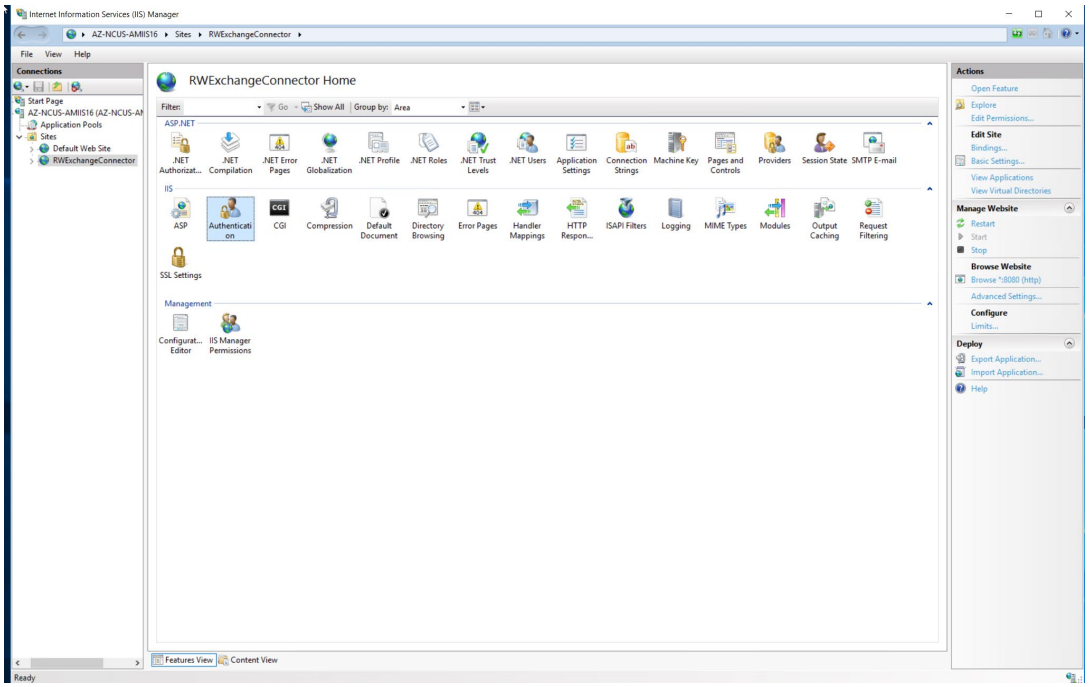
- If this is the first installation, the value chosen here will not matter
- If you are upgrading an existing Exchange Connector, click **Yes**
- Click **Next** to continue



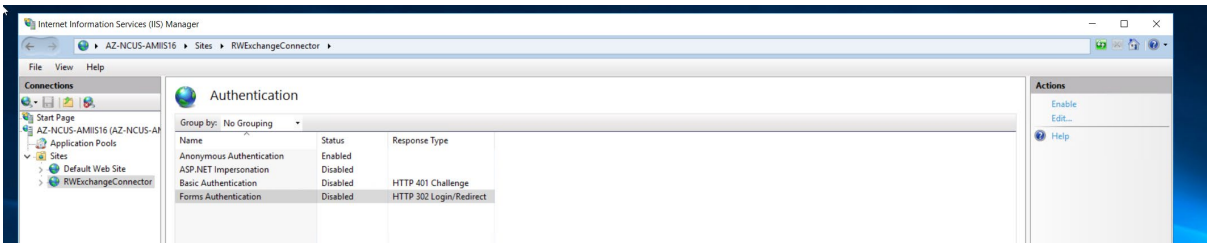
The application has now been installed. Click **Finish** to exit the site installer.



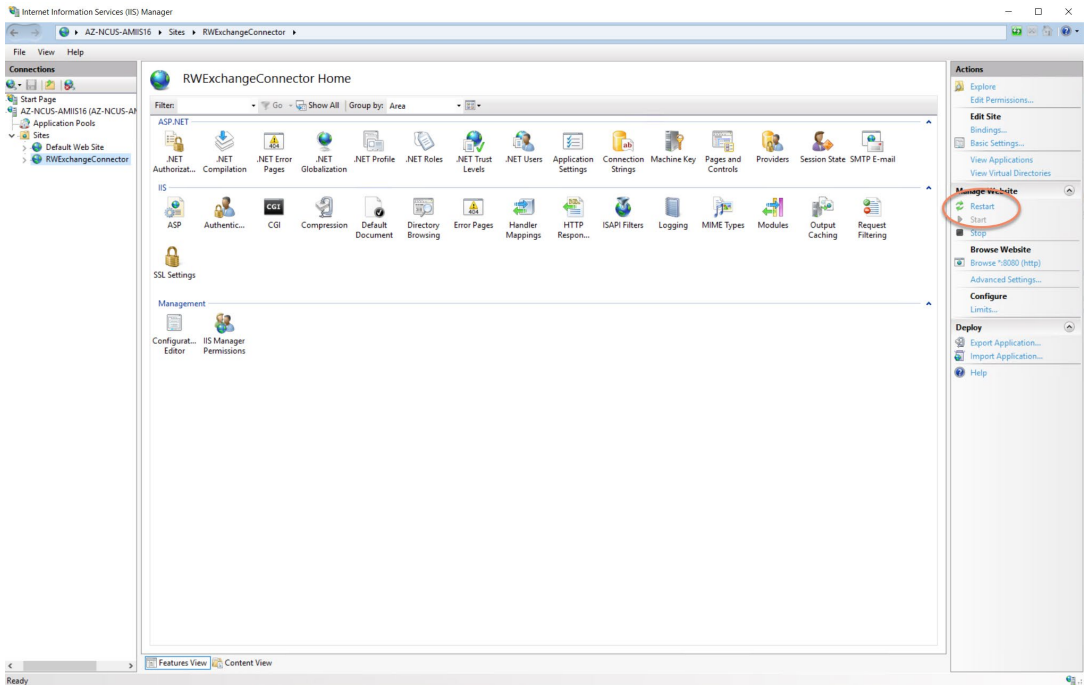
Once this is complete we will need to click on the Web Application and then Double click Basic Authentication



Disable all forms of Authentication except Anonymous



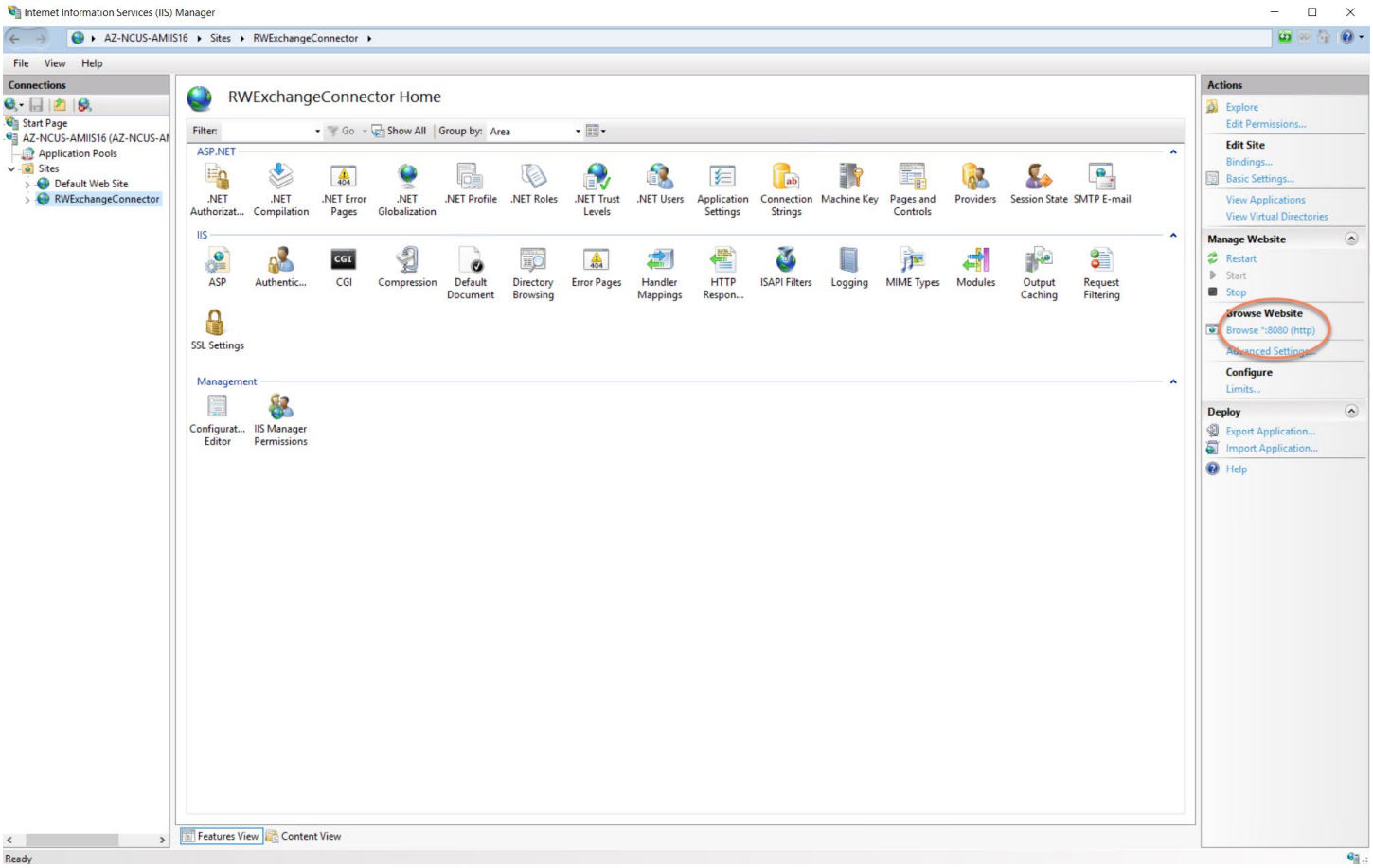
Restart the Web Site



Configuring the Exchange Connector

Your connector is now ready to be configured with your Exchange username, password and license key. Browse your Exchange Connector website and provide login credentials for your server when prompted.

Click on your website and in the right navigation pane click Browse



Your server's web browser will open the web page of your newly installed Connector. This is the configuration page for your connection to Exchange.

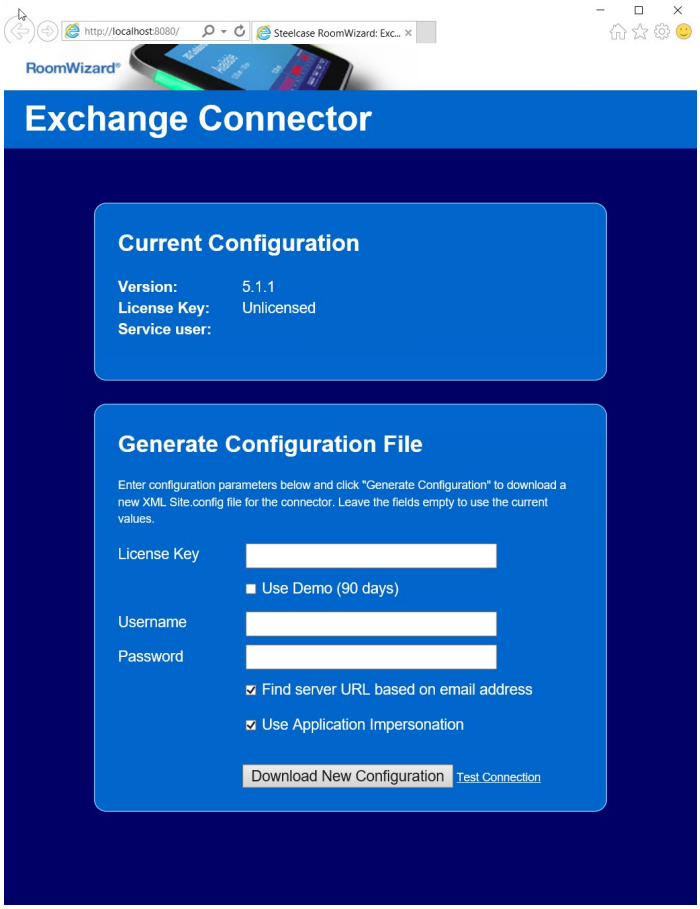
Note: If Basic Authentication for this website was enabled in a previous step, you will be asked for credentials from Windows Security. Please log in using the local domain service account you created according to the Connector prerequisites noted on page 2.

The URL will be based on how you set up your website. For example, if you installed the connector on a server named Server, and configured it to run on port 8080, browse to http://server:8080/.

O365 Configuration

The Exchange Connector needs three pieces of information to operate:

- License key or a 90-day Use Demo
- Username (email address) for the Exchange account for which Application Impersonation was enabled for the RoomWizard resource calendars—this should be in the form user@domain.com, not domain\user
- Password for the Exchange account



Exchange OnPrem Configuration

The Exchange Connector needs three pieces of information to operate:

- License key or a 90-day Use Demo
- Username (email address) for the Exchange account for which Application Impersonation was enabled for the RoomWizard resource calendars—this should be in the form domain\user not User@email.com
- Password for the Exchange account

Generate a New Configuration

To generate a new configuration if you have a license:

1. Enter your **license key**.
2. Enter the **username** and **password** for the Exchange account.
3. Click **Test Connection** to test the Exchange connection.
4. If Test Connection is successful, click **Download New Configuration** and **Save As** Site.conf file over the existing Site.conf in the bin folder of your Connector files (e.g., C:\RoomWizard\bin).
   - If Test Connection is not successful, make sure you are using an Exchange email address and it passes Microsoft's test connectivity for Exchange Web Services. (See Appendix B for testing) testconnectivity.microsoft.com
   - If Test Connection continues to fail, make sure you have an E1 or greater Exchange account (Microsoft link) or contact Microsoft to verify your account.
   - Remove the Check from Find Server URL Based on Email Address and manually enter your EWS URL
     - O365: https://outlook.office365.com/EWS/Exchange.asmx
     - On Prem: https://ServerIP/EWS/Exchange.asmx
5. Restart the connector website and reload the connector page in your browser to see that the new configuration is live.

