INSTALLATION MANUAL

RMS-SCH-EWS

RMS ENTERPRISE SCHEDULING INTERFACE FOR EXCHANGE

AV FOR AN IT WORLD

COPYRIGHT NOTICE

LIABILITY NOTICE

AMX WARRANTY AND RETURN POLICY

The AMX Warranty and Return Policy and related documents can be viewed/downloaded at www.amx.com.

Table of Contents

RMS Enterprise Scheduling Interface for Exchange (RMS-SCH-EWS)

Overview

The RMS Enterprise Scheduling Interface for Exchange (RMS-SCH-EWS) provides ad-hoc bookings and assists attendees in locating meeting rooms by displaying the scheduled appointments on a touch screen in the meeting room and adjacent to room entrances. It also provides automation capabilities for event start and end times.

The RMS Enterprise Scheduling Interface for Exchange utilizes the Microsoft® Exchange Web Services API to communicate with **Exchange 2010**, **2013**, **2016** and **Office 365** servers. This Scheduling Interface updates scheduling information in the Exchange or Office 365 Server, and synchronizes that information with AMX Touch Panels - making the scheduling information seamless between Exchange or Office 365 and AMX Touch Panels.

Scheduling Interfaces for RMS Enterprise are available to download from www.amx.com/rms/.

NOTE: *RMS-SCH-EWS is intended for use with RMS Enterprise version 4.3 or higher.*

The RMS-SCH-EWS Scheduling Interface provides:

- Appointment management features of the RMS application to synchronize RMS room schedules with Exchange servers.
- Add rooms in the RMS application that have you would like to schedule and associate them with an Exchange Room Mailbox.
- Calendaring & Scheduling:
  Display room appointments on AMX Touch Panel Schedule ad-
  hoc appointments
  Extend a meeting
  End a meeting
  Display room schedule along with appointment details to assist and inform meeting attendees

NOTE: *The RMS Enterprise application does not access emails, tasks, notes, etc.*

Microsoft Exchange 2010 & 2013 Server Requirements

- Microsoft Exchange 2010 SP3
- Microsoft Exchange 2013 SP1
- Microsoft Exchange 2016

Installation and Configuration Steps - Overview

1. **Create Room Mailboxes:** Each RMS Location must be associated with a *Room Mailbox*. See *Creating Room Mailboxes* on page 7 for details.
2. **Create a new Room List Distribution Group:** A Room List Distribution Group containing the Room Mailboxes that will be visible to RMS must be created on the server.
   - Each Room List Distribution Group can contain up to 100 entries.
   - Multiple Room Distribution Lists can be created as needed to manage more than 100 room mailboxes. See *Creating Room Lists (Distribution Groups)* on page 9 for details.
3. **Install and configure the RMS Enterprise Scheduling Interface for Exchange:** Refer to *Scheduling Interface for Exchange - Installation and Configuration* on page 11.
4. **Install the RMS Scheduling Interface (if necessary):** In order to add the Scheduling Interface (required to use any external scheduling interface) to your RMS Enterprise system, it is necessary to upgrade your RMS Entitlement with a Scheduling License. The Scheduling License enables support for various scheduling interfaces for RMS Enterprise.
   See *Adding the Scheduling Interface to RMS Enterprise* section on page 10 for details.
5. **Configure the RMS Service account:** In order for RMS Locations to synchronize with the Room Mailboxes, the RMS Enterprise Scheduling Interface for Exchange must add, modify, and cancel appointments using a domain account.
   See *Conf iguring the RMS Service Account* on page 19 for details.

Updating the RMS-SCH-EWS

To upgrade from a previous version of RMS-SCH-EWS, follow the instructions for installing the current version (see the *Installing the RMS Enterprise Scheduling Interface for Exchange* section on page 12).

NOTE: *The RMS-SCH-EWS installation process removes the previous version before installing the new version.*

Upgrading Legacy RMS Exchange Scheduling Plugin to RMS-SCH-EWS

To upgrade to RMS-SCH-EWS from the original RMS Exchange Scheduling Plugin, it is necessary to uninstall both the plugin and the troller. Refer to page 22 for details.

NOTE: *After installing the update, it is necessary to re-configure access to Exchange Room Mailboxes for the RMS Service account. Refer to the Conf iguring the RMS Service Account* on page 19 *for details.*

Creating Room Mailboxes

Overview

Exchange 2010, 2013, 2016 and Office 365 use *Room Mailboxes* to manage meeting room schedules. Each RMS Location (Resource) that will synchronize with RMS Enterprise must be represented by a Room Mailbox.

NOTE: *Appropriate administrator access is required to perform these tasks.*

Creating a New Room Mailbox: Exchange 2010

1. On the Exchange 2010 server, select **Microsoft Exchange Server 2010 > Exchange Management Console** to launchthe *Exchange Management Console* utility.
2. Under *Recipient Configuration*, right-click on **Mailbox** and select **New Mailbox** from the context menu. This selection opens the *New Mailbox - Introduction* dialog.
3. Select **Room Mailbox**, and click **Next** to proceed to the *New Mailbox - User Type* dialog.
4. Select either **New User** or **Existing users**:
   - **New User** - select this option to create a new user.
   - **Existing users** - select this option to assign an existing user that is not currently associated with an Exchange 2010 Mailbox.
5. Click **Next** to proceed to the *New Mailbox - User Information* dialog.
6. Fill in the user information fields in this dialog and click **Next** to proceed to the *New Mailbox - Mailbox Settings* dialog.
7. The default settings in this dialog are sufficient - click **Next** to proceed to the *New Mailbox New Mailbox (Confirmation Summary)* dialog.
   - Use this dialog to review the information entered.
   - To copy the summary information presented in this dialog, click CTRL+C.
8. Click **New** to create the new Mailbox, and proceed to the *New Mailbox - Completion* dialog.
9. Click **Finish**.
   - Repeat this process for each RMS Location that will synchronize with RMS.
   - Once a Room Mailbox has been defined for each RMS Location, all mailboxes must be added to a *Room Distribution List Group* (see *Creating Room Lists (Distribution Groups)* on page 9).

Additional Documentation

For more detailed information on creating a room mailbox, creating a room list and changing room mailbox properties in Exchange 2010, refer to the Microsoft® article "*Managing Resource Mailboxes and Scheduling*":

http://technet.microsoft.com/en-us/library/bb124374(v=EXCHG.141).aspx

Note that this article also provides instructions on using the Exchange Management Shell to create room mailboxes and room lists.