To use the demo for up to 90 days:

1. Check **Use Demo**.
2. Follow steps 2-5 from above, as if you have a license.

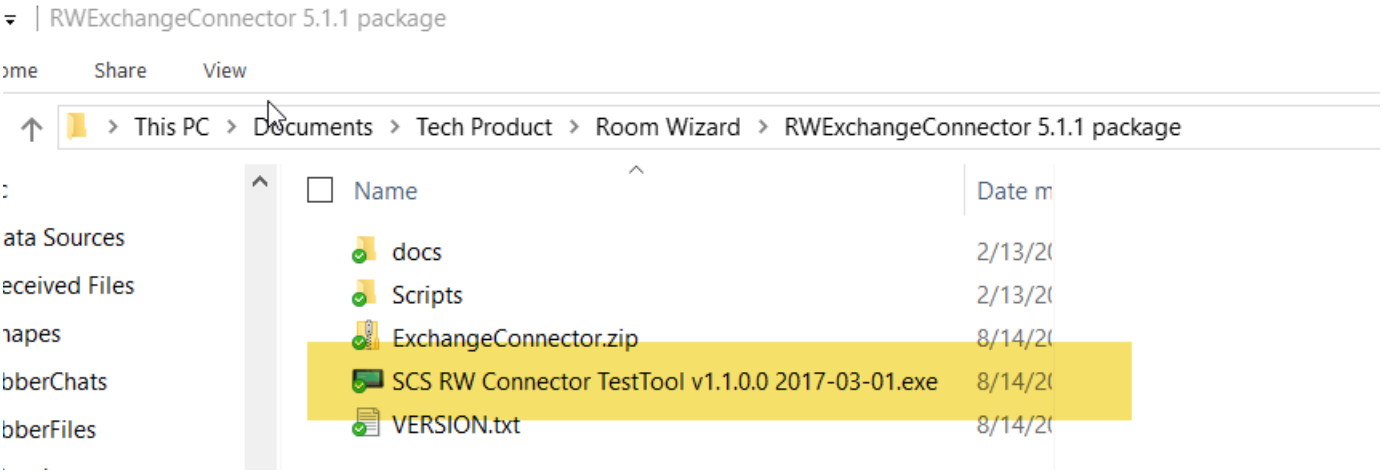
To update your configuration from a demo to a licensed version:

Open the configuration web page, then:

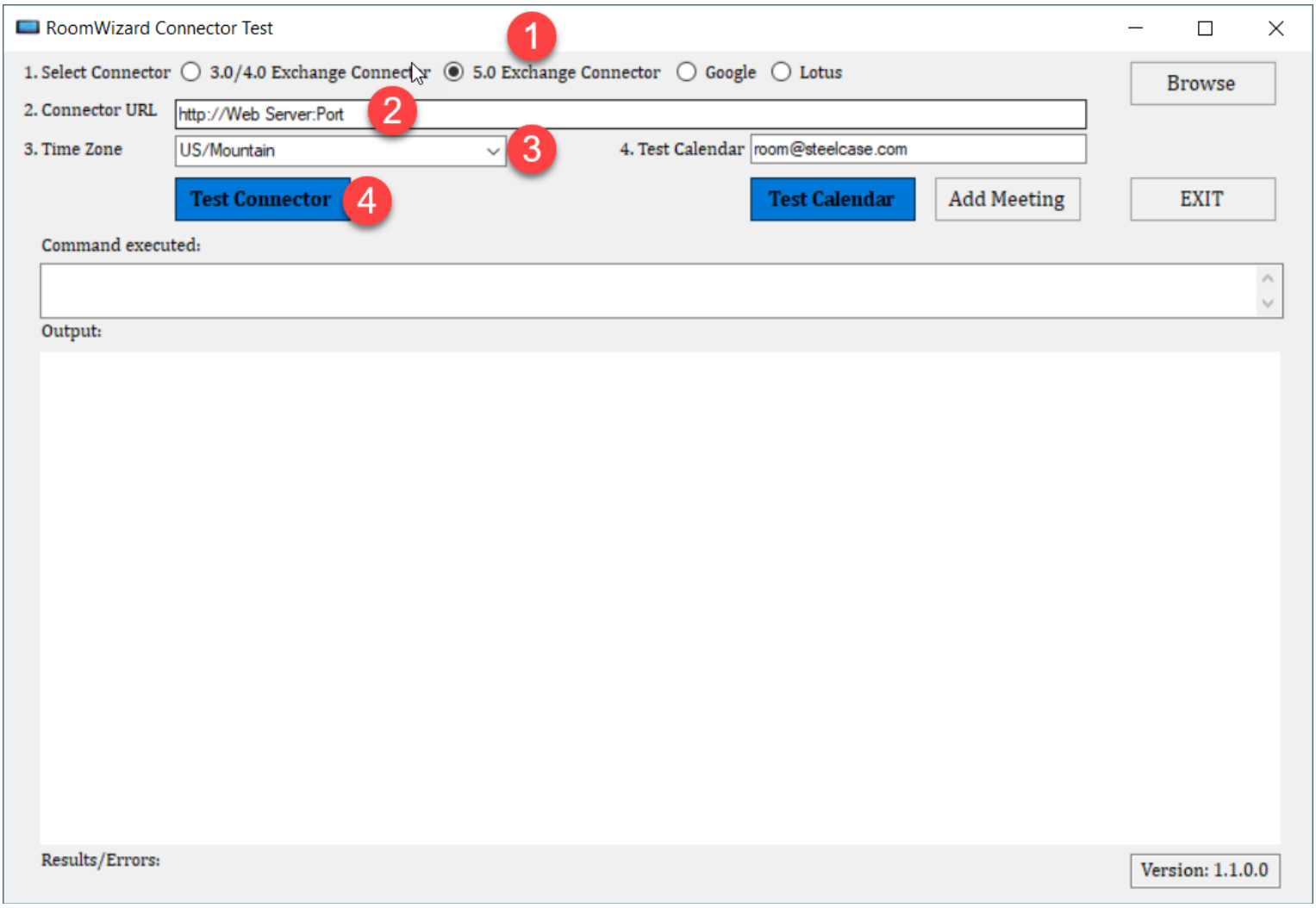
1. Enter your **license key**.
2. Uncheck the **Use Demo** checkbox.
3. Download and install the new configuration as before.
4. Restart the connector's website.

Test Connection Using Connector Test Tool

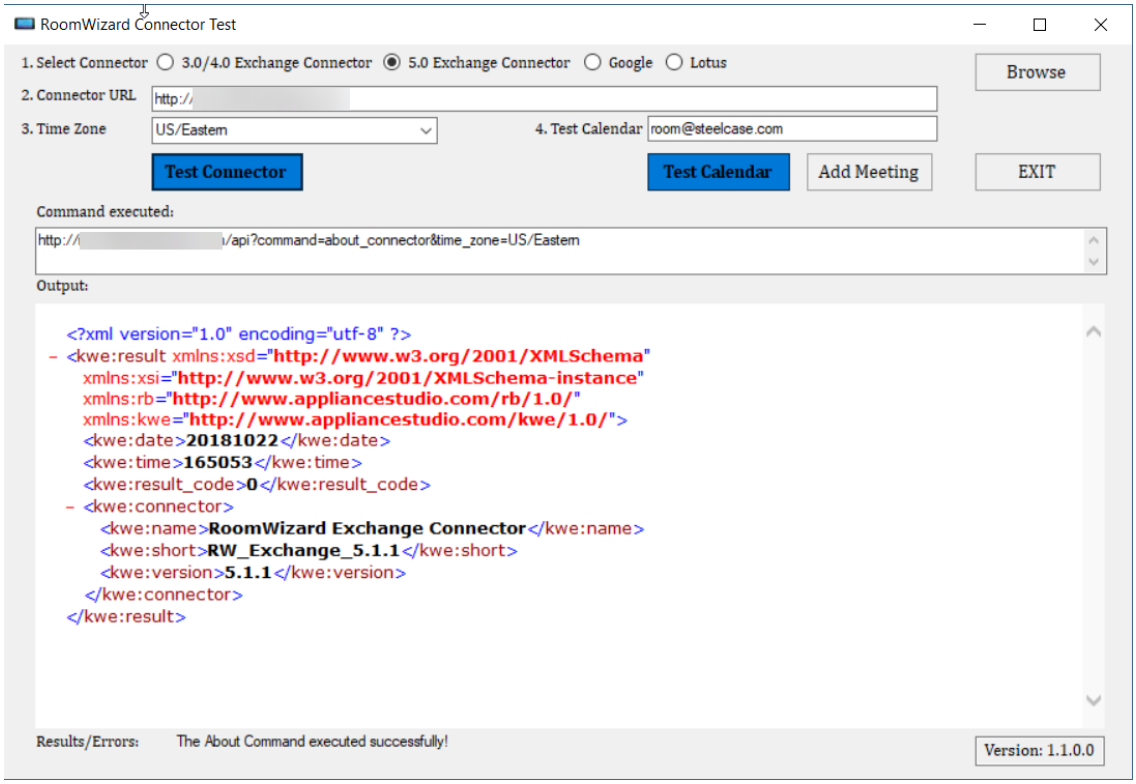
The Connector test tool is packaged with the 5.1.1 Connector.



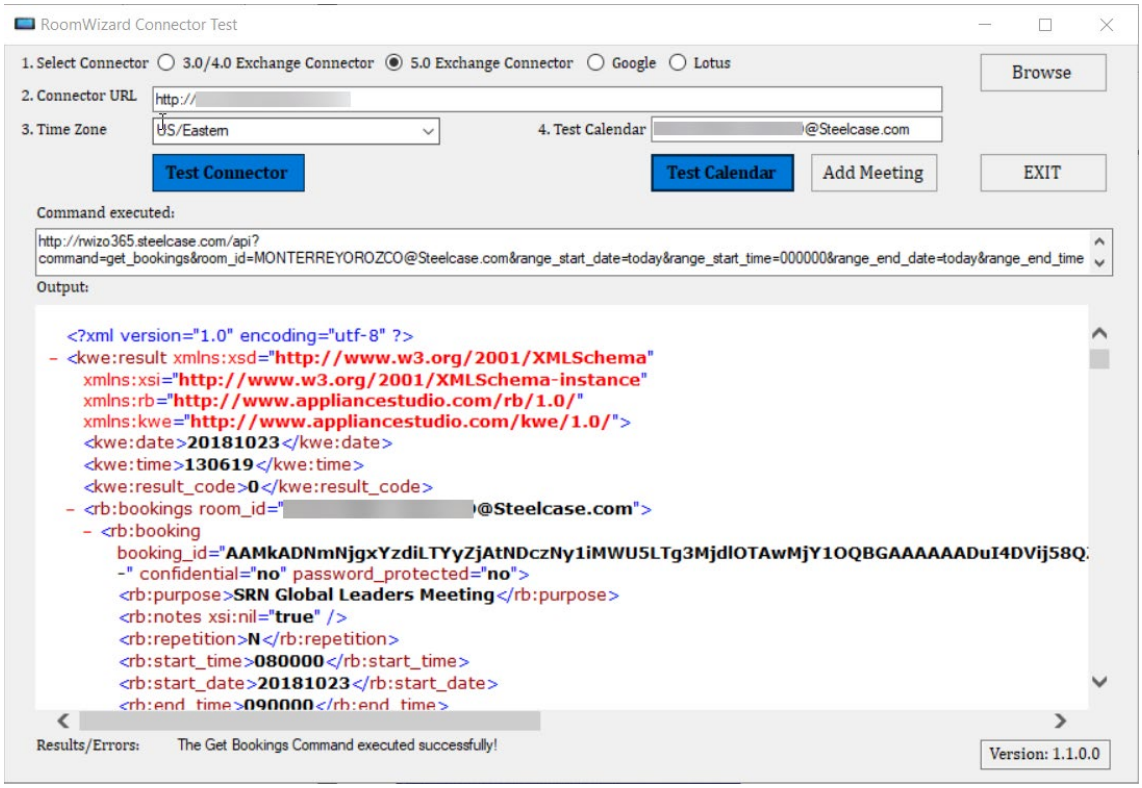
Launch the Connector Test Tool Select the Connector Type (5.0 Exchange Connector), Enter your connector URL, and Choose your Time Zone, then click Test Connector



Click Test Connector and you should see a return result like this:



Next, enter the email address of a resource calendar you plan to use for RoomWizard. ClickTest Calendar, and click ok on the pop up screen, you should see a return result like this.



This indicates that the connector is working and able to pull bookings from Exchange.

Configuring the RoomWizard

The RoomWizard is configured for synchronization in the Synchronization web page via the IP address of the device.

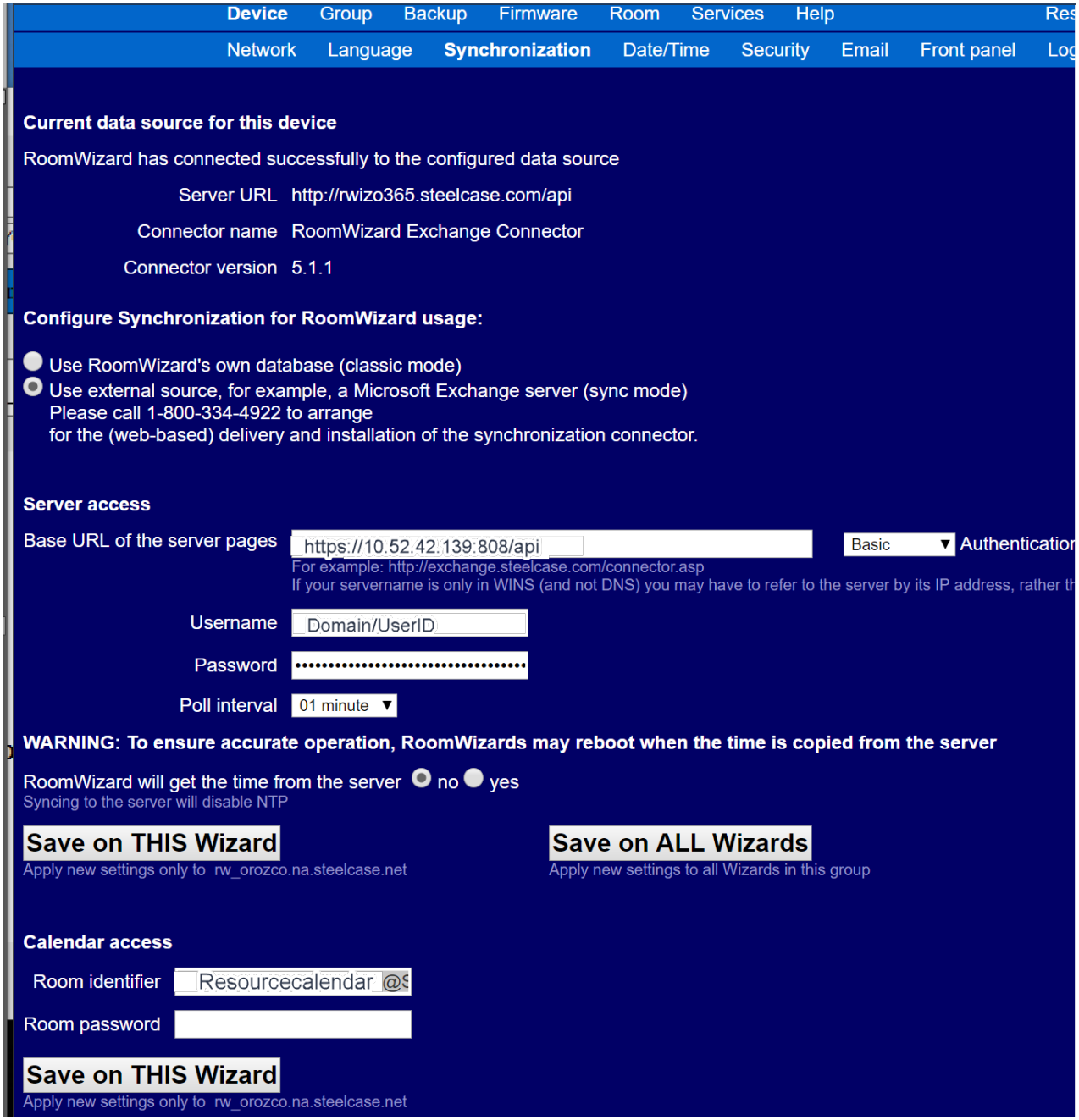
1. Find the IP address of your RoomWizard from the **About** button on the front panel of the device. Scroll down to the bottom of the main web page and select **RoomWizard setup**.

2. Log in. The default password will be either **roomwizard** or **79201** depending on when the RoomWizard was purchased. Your organization may have changed the password, so be sure to check with your system administrator for an updated password.
3. Select **Synchronization**.

4. The RoomWizard should be set to Synchronized mode by selecting the radio button **Use external source**.

The URL for the connector will be something like: http://your web server:8080/api.

1. “Your web server” is the server you installed the connector on and “8080” is the port number you used for your website. Please use the local domain service account you created according to the Connector prerequisites on page 2 for username and password.
2. Click the first **Save on THIS Wizard** button to make the connection to your Connector.
3. In the Room identifier field, enter the **name of the mailbox** exactly as it is configured in Exchange (e.g., ConferenceRoom@company.com). Click the second **Save on THIS Wizard** button to make the Connection to your Exchange Calendar.

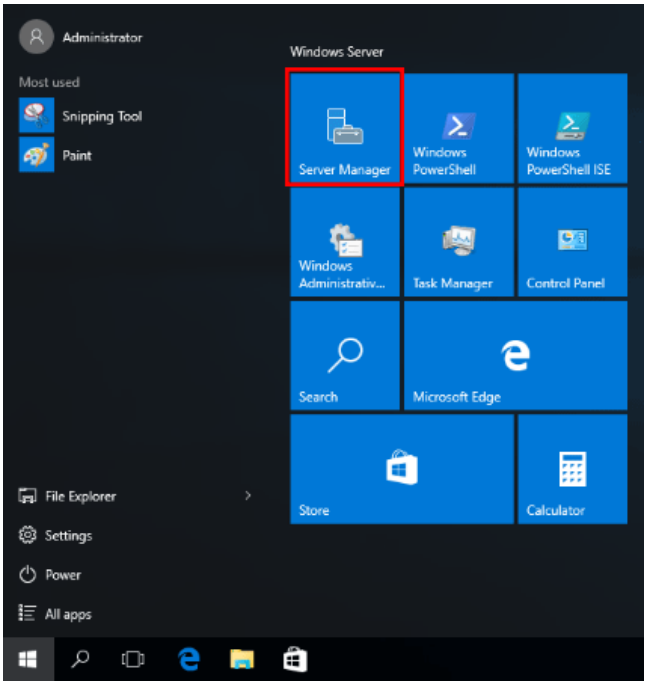


Appendix A (IIS)

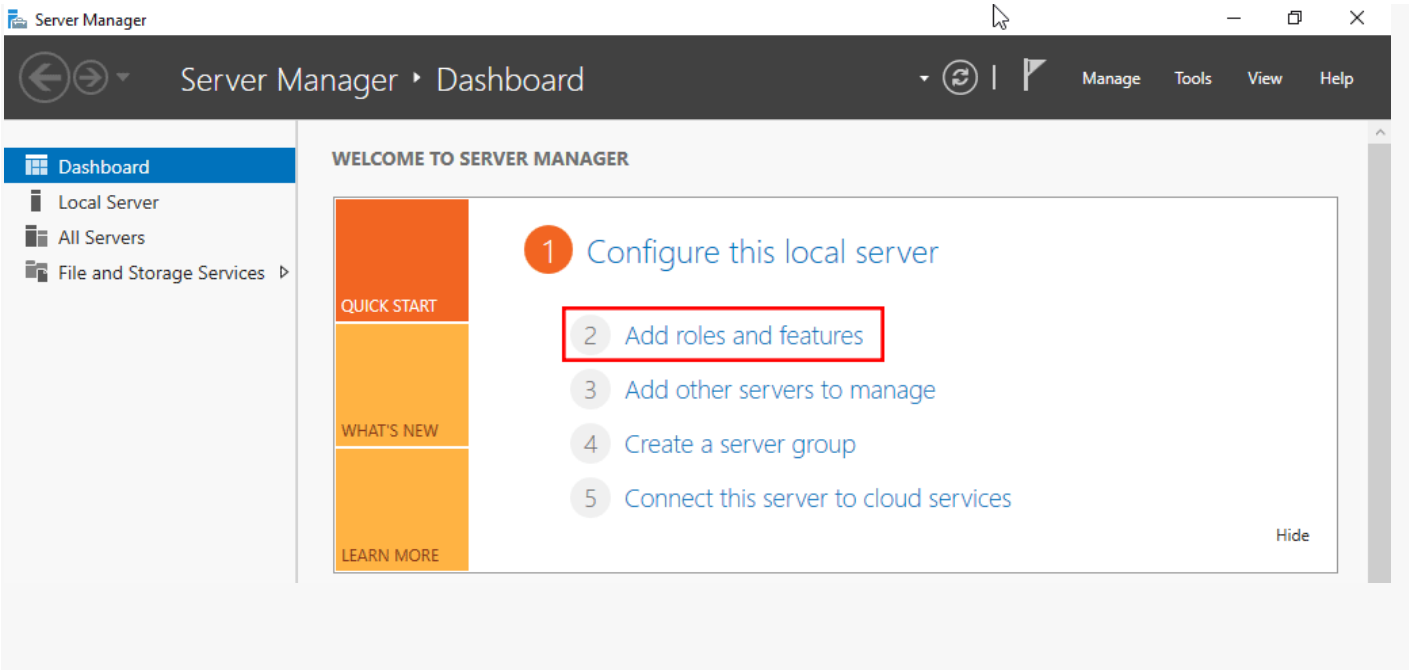
This section walks through the process of setting up the environment to run the Exchange Connector. This section will cover installing the appropriate software installed as listed in the System Requirements section. Instructions may vary based on Server OS

Installing the IIS Role and additional Features (Server 2016)

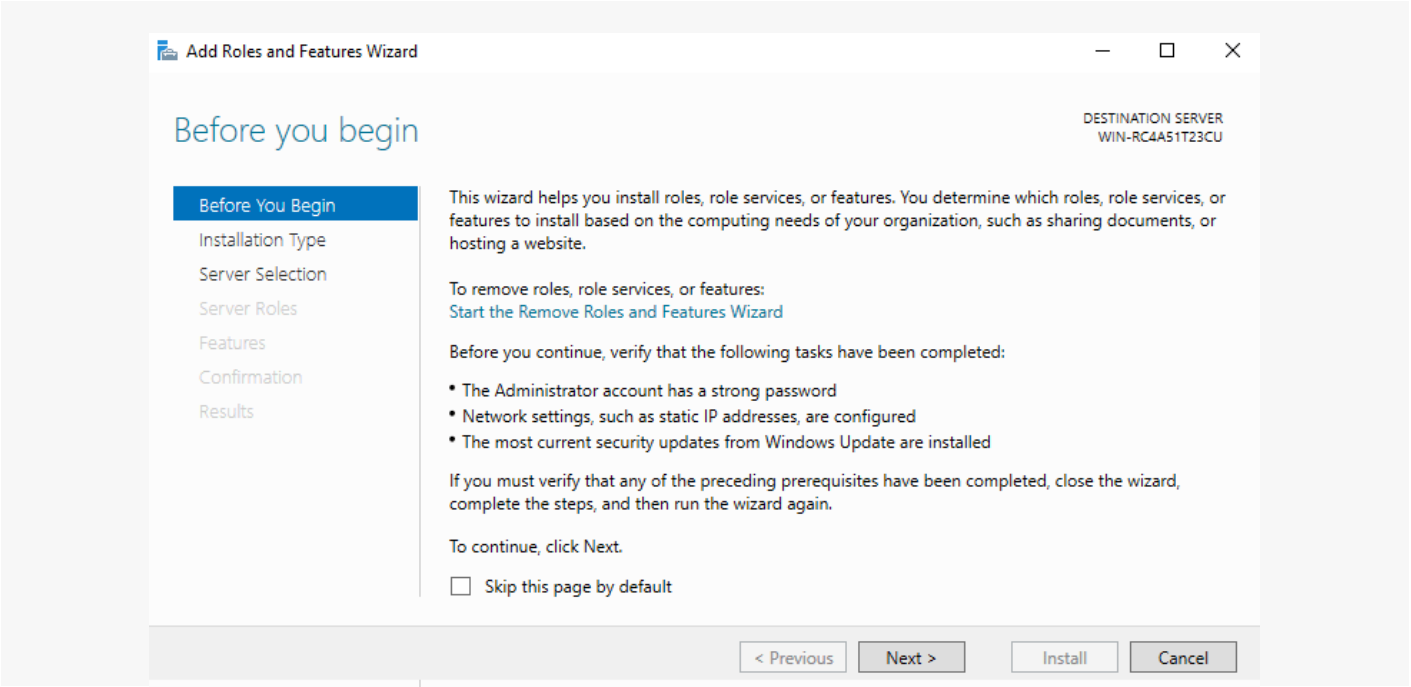
Open Server Manager, this can be found in the start menu. If it's not there simply type "Server Manager" with the start menu open and it should be found in the search.



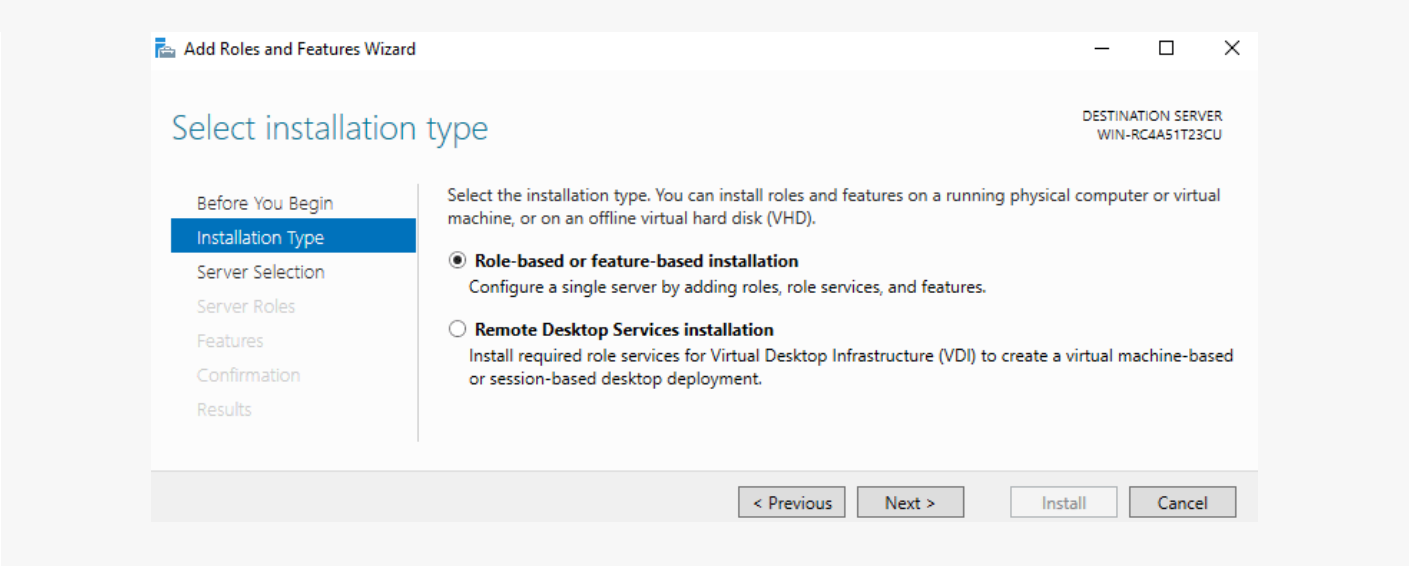
Click the "Add roles and features" text.



On the "Before you begin" window, simply click the Next button.

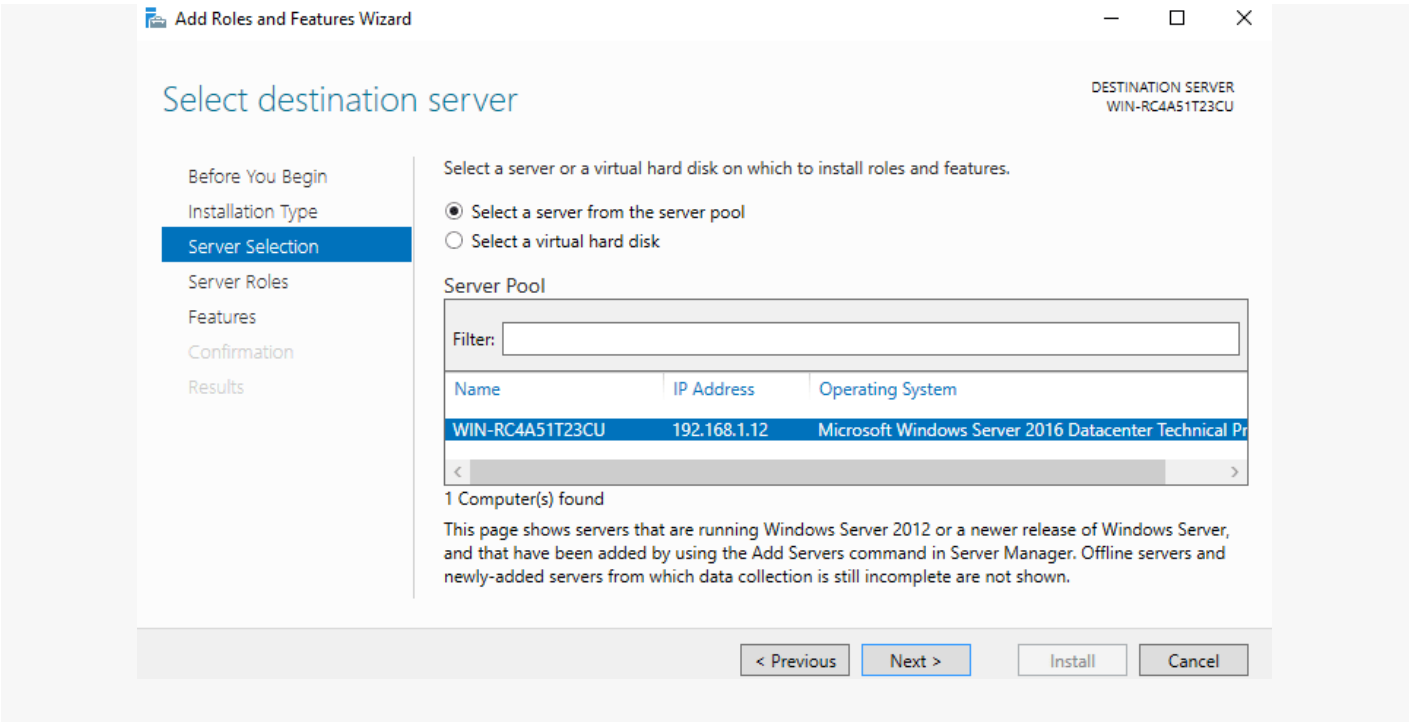


On the “Select installation type” window, leave “Role-based or feature-based installation” selected and click Next.