Creating a New Room Mailbox: Exchange 2013 and Exchange 2016

1. Log in to the Exchange Admin Center (EAC):

   https://<ip address of Exchange server>/ecp

   - or -

   https://<host name of Exchange server>/ecp

   a. Provide your credentials to log into Exchange.
   b. The Exchange Admin Center opens in your browser window.
2. Under *Recipients*, select **Resources**.
3. In the *Resources* page toolbar, click the **Add (+)** button then select **Room mailbox** to open the *New Room Mailbox* dialog.
4. Fill in the fields, and click **Save** to create the new mailbox and close the *New Room Mailbox*dialog.

NOTE: *The only required f ields in this dialog are Room name and Email address.*

   The new room should now be included in the list of Resources (on the *Resources* page).
5. Select the new mailbox and click **Edit** to open the *Room Mailbox* dialog. Use the options in this dialog to configure the new room mailbox.
6. Select **Booking Delegates**.
7. Under *Booking requests*, verify that **Accept or decline booking automatically** is selected (the defaultsetting).
8. Click **Save** to save changes and close the *New Room Mailbox* dialog.
   - Repeat this process for each RMS Location that will synchronize with RMS.
   - Once a Room Mailbox has been defined for each RMS Location, all mailboxes must be added to a *Room Distribution List Group* (see *Creating Room Lists (Distribution Groups)* on page 9).

Additional Documentation

For more detailed information on creating a room mailbox, creating a room list and changing room mailbox properties in Exchange 2013/2016, refer to the Microsoft® article "*Create and manage room mailboxes*":

http://technet.microsoft.com/en-us/library/jj215781%28v=exchg.150%29.aspx

Note that this article also provides instructions on using the Exchange Management Shell to create room mailboxes and room lists.

Creating a New Room Mailbox: Office 365

1. Log in to the Exchange Admin Center (EAC):

   https://outlook.off ice365.com/ecp/

   a. Provide your credentials to log into Office 365.
   b. The Exchange Admin Center opens in your browser window.
2. Under *Recipients*, select **Resources**.
3. In the *Resources* page toolbar, click the **Add (+)** button to open the *New Room Mailbox* dialog.
4. Fill in the fields, and click **Save** to create the new mailbox and close the *New Room Mailbox*dialog.

NOTE: *The only required f ields in this dialog are Room name and Email address.*

The new room should now be included in the list of Resources (on the *Resources* page).

5. Select the new mailbox and click **Edit** to open the *Room Mailbox* dialog. Use the options in this dialog to configure the new room mailbox.
6. Select **Booking Delegates**.
7. Under *Booking requests*, verify that **Accept or decline booking automatically** is selected (the defaultsetting).
8. Click **Save** to save changes and close the *New Room Mailbox* dialog.

- Repeat this process for each RMS Location that will synchronize with RMS.
- Once a Room Mailbox has been defined for each RMS Location, all mailboxes must be added to a *Room Distribution List Group* (see *Creating Room Lists (Distribution Groups)* on page 9).

Additional Documentation

For more detailed information on creating a room mailbox, creating a room list and changing room mailbox properties in Office 365, refer to the Microsoft® article "*Create and manage room mailboxes*":

http://technet.microsoft.com/en-us/library/jj215781%28v=exchg.150%29.aspx

Note that this article also provides instructions on using the Exchange Management Shell to create room mailboxes and room lists.

Creating Room Lists (Distribution Groups)

Overview

All Room Mailboxes or Resources to be synchronized with the RMS Enterprise Scheduling Interface for Exchange must be a member of a *Room List* Distribution Group. Each Room List Distribution Group can contain up to 100 entries; multiple Room Distribution Lists can be created as needed to manage more than 100 room mailboxes.

Resources that are not a member of a Room List Distribution Group will not be visible to the Scheduling Interface.

NOTE: *Appropriate administrator access is required to perform these tasks.*

Creating Room List Distribution Groups: Exchange 2010

The following Microsoft® articles provide detailed information on creating Room List Distribution Groups on the Exchange 2010 server - click links below to open:

- "**Create a Room List Distribution Group**" (http://technet.microsoft.com/en-us/library/ee633471%28v=exchg.141%29.aspx)
- **"Add a Member to a Distribution Group**" (http://technet.microsoft.com/en-us/library/aa995970%28v=exchg.141%29.aspx)

Creating Room Lists: Exchange 2013

The following Microsoft® article includes detailed information on creating *Room Lists* (which are specially marked distribution groups) on the Exchange 2013 server - click link below to open:

- "**Create and manage room mailboxes**" (http://technet.microsoft.com/en-us/library/jj215781%28v=exchg.150%29.aspx)

Creating Room Lists: Exchange 2016

The following Microsoft® article includes detailed information on creating Room Lists (which are specially marked distribution groups) on the Exchange 2016 server - click link below to open:

- **"Create and manage room mailboxes"** (https://technet.microsoft.com/en-us/library/jj215781(v=exchg.160).aspx)

Creating Room Lists: Office 365

The following Microsoft® article includes detailed information on creating *Room Lists* (which are specially marked distribution groups) on the Office 365 server - click link below to open:

- "**Create and manage room mailboxes**" (http://technet.microsoft.com/en-us/library/jj215781%28v=exchg.150%29.aspx)

Adding the Scheduling Interface to RMS Enterprise

Overview

In order to add the Scheduling Interface (required to use any Scheduling Interface) to your RMS Enterprise system, it is necessary to upgrade your RMS Entitlement with a *Scheduling License*. The Scheduling License enables support for various Scheduling Interfaces for RMS Enterprise.

This section describes upgrading your RMS Entitlement with a *Scheduling License*. The Scheduling License enables support for various Scheduling Interfaces for RMS Enterprise.

NOTE: *To ensure optimal performance of the RMS Enterprise UI, the RMS Scheduling Interface application should not be installed on the Primary RMS Enterprise Server. Install the RMS Scheduling Interface application on a separate server.*

Verify that the server that will run the RMS Enterprise Scheduling Interface meets or exceeds the minimum OS and hardware requirements indicated below.

Scheduling Server Recommendations

Verify that each server that will run the RMS Enterprise Scheduling Interface meets or exceeds the following minimum recommendations (check the appropriate boxes below):

Scheduling Server Hardware Recommendations			
Does your Scheduling server meet the following Minimum Hardware Recommendations?		**Yes**	**No**
• Processor	Dual core Intel Xeon processor @ 2.67GHz (or equivalent)		
• Memory	4 GB		
• Display	1280 x 1024 resolution		
• Hard Disk	1 GB available space for RMS Enterprise Scheduling application files.		
Yes to all	Please continue to the next step.		
No to any	You must obtain a server that meets these minimum requirements to install RMS Enterprise.		

For installations with more than 50 locations that use the Scheduling Interface, a separate server from the RMS Application is required.

Scheduling Interface Operating System			
Do you have a compatible server OS installed?		**Yes**	**No**
Supported Microsoft Server Operating Systems: • Microsoft Windows Server 2012 R2 (64-bit) • Microsoft Windows Server 2008 R2 (64-bit): Web Edition / Standard Edition / Enterprise Edition			
Yes	Please continue to the next step.		
No	You must obtain a compatible server OS to install RMS.		
Do you have an administrative account to the server where RMS will be installed?		**Yes**	**No**
Note: RMS is a system level application and requires administrative access to install and configure RMS, including the Scheduling Interface and Scheduling Configuration Tool.			
Yes	Please continue to the next step.		
No	You must obtain an administrative logon account, or logon to the server with a user account that has administrative access to the server.		

Before You Start

- Verify that the Primary RMS Server is running.
- Have the IP Address and login credentials for the RMS Enterprise Server.
- Have the IP Address and login credentials for the scheduling interface.

Scheduling Interface for Exchange - Installation and Configuration

Overview

To use the RMS Enterprise Scheduling Interface for Exchange, it must first be registered. Only a single Scheduling Interface should be registered at one time. The RMS Enterprise Scheduling Interface for Exchange communicates with a single Exchange (2010, 2013) or Office 365 server.

NOTE: RMS Enterprise must be configured to use External Scheduling Systems in order for the RMS Scheduling Configuration tool to work. See the Adding the Scheduling Interface to RMS Enterprise section on page 10.

Preparing to Install the Scheduling Interface for Exchange

When the RMS Enterprise Scheduling Interface for Exchange installation is launched, the program will indicate if required software is not detected:

- **If a previous version of the Scheduling Interface for Exchange is installed on the PC, it must be uninstalled before installing the current version.**
- **When the previous version of the Scheduling Interface is uninstalled, all room mapping and scheduling data will be lost. All rooms will have to be re-mapped in the updated Scheduling Interface for Exchange.**

NOTE:

RMS-SCH-EWS 1.0.41 and later comes with bundled JRE(Java-11.0.4) and doesn't require Java to be installed separately.

Below steps should be followed to upgrade from earlier version to current RMS-SCH-EWS(1.0.41):

1. **Upgrade without uninstalling existing version of RMS-SCH-EWS:**
    a. **Download and install RMS-SCH-EWS(1.0.41).**
    b. **Uninstall Java if not required.**

2. **Upgrade with uninstallation of existing version of RMS-SCH-EWS:**
    a. **Uninstall existing version of RMS-SCH-EWS.**
    b. **Uninstall Java if not required.**
    c. **Download and install RMS-SCH-EWS(1.0.41)**

3. **In-case user uninstall Java (without uninstalling existing version of RMS-SCH-EWS), and then Downloads and install RMS-SCH-EWS(1.0.41), installed RMS-SCH-EWS won't work.**
4. **To recover, user must uninstall existing RMS-SCH-EWS and then install RMS-SCH-EWS(1.0.41) again.**

Installing the RMS Enterprise Scheduling Interface for Exchange

When all perquisite software has been installed (and any previous version of the Scheduling Interface has been uninstalled), the new RMS Enterprise Scheduling Interface for Exchange can be installed:

1. Launch the Setup Wizard (installation file): **RMSExchangeEWSPlugin.exe**.

2. The first dialog to display is the *Welcome* screen(FIG. 3):

FIG. 3 Welcome to the RMS Enterprise Scheduling Interface for Exchange Setup Wizard dialog

3. Click **Next** to proceed to the End-User License Agreement (FIG. 4):

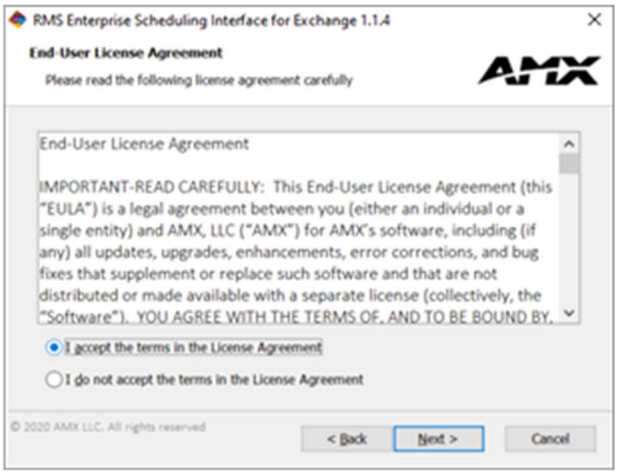


FIG. 4 End-User License Agreement dialog

4. Click *I accept the terms in the License Agreement* then click **Next** to proceed to the *Select Installation Folder* dialog (FIG. 5):