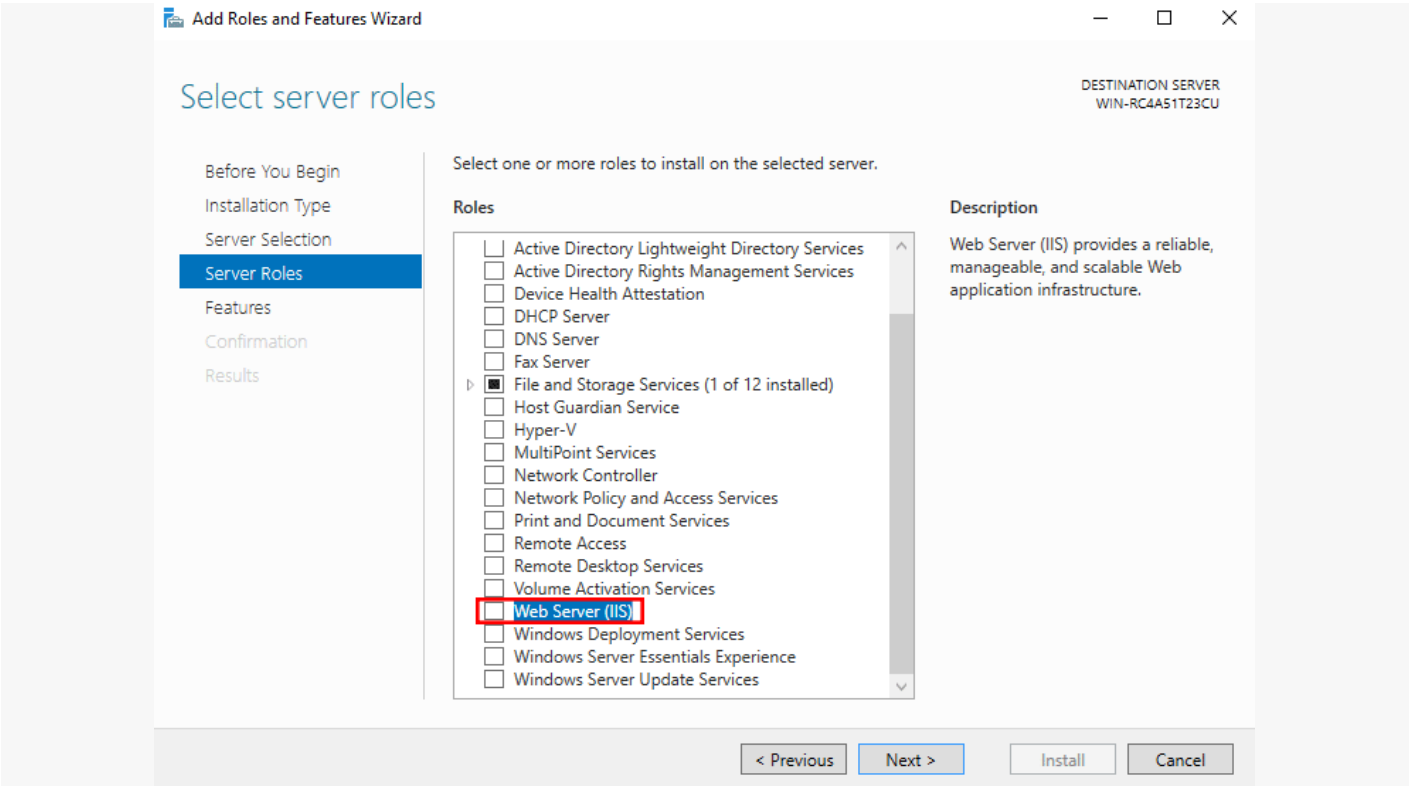


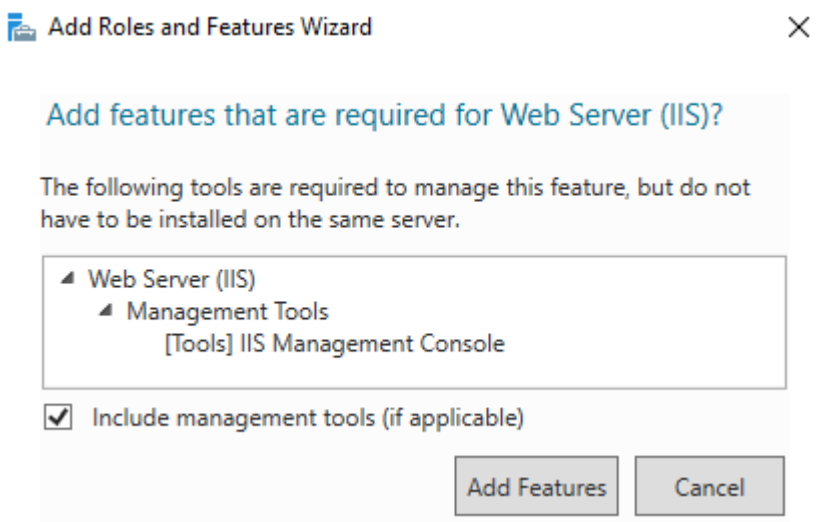
As we’re installing to our local machine, leave “Select a server from the server pool” with the current machine selected and click Next.

Alternatively, you can select another server that you are managing from here, or a VHD.

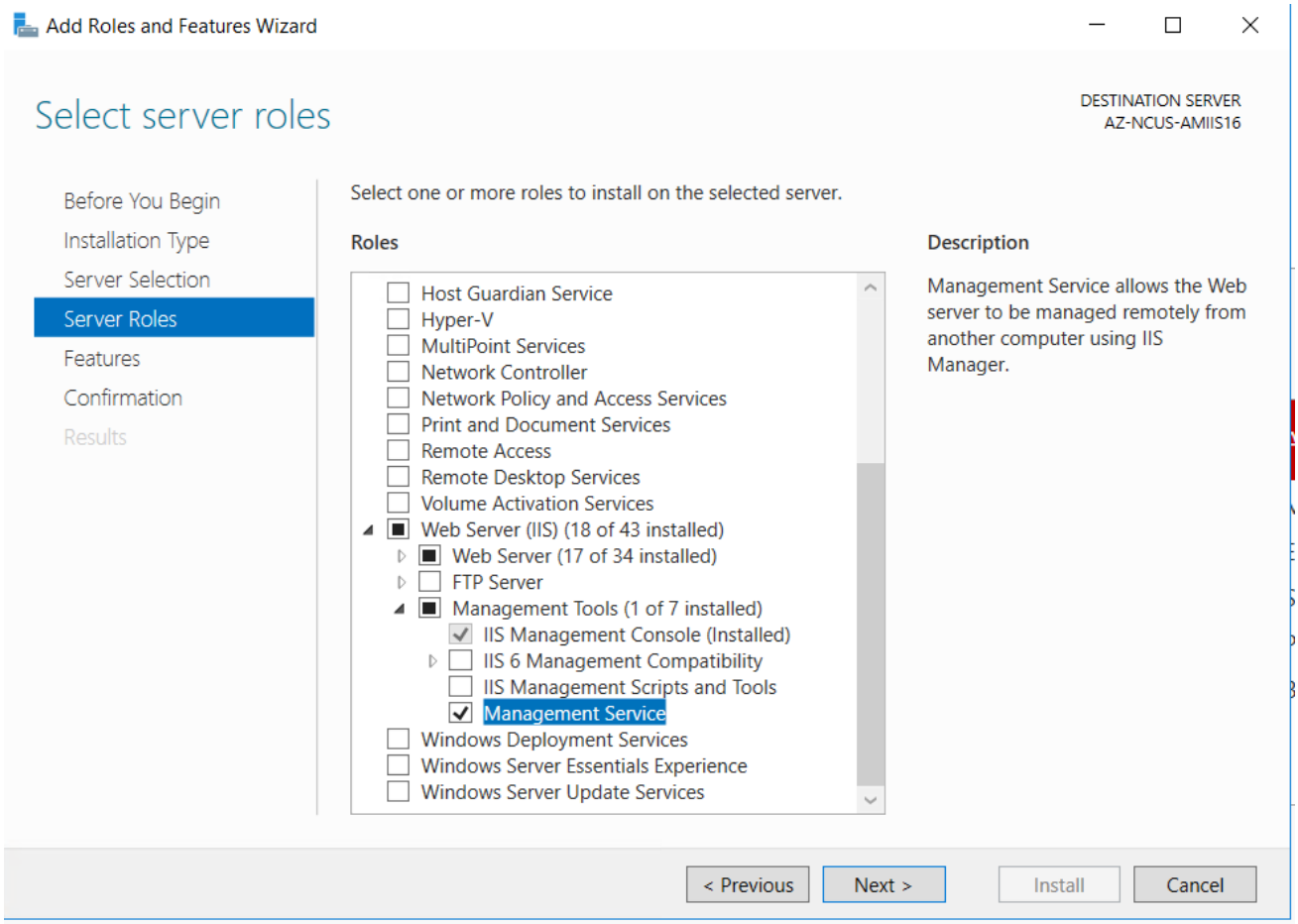


From the “Select server roles” window, check the box next to “Web Server (IIS)”. Doing this may open a new window advising that additional features are required, simply click the “Add Features” button to install these as well. Click Next back on the Select server roles menu once this is complete.

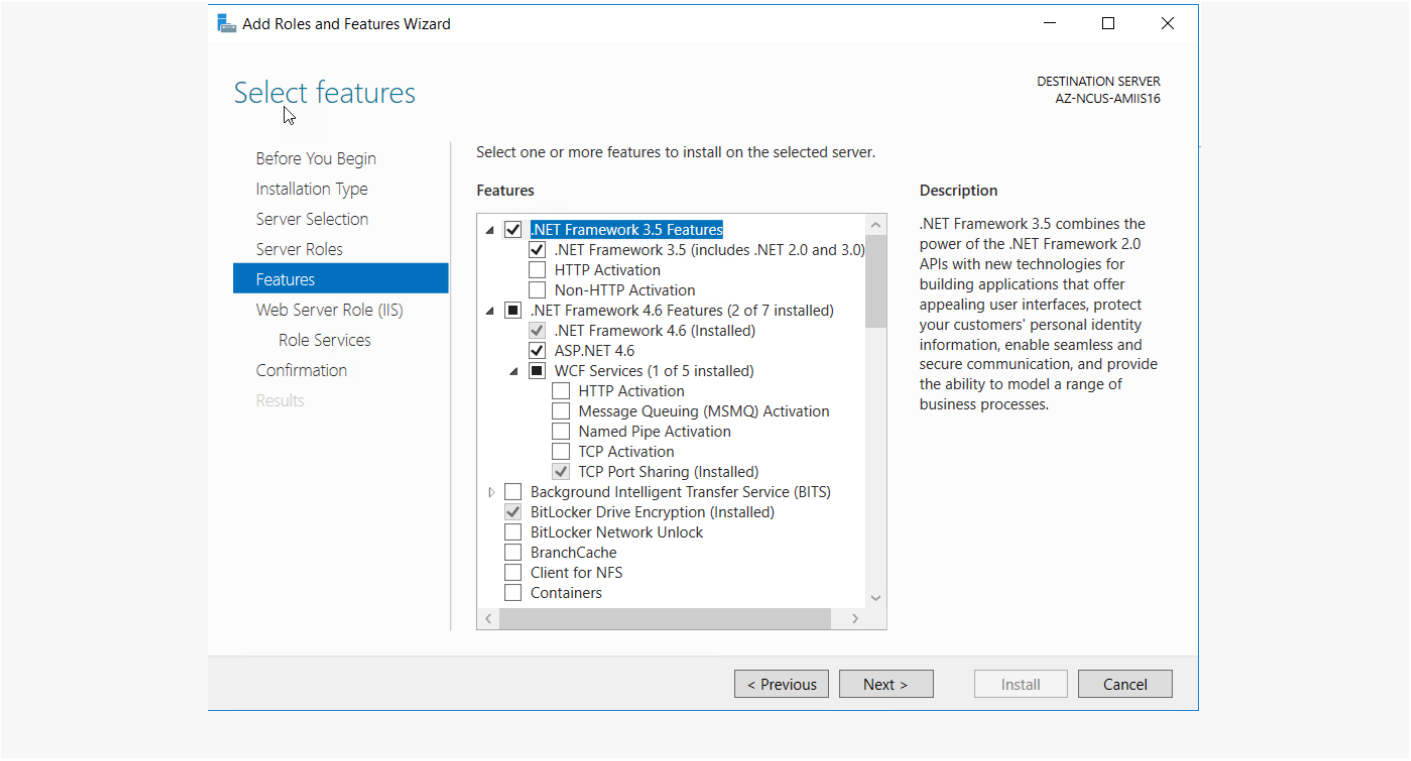




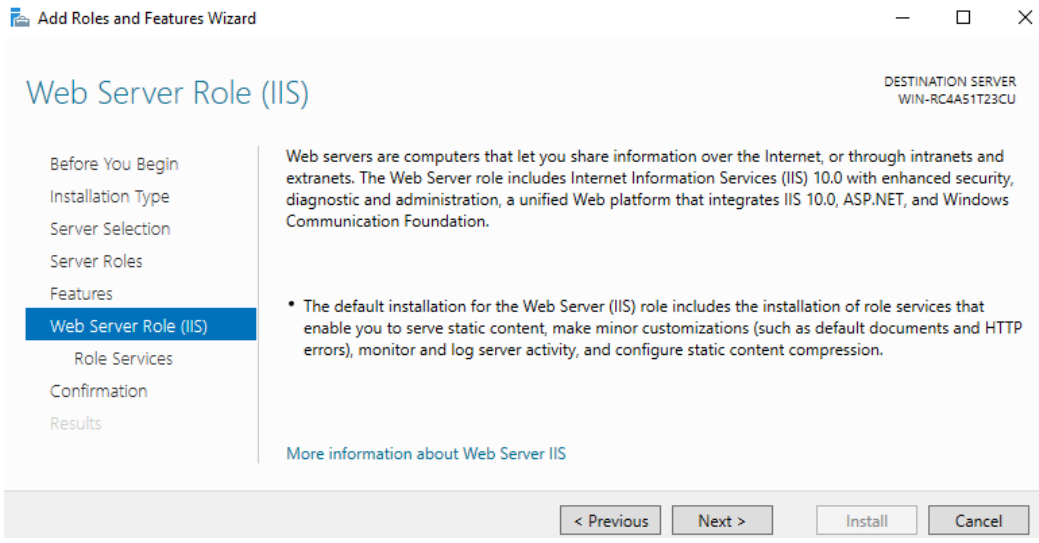
Expand Web Server and choose Management Tools Management Services