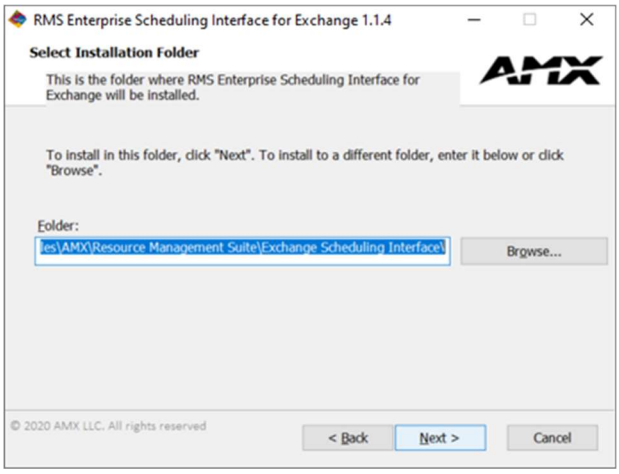


FIG. 5 Select Installation Folder dialog

5. Click **Next** to proceed to the *Ready to Install* dialog (FIG. 6):

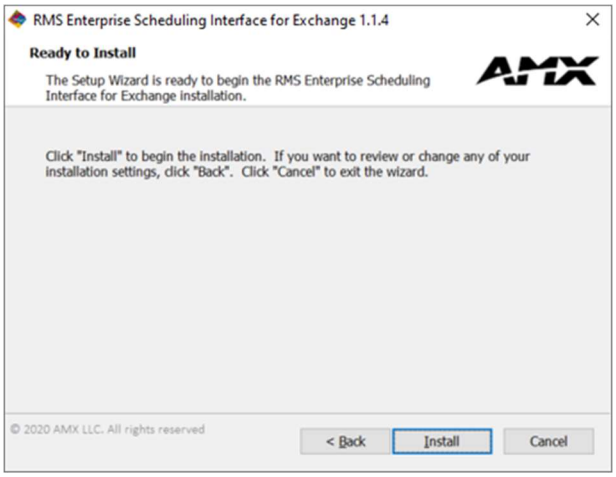


FIG. 6 Ready to Install dialog

6. Click **Install** to start the installation (FIG. 7):

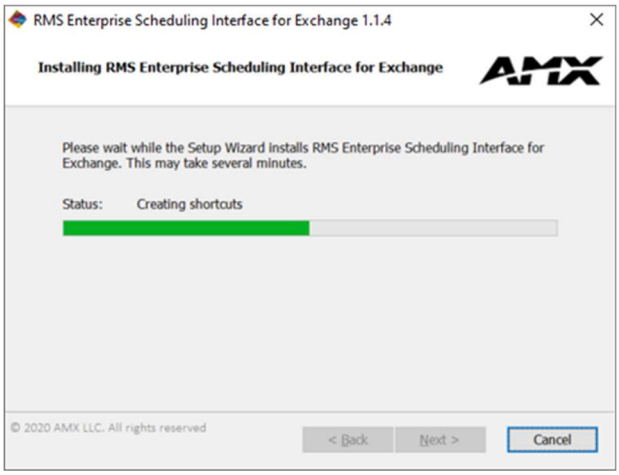


FIG. 7 Installing (status) dialog

7. In the final Setup Wizard dialog, click **Finish** to exit the Setup Wizard and launch the *RMS Scheduling Configuration* tool (FIG. 8). The *RMS Enterprise Scheduling Configuration* tool is described in the following section.

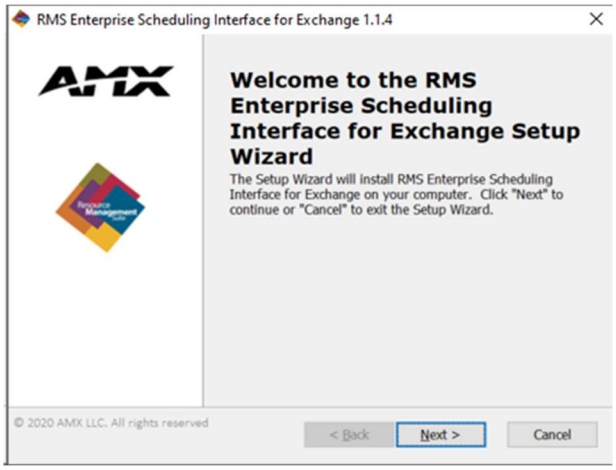


FIG. 8 RMS Enterprise Scheduling Interface for Exchange - Installation Completed

NOTE: *Refer to Upgrading From the Legacy RMS Exchange EWS Scheduling Plugin to RMS-SCH-EWS* section on page 22 *for instructions on uninstalling and upgrading to RMS-SCH-EWS from previous versions of the scheduling interface plugin.*

Configuring the Scheduling Interface

Once the Scheduling Interface for Exchange has been installed, it must be registered and configured to communicate with RMS Enterprise, via the *AMX-RMS Scheduling Configuration for Exchange* tool.

Click **Finish** in the final Setup Wizard dialog to launch the *AMX-RMS Scheduling Configuration for Exchange* tool. The Scheduling Configuration tool UI consists of four tabs: *RMS Server*, *Exchange Settings*, *Synchronization Options* and *Resource Profiles*. Each tab is described in the following sections:

RMS Scheduling Configuration - RMS Server tab

The initial view of the RMS Scheduling Configuration tool is the *RMS Server* tab. Use the options in this tab to enter connection information for the RMS Enterprise server (FIG. 9):

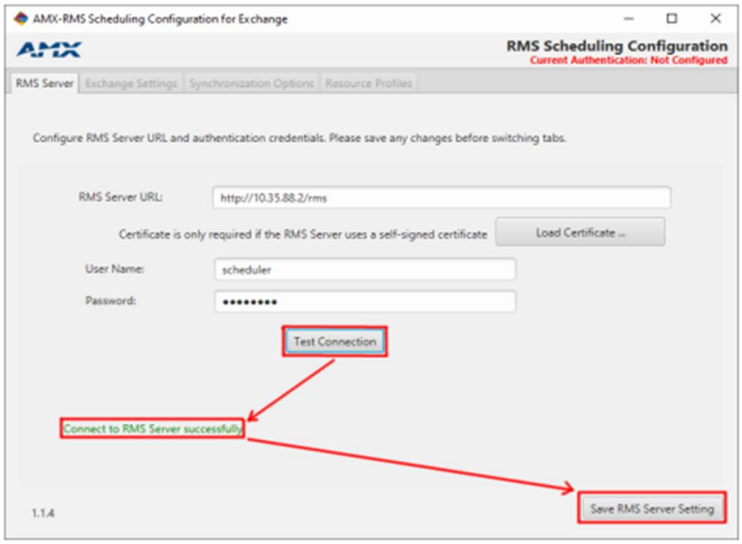


FIG. 9 AMX-RMS Scheduling Configuration for Exchange tool - RMS Server tab

1. In the **RMS Server URL** field, enter the URL or IP address of the RMS Server that will use this scheduling interface.
2. If the RMS Server uses a self-signed certificate, click **Load Certificate** to locate and select the appropriate certificate, via the *Select RMS Server Self Signed Certificate* dialog.
3. In the **User Name** field, enter the user name required by the server (default = "*scheduler*").
4. In the **Password** field, enter the password required by the server (default = "*password*").
5. Click **Test Connection** to verify the information entered. The program will indicate whether the connection was successful (see FIG. 9).
   If the connection attempt fails, re-enter the RMS Server information and try again.
   NOTE: *You cannot proceed until you have successfully connected to the RMS Server. The "Save RMS Server Settings" button is enabled only after a successful connection test.*
6. Click **Save RMS Server Setting** to save these settings and register the Scheduling Interface with the RMS Server.
   Once the dialog indicates that the RMS Server Settings were saved, the *Exchange Settings* tab are enabled (FIG. 10)

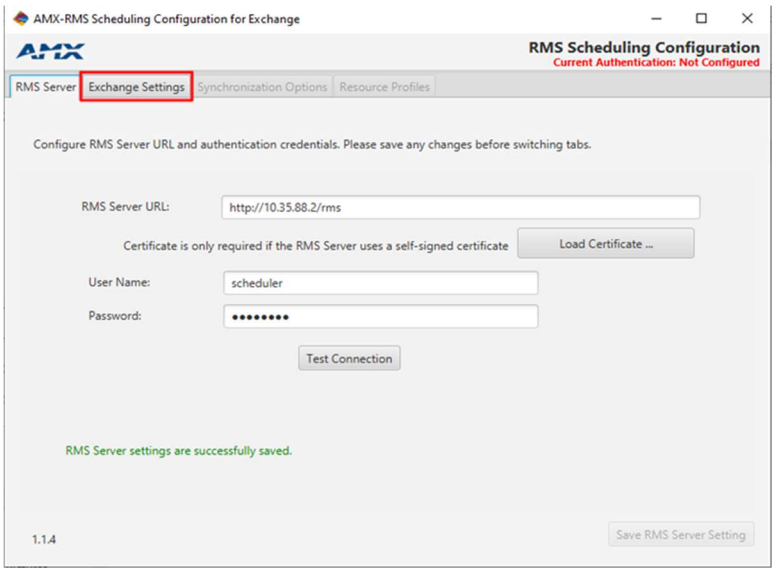


FIG. 10 AMX-RMS Scheduling Configuration for Exchange tool - RMS Server tab – Exchange Settings tab enabled

RMS Scheduling Configuration - Exchange Settings tab – Basic Authentication

Use the options in the *Exchange Settings* tab to configure RMS access to Exchange by entering the URL for Exchange Web Services and specify the authentication method and credentials for the RMS Service account (FIG. 11):

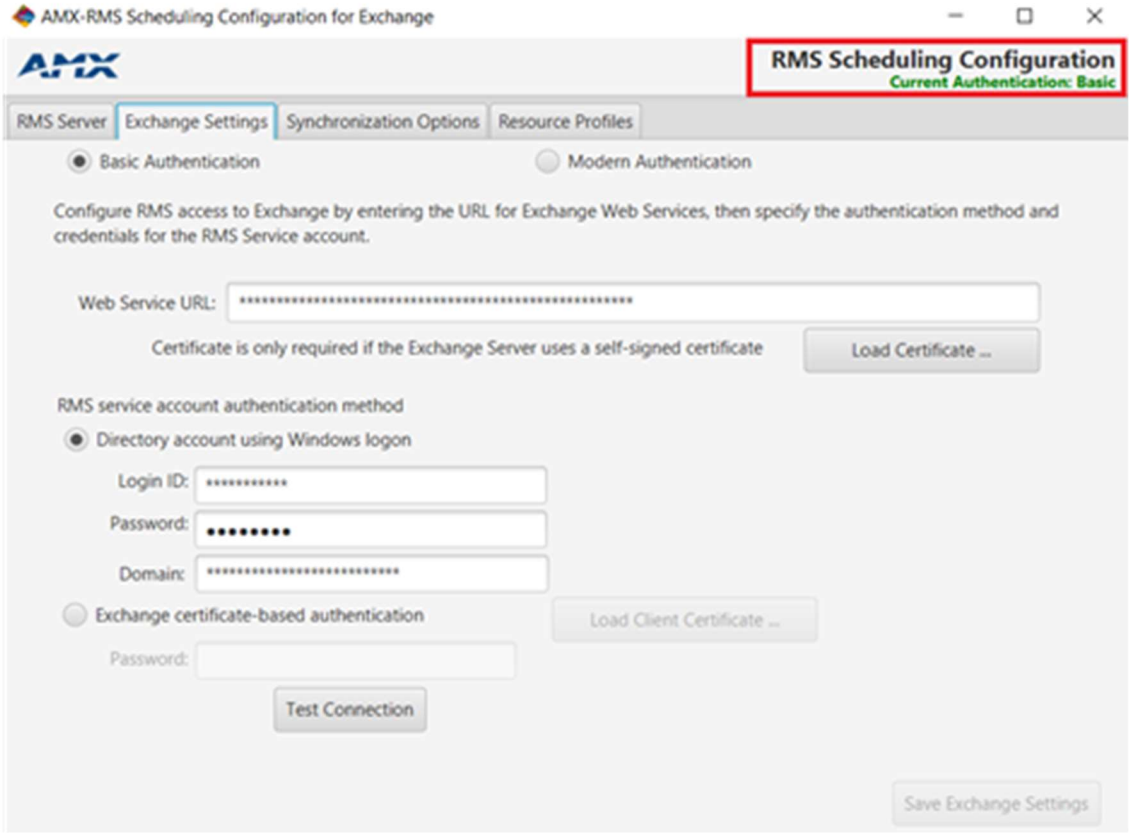


FIG. 11 AMX-RMS Scheduling Configuration for Exchange tool - Exchange Settings tab

1. For Basic Authentication, ensure the Basic Authentication radio button is selected.
2. In the **Web Service URL** field, enter the URL for the Web Service on the Exchange (or Office365) server (see FIG.11).
3. If the Exchange (or Office365) server uses a self-signed certificate, click **Load Certificate** to locate and select the appropriate certificate (via the *Select Exchange Self Signed Certificate* dialog). Double-click on a certificate to view details.
4. Under *RMS Service Account Authentication Method*, select the authentication method to employ (*Directory account using Windows login* or *Exchange certificate-based authentication*):
   - Select **Directory Account using Windows login** (the default setting) to use Windows login credentials to authenticate the RMS Service Account.

     NOTE: *This is the account that will query, create and modify bookings via the touch panel. This account must have full permissions (Exchange 2010/2013) or be a delegate for all resources (Office 365). See Configuring the RMS Service Account* section on page 19 *for details.*

     With this option selected, the following entries are required:
     - **Login ID**: Enter a valid login ID associated with the Exchange server.
     - **Password**: Enter the password associated with the login ID entered above.
     - **Domain**: Enter the domain for the Exchange server.
   - Select **Exchange certificate-based authentication** to use a client certificate to authenticate the RMS Service Account. Click **Load Client Certificate** to locate and select the appropriate client certificate (via the *Select Exchange Client Certificate* dialog. Double-click on a certificate to view details.
5. Click **Test Connection** to test these settings. The program will indicate whether the connection was successful (see FIG. 9 on page 14). If the connection attempt fails, re-enter the server information and try again.

   NOTE: *You cannot proceed until you have successfully connected to the RMS Server.*
6. Click **Save Exchange Settings**. Once the dialog indicates that the **Exchange Settings** were saved, proceed to the *Synchronization Options* tab.