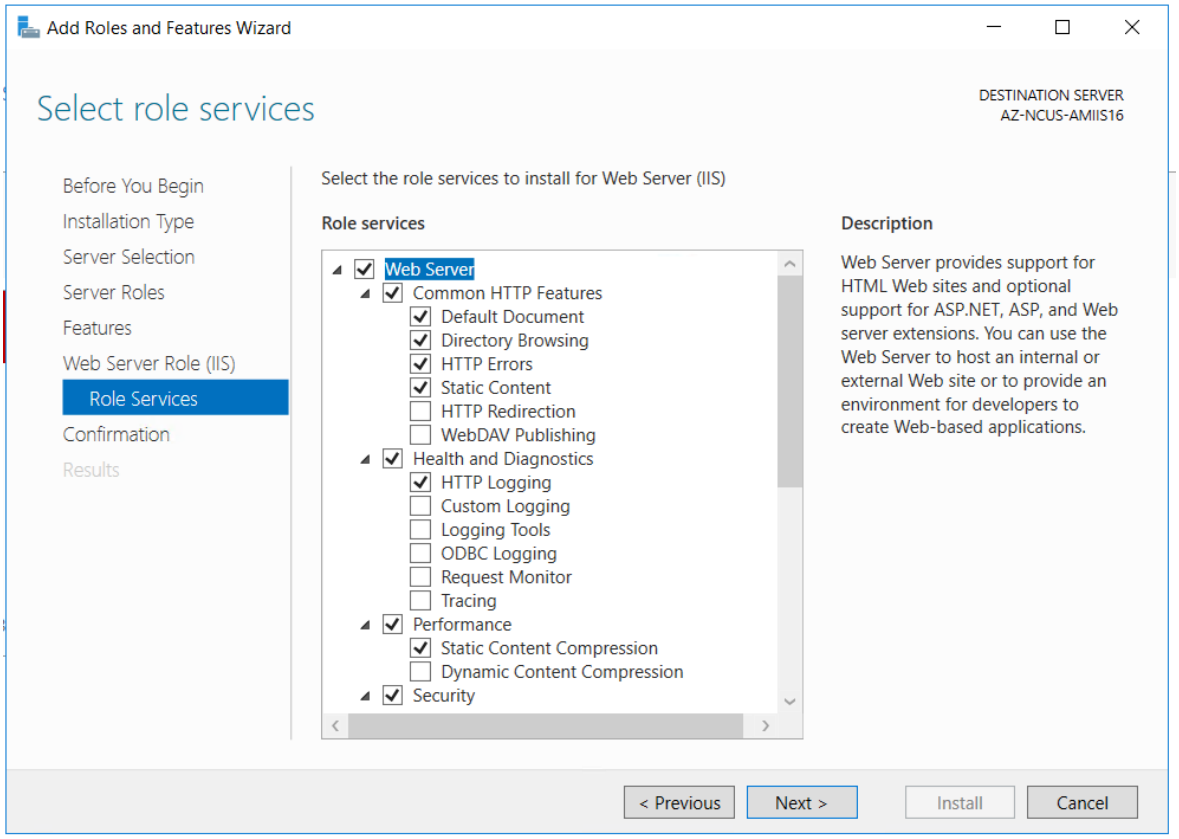
We will be installing additional features at this stage.

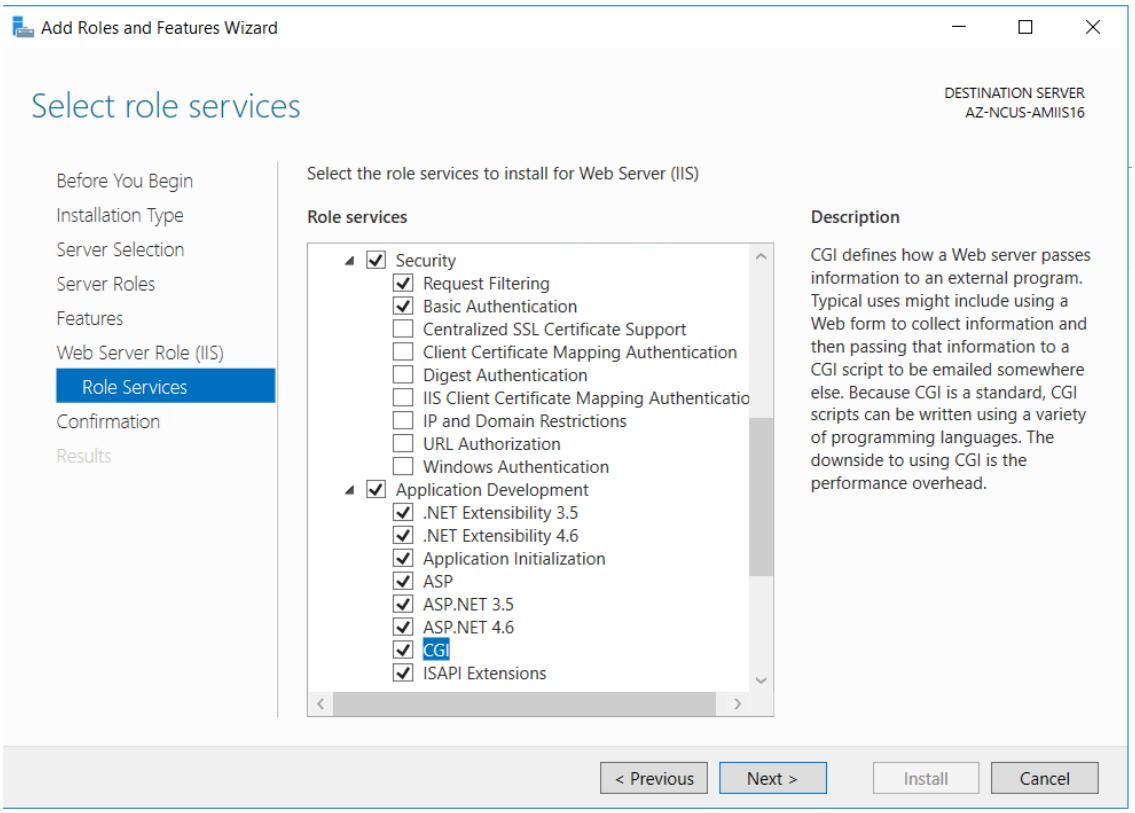


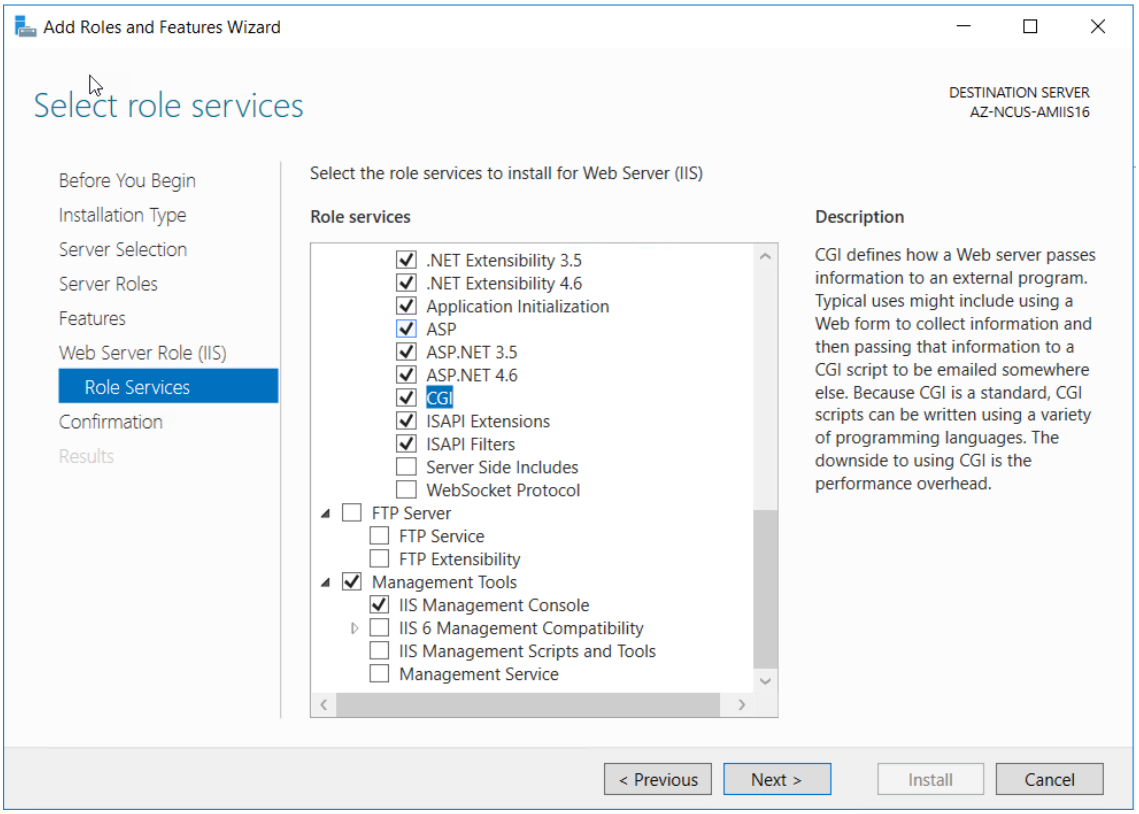
Click Next on the “Web Server Role (IIS)” window after reading the information provided.



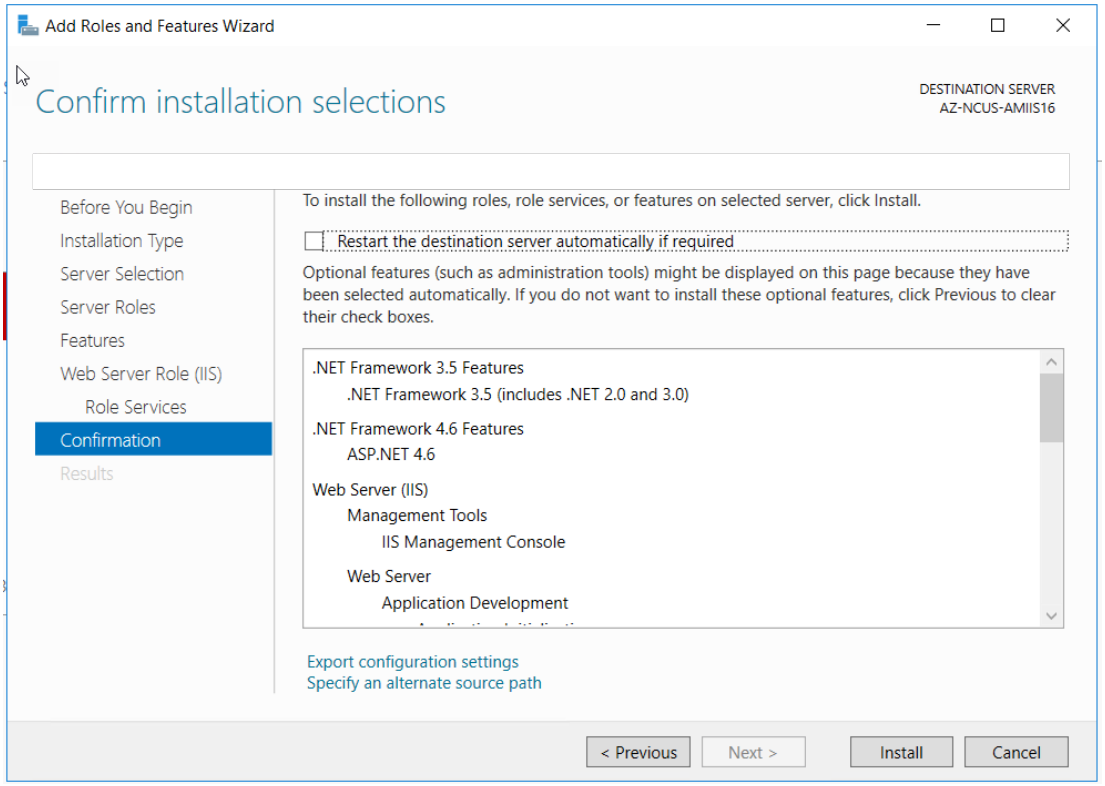
At this point on the “Select role services” window you can install the additional required services for IIS.





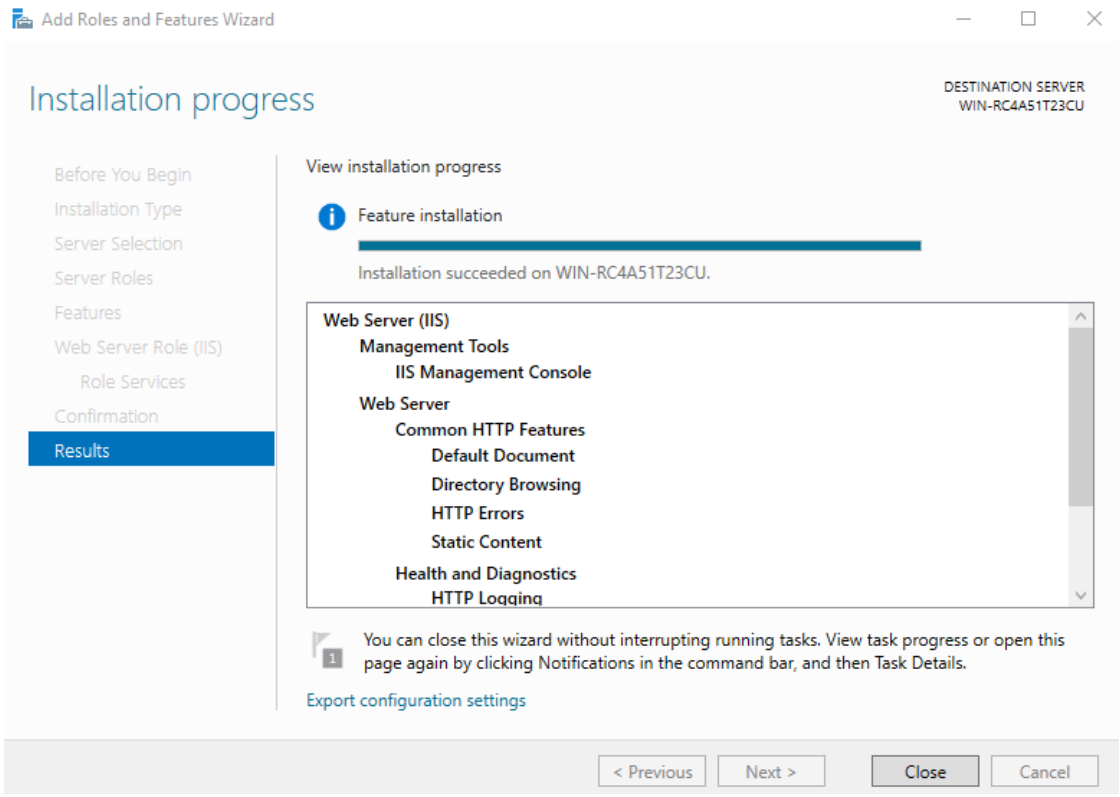


Finally, on the “Confirm installation selections” window, review the items that are to be installed and click Install when you’re ready to proceed with installing the IIS web server.



No reboot should be required with a standard IIS installation, however if you remove the role a reboot will be needed.