NOTE: *The current **saved** Exchange authentication method (Basic vs Modern) is indicated in the upper right-hand side of the AMX-RMS Scheduling Configuration for Exchange. Changing the radio button selection to Basic or Modern does not commit the change, only the Save Exchange Settings button does this.*

RMS Scheduling Configuration - Exchange Settings tab – Modern Authentication

Use the options in the *Exchange Settings* tab to configure RMS access to Exchange by entering the URL for Exchange Web Services and specify the authentication method and credentials for the RMS Service account (FIG. 12):

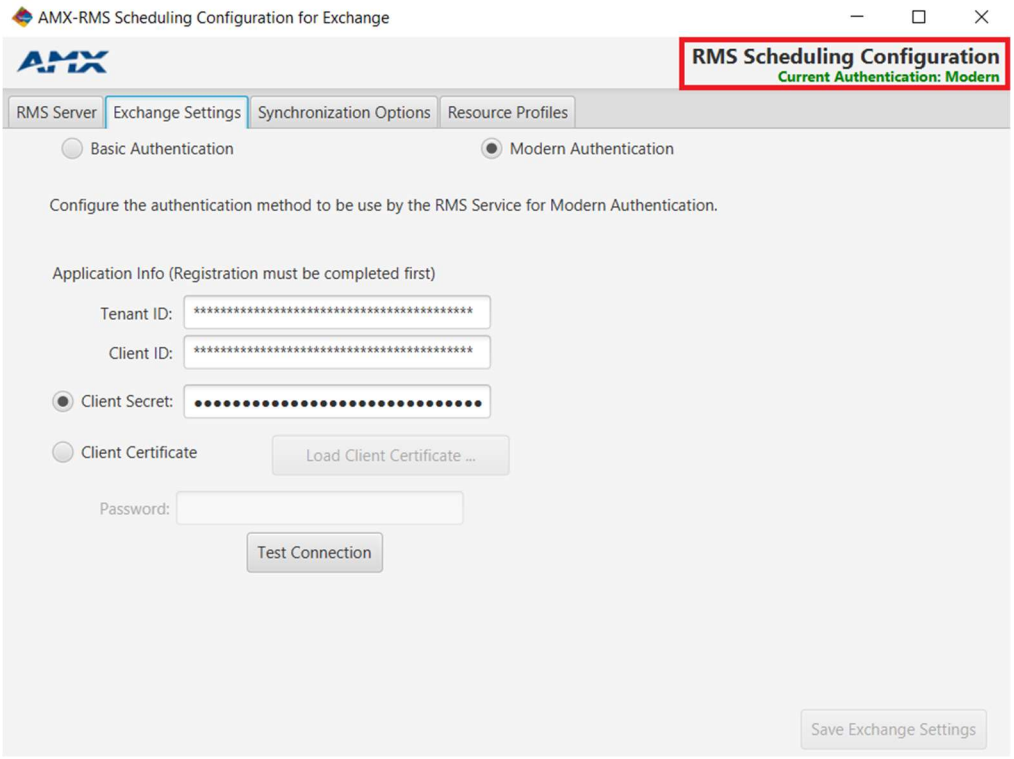


FIG. 12 AMX-RMS Scheduling Configuration for Exchange tool - Exchange Settings tab – Modern Authentication

1. For Modern Authentication, ensure the Modern Authentication radio button is selected.
2. Enter the Azure settings for your Office 365 account. Tenant ID and Client ID are required for either authentication method. (see FIG.12).
3. For Modern Authentication, there is a choice of two types of credentials for authorization: Client Secret and Client Certificate.
    a. For Client Secret, select the radio button and enter the Client Secret text
    b. For Client Certificate, select the radio button, then:
        i. Hit Load Client Certificate to upload the Azure-generated certificate
        ii. Enter the password for the Azure-generated certificate
4. Click **Test Connection** to test these settings. The program will indicate whether the connection was successful (see FIG. 9 on page 14). If the connection attempt fails, re-enter the server information and try again.
   NOTE: *You cannot proceed until you have successfully connected to the RMS Server.*
5. Click **Save Exchange Settings**. Once the dialog indicates that the **Exchange Settings** were saved, proceed to the *Synchronization Options* tab.

NOTE: *The current **saved** Exchange authentication method (Basic vs Modern) is indicated in the upper right-hand side of the AMX-RMS Scheduling Configuration for Exchange. Changing the radio button selection to Basic or Modern does not commit the change, only the Save Exchange Settings button does this.*

RMS Scheduling Configuration - Synchronization Options tab

Many systems perform nightly backups or system related processing where the server may not be available or should not be accessed. The blackout option prevents the RMS application from accessing the server during these times. During this blackout period, The RMS application will not attempt to establish a connection to any Exchange server.

NOTE: *By default, RMS Enterprise synchronizes with the Exchange server every 15 minutes.*

Use the options in the **Synchronization Options** tab to configure a blackout period and set polling and synchronization settings (FIG. 13):