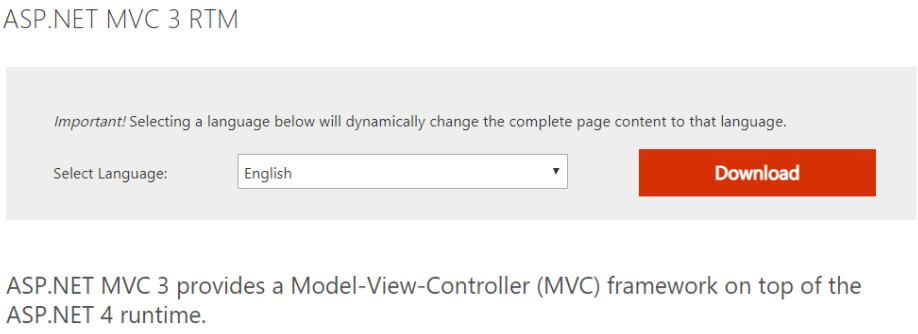
Once the installation has succeeded, click the close button. At this point IIS should be running on port 80 by default with the firewall rule "World Wide Web Services (HTTP Traffic-In)" enabled in Windows firewall automatically.



Appendix B (Installing and Configuring ASP.NET MVC3 and Web Deploy 3.6)

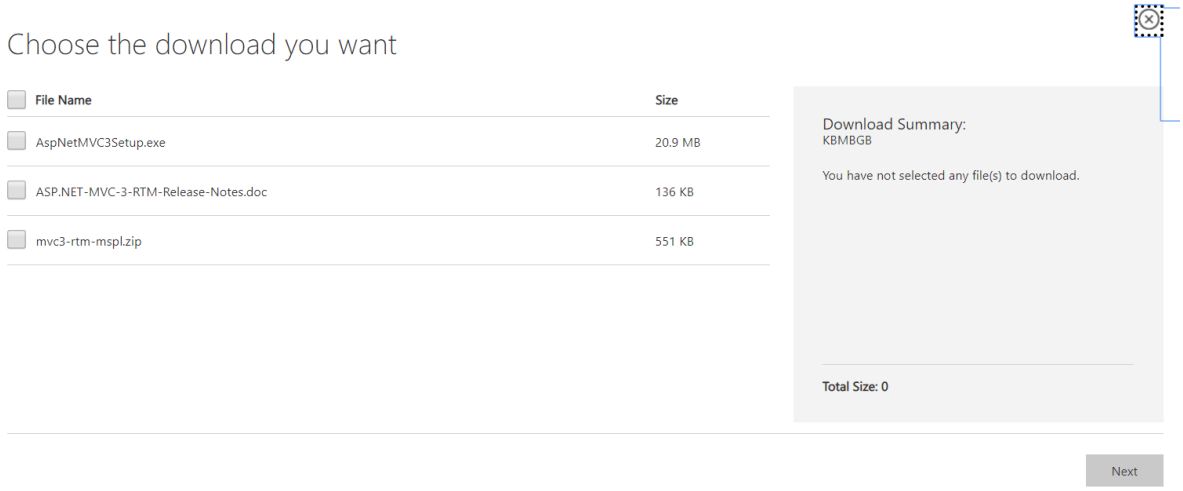
This will walk you through installing and configuring WebDeploy and ASP.NET MVC3

Install ASP.NET MVC 3
Browse to https://www.microsoft.com/en-us/download/details.aspx?id=4211, select your language and click download

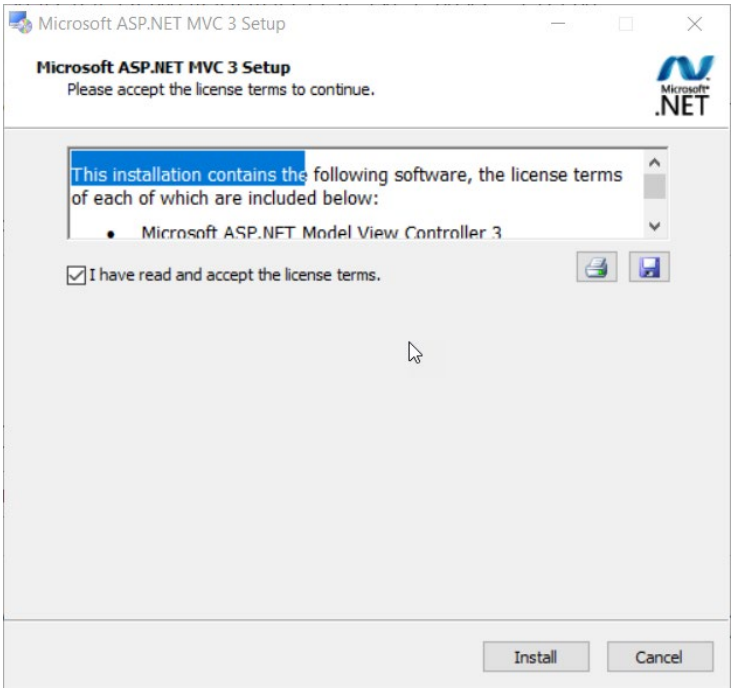


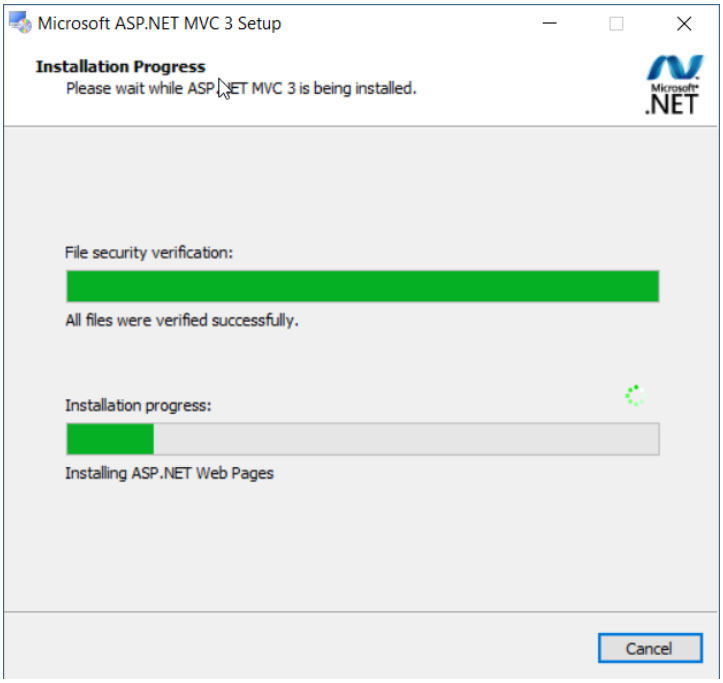
Choose the AspNetMVC3Se

tup.exe and click Next

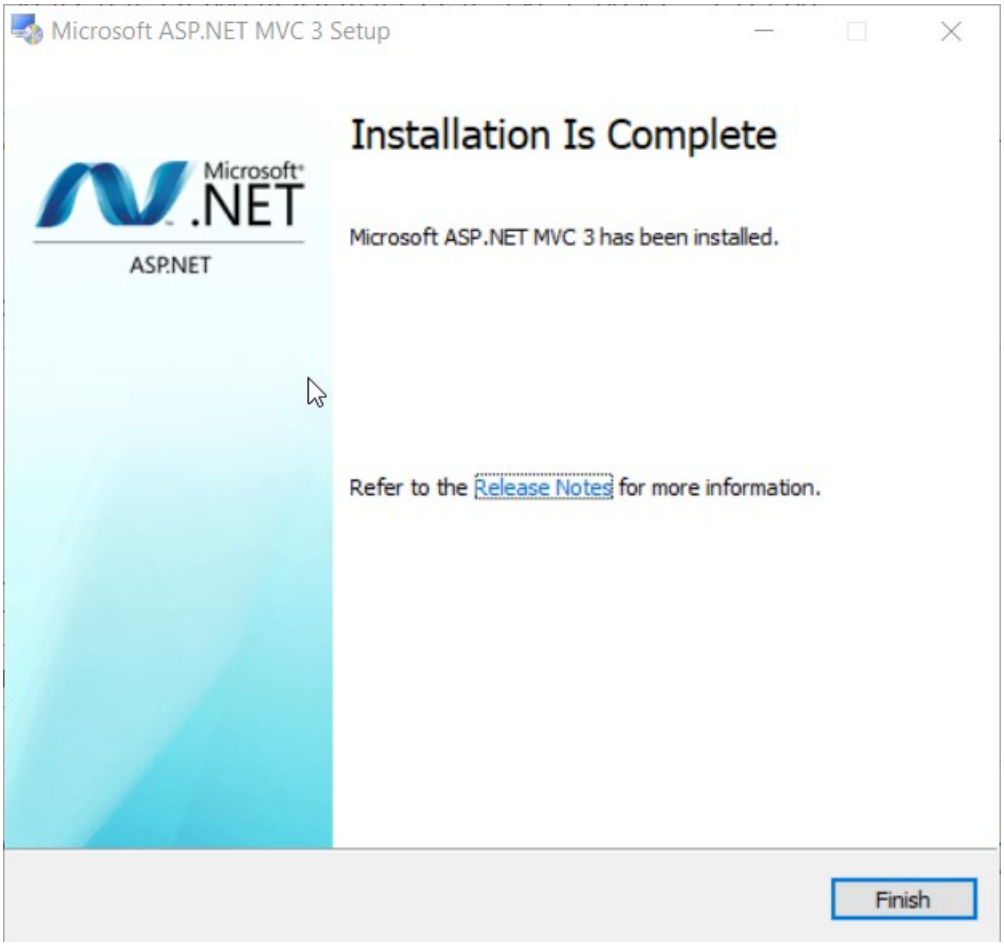


Double click on downloaded file, Accept the License Terms, and click Install



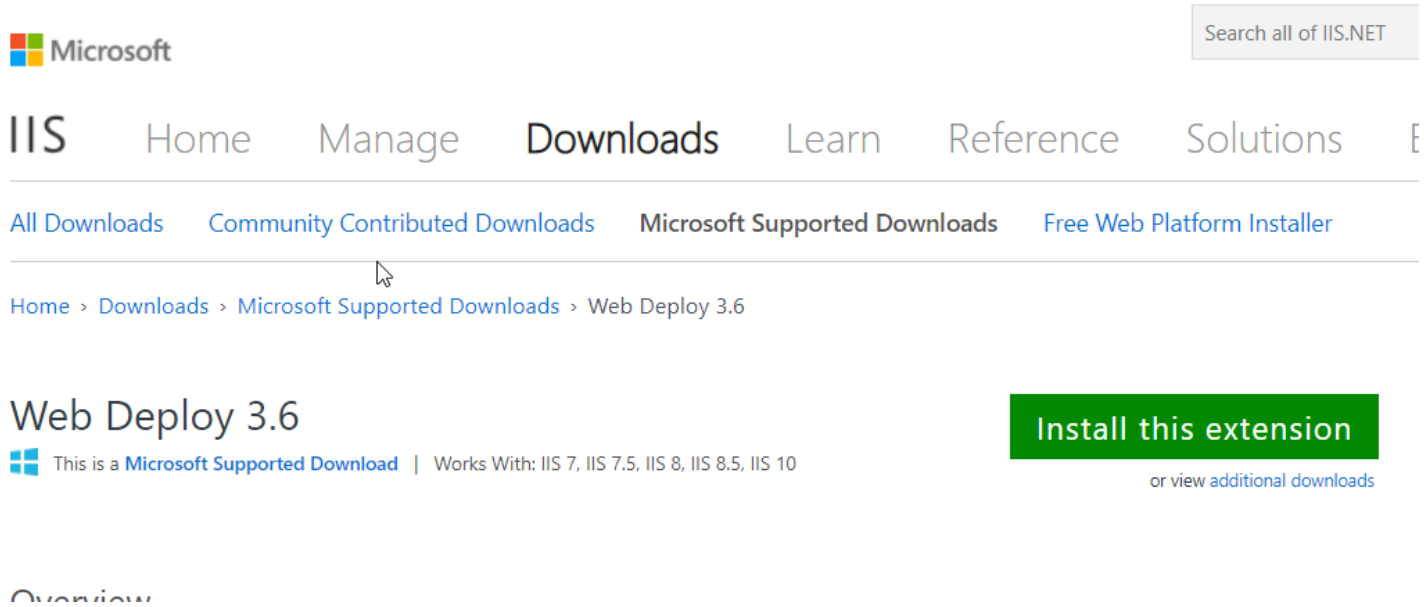


Click Finish

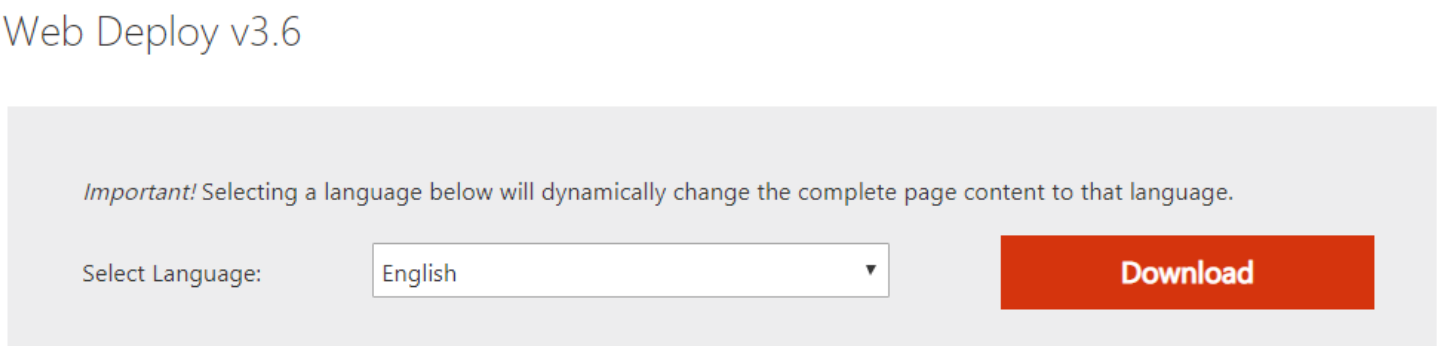


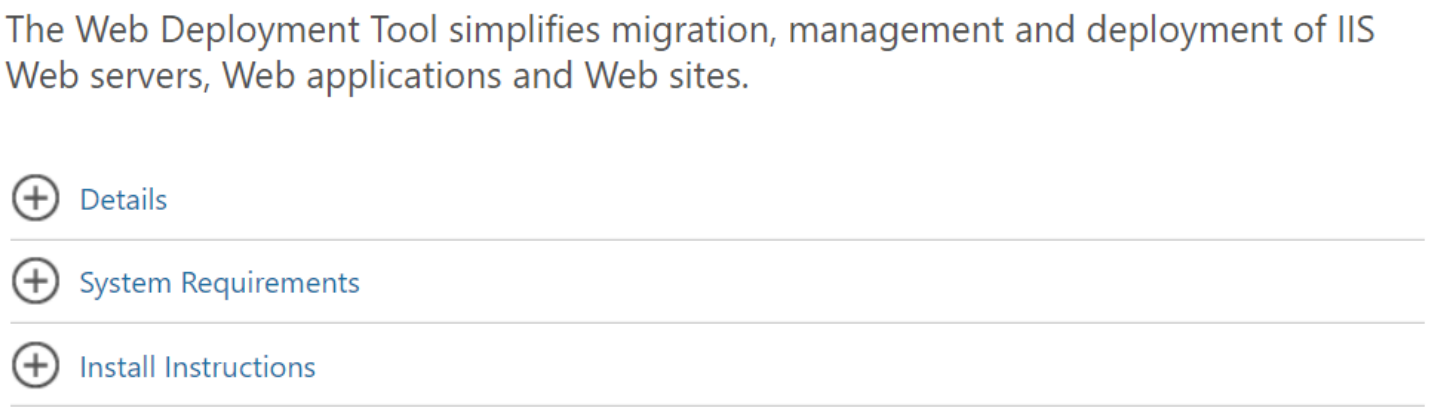
Installing and Configuring Web Deploy 3.6