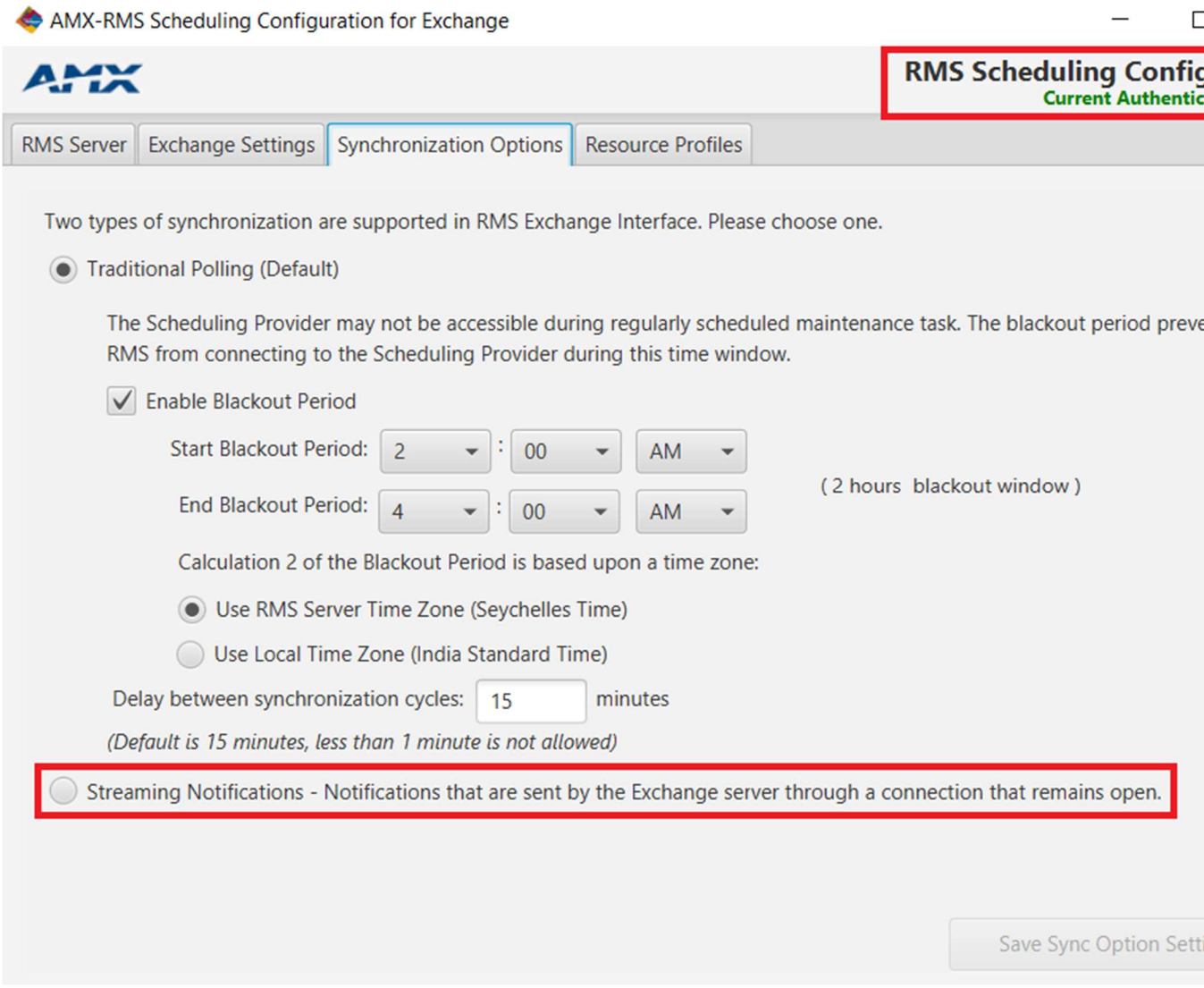


FIG. 13 AMX-RMS Scheduling Configuration for Exchange tool - Synchronization Options tab

Select one of the two synchronization options supported in the RMS Exchange interface (*Traditional Polling* or *Streaming Notifications*).

Traditional Polling

NOTE: *To use the Traditional Polling method (for both Exchange and Office365), each Location that will managed by the Scheduling Interface can use either Full Access, Delegation or Impersonation for access rights.*

If **Traditional Polling** is selected (the default setting), the following information is required:

- **Enable Blackout Period**: Select to enable the *Start / End Blackout Period* fields. This option is enabled by default and is recommended. Use these fields to specify the start and end times for the Blackout Period to accommodate your specific environment.

  Start Blackout Period default setting = **2:00 AM** (click the *Hours*, *Minutes* and *AM/PM* menus to adjust)

  End Blackout Period default setting = **4:00 AM** (click the *Hours*, *Minutes* and *AM/PM* menus to adjust)
- **Calculation 2 of the Blackout Period is based upon a time zone**: Use these options to specify whether to use the *RMS Server Time Zone* (default setting) or to *Use Local Time Zone (Central Standard Time)* as the basis for the blackout period.

  NOTE: *The Scheduling Provider may not be accessible during regularly scheduled maintenance tasks. The blackout period prevents RMS from connecting to the Scheduling Provider during this time window.*
- **Delay between synchronization cycles:** Use this option to adjust the synchronization cycles delay (in minutes).

Streaming Notifications

NOTE: *To use the Streaming Notifications method (for Basic Authentication with Exchange), each Location that will managed by the Scheduling Interface must use Impersonation for access rights.*

If **Streaming Notifications** is selected, notifications sent by the server are sent through an open connection, as the notifications are generated. When this option is selected, the program checks to verify that the target Exchange server supports streaming notification.

- If it is determined that the Exchange server *does not* support streaming notification, a message is presented to indicate that the sync selection has automatically been reverted to *Traditional Polling.* In this case, use the *Enable Blackout Period* and *Calculation 2 of the Blackout Period...* options as described above.
- If the Exchange server does support streaming notification, a message is presented and the *Save Sync Option Setup* button is enabled (FIG. 14):

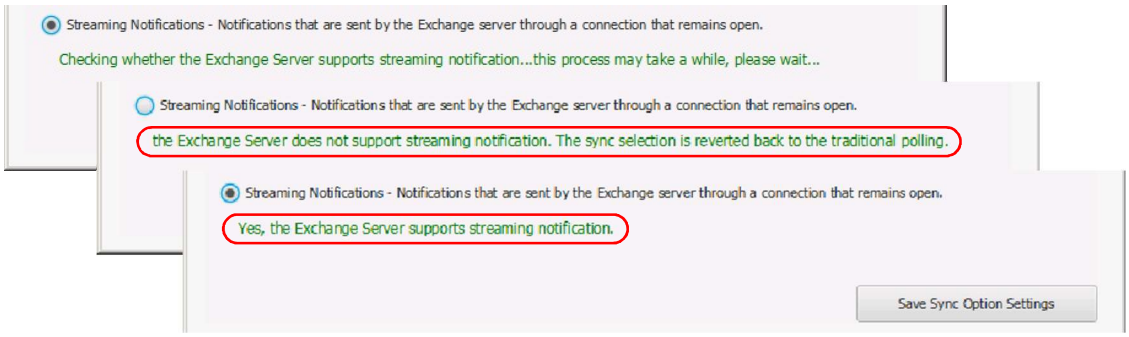


FIG. 14 Synchronization Options tab - checking Exchange server for Streaming Notification support

NOTE: *Streaming Notifications method for Modern Authentication with Office365 is not currently supported*

RMS Scheduling Configuration - Resource Profiles tab

RMS Enterprise will retrieve resource profiles (for all Locations on the RMS Server) for the currently registered Exchange server. Use the **Resource Profiles** tab to specify which Locations (Resources) will use the RMS Enterprise Scheduling Interface for Exchange.