Browse to https://www.iis.net/downloads/microsoft/web-deploy and click Install this Extension

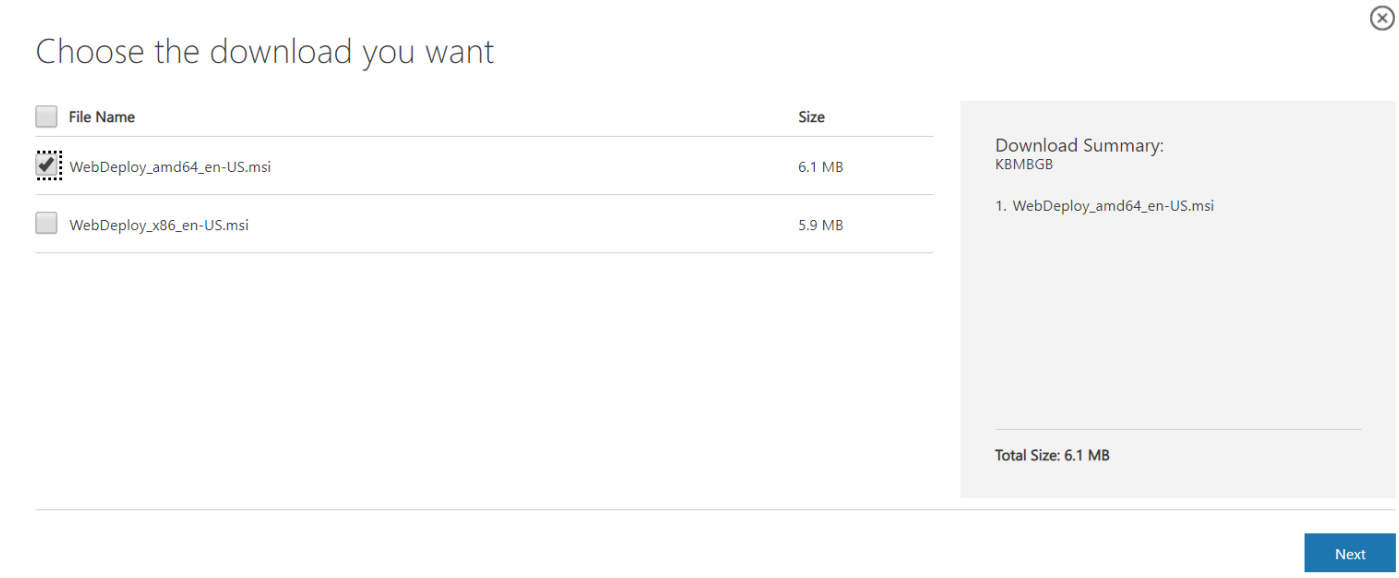


Choose your Language and click Download

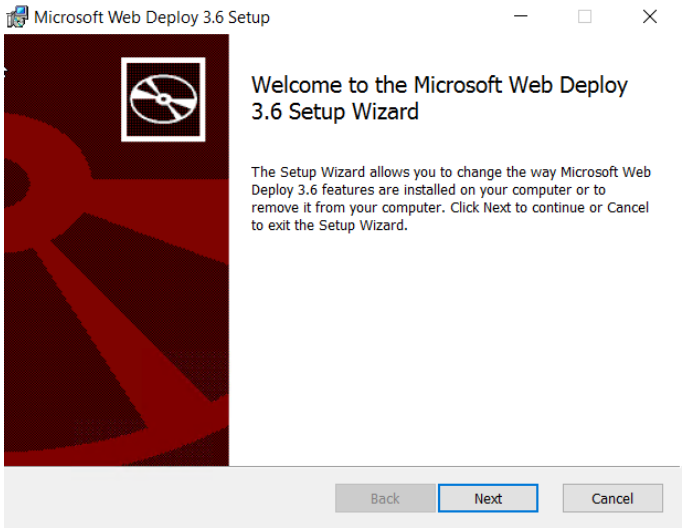


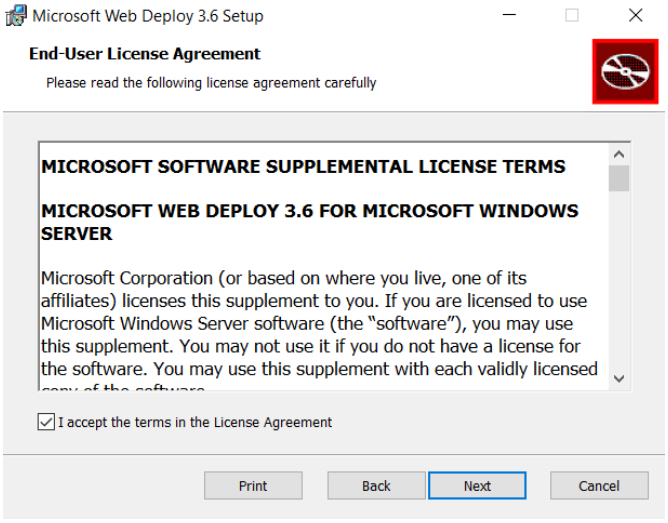


Choose the operating system that is accurate for your environment and click next

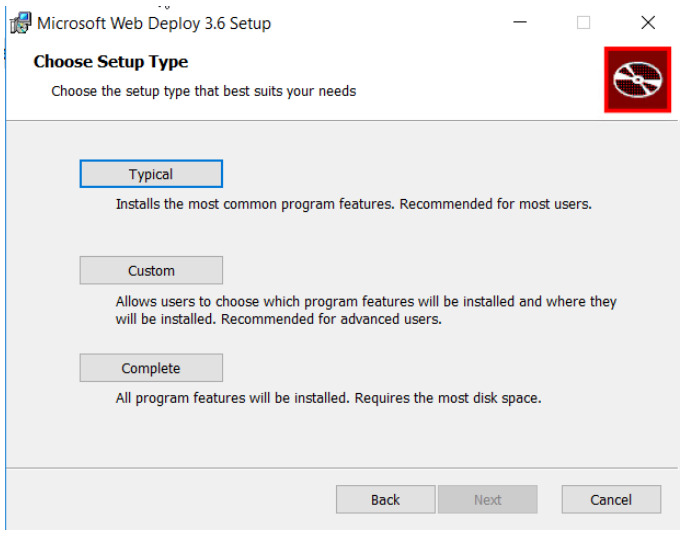


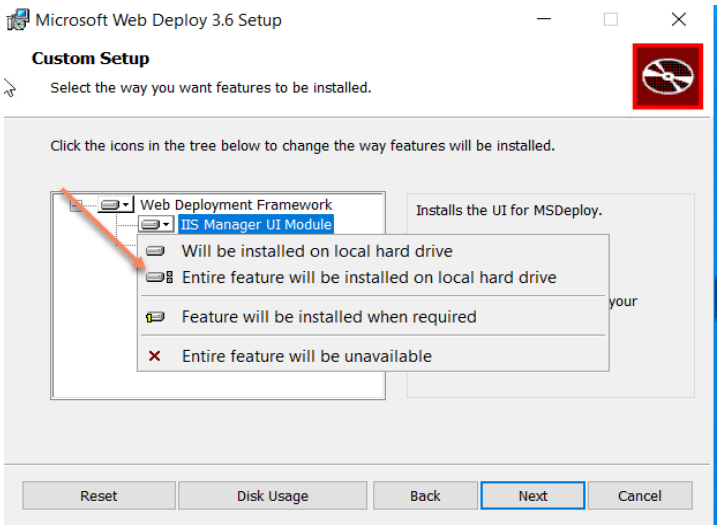
Click on the Downloaded File | Next | and accept the Terms in the License Agreement | Next

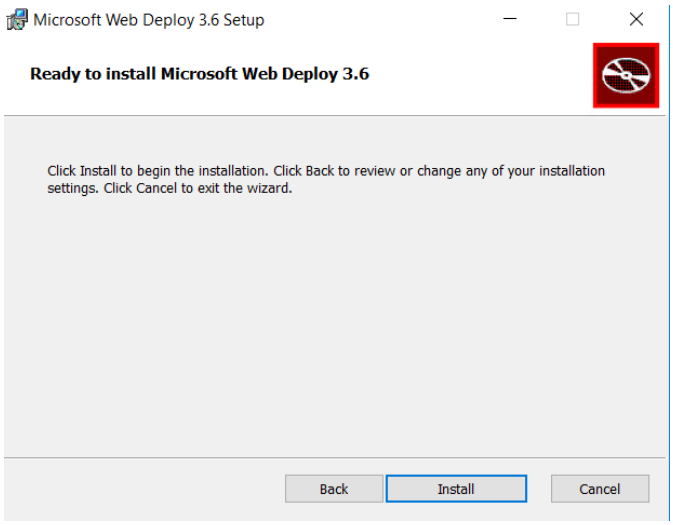




Select Custom and click Install

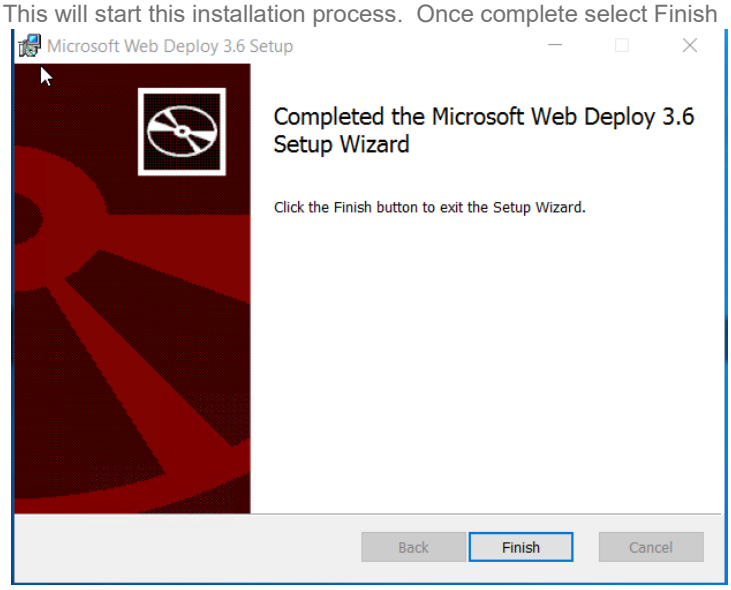




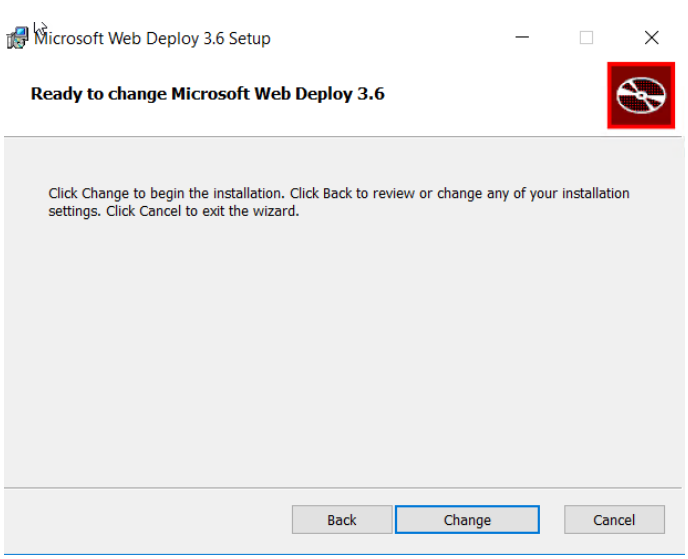


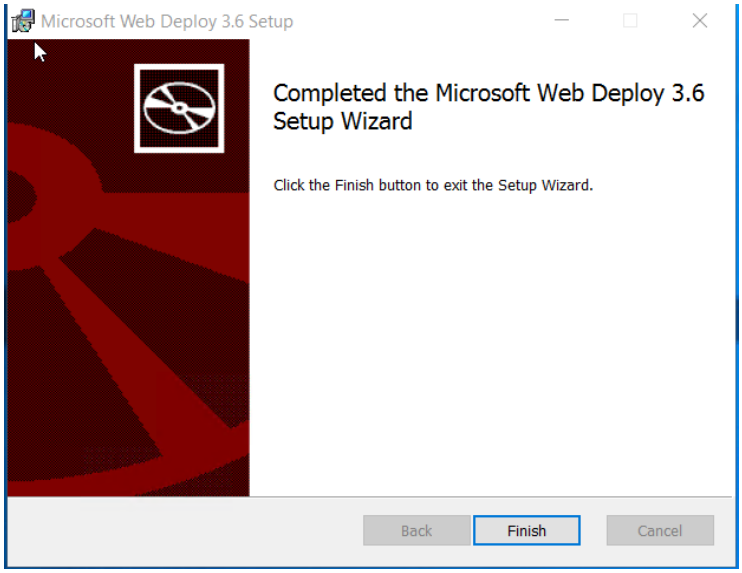
Once the setup has completed we will need to add additional features to Web Deploy, go to App & Features and choose modify on Microsoft Web Deploy 3.6

This will start this installation process. Once complete select Finish



Click Change and Finish





We should not be able to import and export applications using the IIS Manager

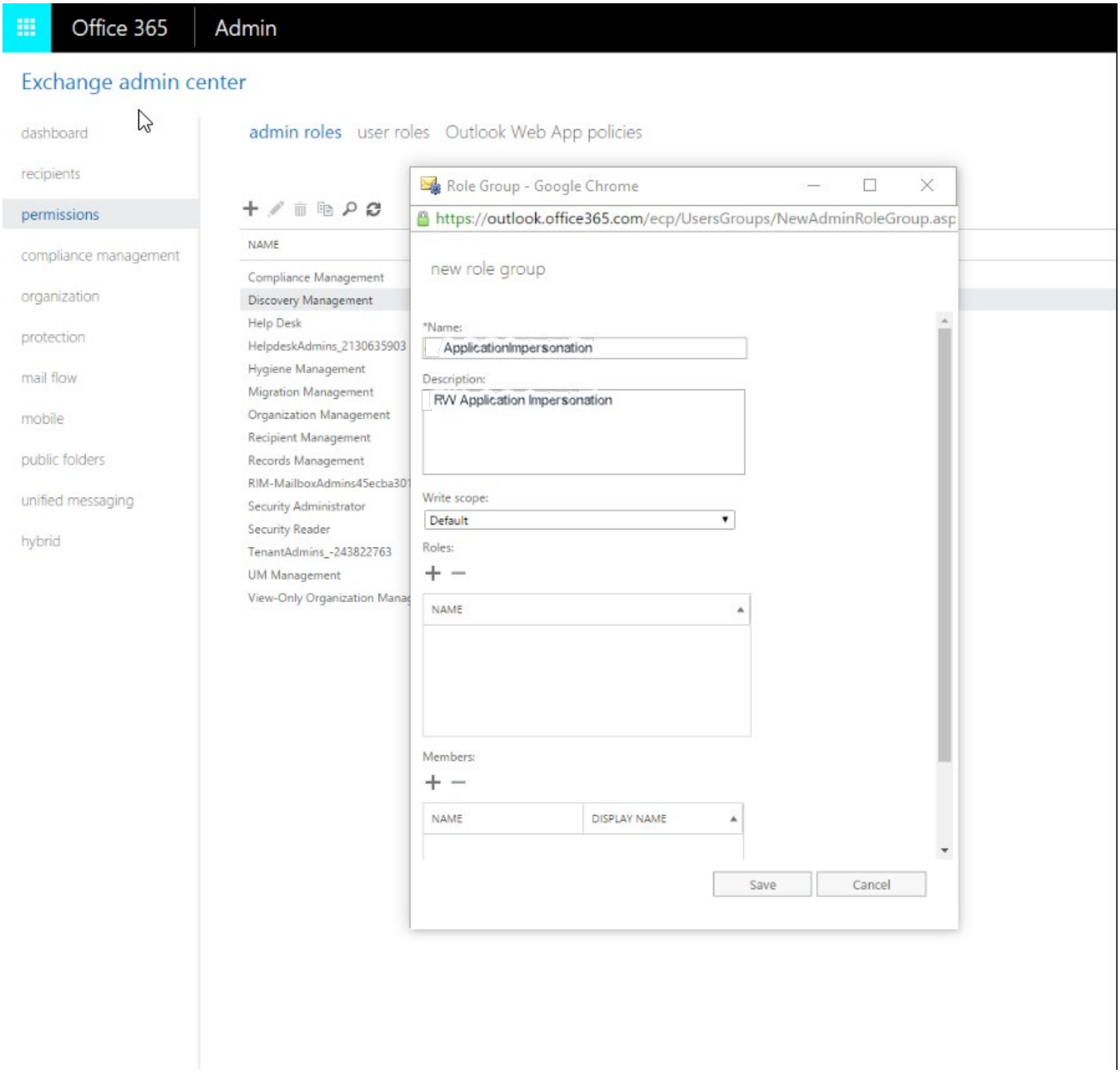
Appendix C (Application Impersonation)

The Exchange Connector requires Application Impersonation to access to the room mailboxes managed by the RoomWizard devices.

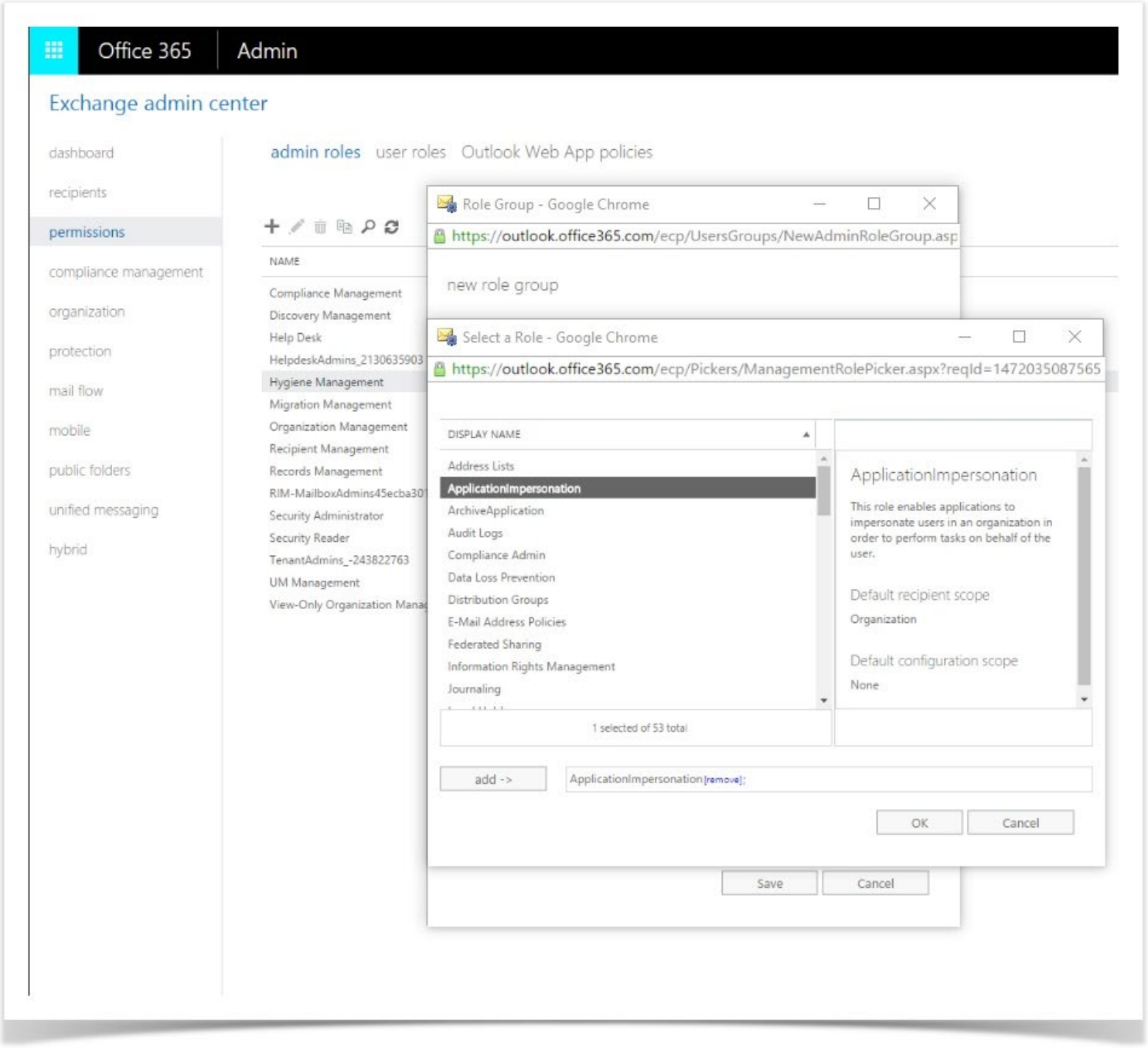
Configuring Application Impersonation Via EAC

Login to the Office 365 Exchange Admin Portal.

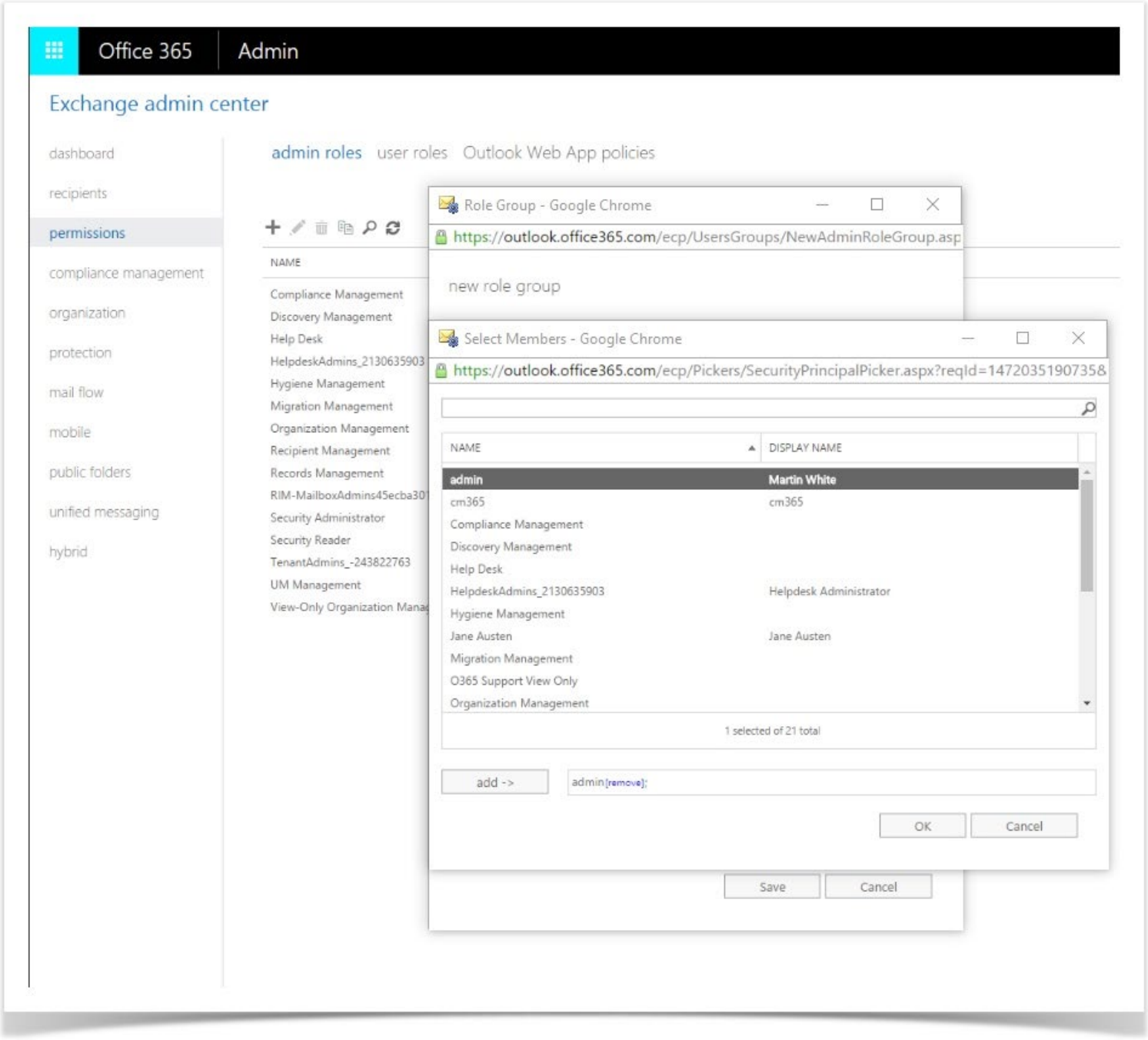
Go to Permissions, then under Admin Roles click the '+' symbol to add a new role and enter the Name and Description 'ApplicationImpersonation'.



Click the '+' symbol under 'Roles:', select ApplicationImpersonation, click 'add →' then 'OK'



Click the '+' symbol under 'Members:' and select your RoomWizard Service Account, click 'add →' then 'OK'



Click 'Save' in the 'Role Group' window and you will then see the Impersonation role listed in Admin Roles. You can now use application impersonation with your Service Account user in RoomWizard.

Testing Microsoft Office 365 Auto Discovery

1. To test Auto Discovery for an Office 365 account, navigate to: testconnectivity.microsoft.com.
2. On the Exchange Server tab, under Microsoft Exchange Web Services Connectivity Tests, select the radio button next to **Synchronization, Notification, Availability, and Automatic Replies** then click **Next** in the upper right corner.

Appendix D (PowerShell Commands)

Establishing Remote Session with Outlook

In order to configure mailbox access permissions, you will need to establish a remote PowerShell session using your Exchange account. This section assumes you have a working knowledge of PowerShell.

Note: You will need to run PowerShell as an Administrator.

The following commands will establish a remote session with Outlook :

1. Enter your Outlook credentials: $credentials = Get-Credential.
2. Establish a remote session: $session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://ps.outlook.com/powershell -Credential $credentials -Authentication Basic -AllowRedirection.
3. Depending on your security policy, you may need to execute this command in order to import the session (including the commands): Set-ExecutionPolicy -ExecutionPolicy RemoteSigned.
4. Import session: $sessionimport = Import-PSSession $session.

   You should now be able to execute Exchange commands against your remote Outlook account.

Granting Application Impersonation Role Manually via PowerShell

This section provides the necessary commands to configure a service user that has the Application Impersonation role. To proceed, a working knowledge of PowerShell is recommended.

Grant the Application Impersonation role:

New-ManagementRoleAssignment –Name:impersonationAssignmentName –Role:ApplicationImpersonation –User: <Service User>

For example: New-ManagementRoleAssignment –Name:impersonationAssignmentName– Role:ApplicationImpersonation –User: “roomwizard@onmicrosoft.com”

Check if a user has the Application Impersonation role:

Get-ManagementRoleAssignment -RoleAssignee <Service User> -Role ApplicationImpersonation -RoleAssigneeType user

For example: Get-ManagementRoleAssignment -RoleAssignee “roomwizard@onmicrosoft.com” -Role ApplicationImpersonation -RoleAssigneeType user

Configuring Room Mailbox

By default, a room does not auto-accept invitations. In order for the RoomWizard and Exchange Connector to work properly, the room needs to be configured to auto-accept invitations. The room should also be configured to reject conflicting meetings.

Configure every room’s mailbox to auto-accept invitations:

Get-Mailbox | where{$_.ResourceType -eq “Room”} | Set-CalendarProcessing -AutomateProcessing AutoAccept -AllowConflicts $false

If you want to maintain the comments and private flag between the resource and the user, add the following arguments to the command above: -RemovePrivateProperty $false -DeleteComments $false

Reference: http://technet.microsoft.com/en-us/library/dd335046.aspx

Configure a specific room’s mailbox to auto-accept invitations:

Get-Mailbox “UpstairsConferenceRoom” | Set-CalendarProcessing -AutomateProcessing AutoAccept

By default, the room does not display the original subject of an invitation. Instead, the room shows the organizer's name as the subject. If this format is not desired, the following command will reconfigure the room mailbox to show the invitationsubject:

Set-CalendarProcessing -Identity "$$ResourceName$$" -AddOrganizerToSubject $false -DeleteSubject $false

Viewing Attendee Response Status from RoomWizard

For the Connector to see how attendees have responded to an invitation, the service user requires delegate access to all of the user's mailboxes. The Connector will function without delegate access; however, the attendees' response status will be unknown.

Find and grant all users and grants a service user full access:

Get-Mailbox -filter {isResource -eq $False} -Resultsize unlimited | Add-MailboxPermission -User: <Service User> -AccessRights: FullAccess -InheritanceType: All

Steelcase®

Visit Steelcase.com

facebook.com/Steelcase twitter.com/Steelcase youtube.com/SteelcaseTV

06/2016 © 2016 Steelcase Inc. All rights reserved. All specifications subject to change without notice. Trademarks used herein are the property of Steelcase Inc. or of their respective owners.