NOTE: *This tab is initially empty until the application automatically loads the room list from the Exchange server.*

In a few seconds, the *Resource Name* column is populated with a listing of Locations from the Exchange Server (FIG. 15):

NOTE: *In some circumstances, a delay of up to 24 hours can occur before newly added rooms will populate in the Resources Tab. This is an issue with the Microsoft Graph API and the returned data from a query of the associated rooms.*

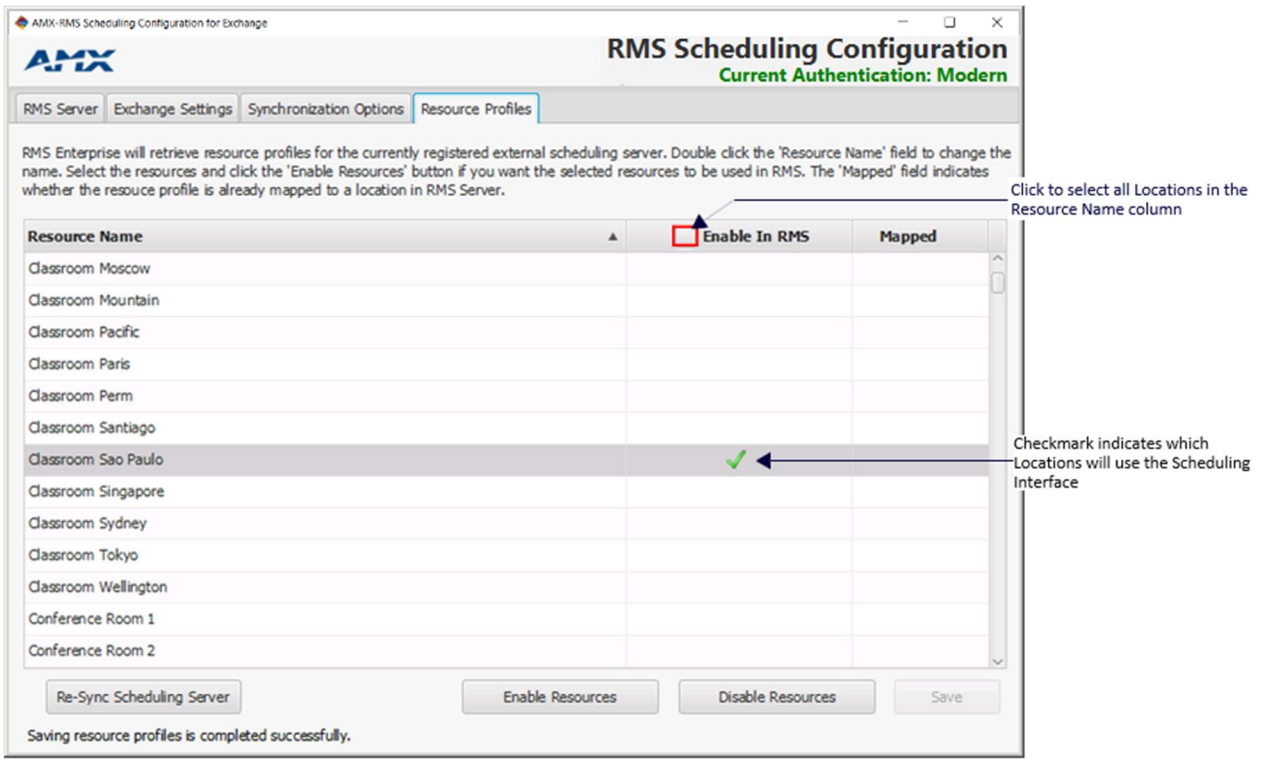


FIG. 15 RMS Scheduling Configuration - Resource Profiles tab

NOTE: *Double-click the Resource Name field to edit Resource Names as desired.*

1. Select which of the Locations (Resources) will use the Scheduling Interface:
   - Click to select a Location in the *Resource Name* column and select **Enable Resources** to use the Scheduling Interface with that Location.
   - Shift + click two Locations in the list to select a range of Locations; Ctrl + click to manually select multiple Locations. The *Enable Resources* and *Disable Resources* buttons work on the selected Locations.
   - Click **Enable In RMS** to either select or de-select all Resources in the list.

   NOTE: *The Mapped column indicates which of the Locations (Resource Profiles) are currently mapped to a location on the RMS Server. For information on mapping Resource Profiles to Locations on the RMS Server, refer to the Location to Resource Profile Mapping* section on page 20.
2. Click **Save**. This will push the selected (checked) Resources to the RMS Server, where they become "Resource Profiles" in RMS.
3. Exit the **RMS Scheduling Configuration** application.

Updating the Resource Name list

Click **Re-Sync Scheduling Server** (Resource Profiles tab) to refresh the *Resource Name* list.

When the re-sync is complete, the *Re-sync Resource Profiles* dialog is displayed, indicating all rooms detected on the

Recurring Appointments in Exchange With "No End Date"

Recurring appointments in Exchange that have "*No End Date*" specified are limited to two years of occurrences synchronized into RMS. After the two years elapses, no further bookings for that series will be synchronized into RMS.

NOTE: *It is recommended that recurring appointments either have a specific end date or a number of occurrences defined.*

Configuring the RMS Service Account

Overview

In order for RMS Locations to synchronize with Room Mailboxes (Exchange) or Resources (Office 365), the scheduling plug-in must add, modify, and cancel appointments using a domain account with full access permissions. This domain account is referred to as the *RMS Service Account*.

The RMS Service Account must be configured on both the Scheduling Server (the PC running RMS Enterprise and Scheduling Plug- In), and the Exchange (2010, 2013 or 2016) or Office 365 Server.

Configuring the RMS Service Account on the Scheduling Server

1. On the server that has the RMS Scheduler and Plug-In installed, open the *Services Management* page.
2. Right-click on the *RMS Enterprise Legacy Troller* service and select **Properties** to open the *RMS Enterprise Troller Properties* dialog.
3. Click on the **Log On** tab.
4. Select **This Account** and enter the RMS Service Account user account information that will be used as the RMS Trolling Service.
   The account information entered here must match the account information for the RMS Service Account.
5. Click **Apply** to save changes, close this dialog and return to the main *Services* page.

At this point, the **Log On As** entry for *RMS Enterprise Legacy Troller* service should indicate the RMS Service Account that was defined in the *RMS Enterprise Troller Properties* dialog.

Configuring the RMS Service Account on the Exchange 2010/2013/2016 or Office 365 Server

The *RMS Service Account* on the Exchange or Office 365 server must meet the following requirements:

- The account must have an associated Exchange Mailbox.
- The account must have rights to add, modify, and cancel/delete appointments in each Exchange Room Mailbox with which RMS will synchronize. This may be accomplished via any of the following three methods:

a. *Delegate* access to the mailbox.
b. *Impersonate* the mailbox owner using Exchange Impersonation.
c. *Assign* full-access permissions to the mailbox.

The following links provide access to Microsoft documentation regarding each of these methods for each supported server OS:

Exchange 2010	Set a Delegate on a Resource Mailbox: http://technet.microsoft.com/en-us/library/bb124973(v=exchg.141).aspx
Exchange 2013, 2016, Office 365	Delegating Permissions: http://technet.microsoft.com/en-us/library/jj215781%28v=exchg.150%29.aspx (go to **Create a room mailbox > Use the EAC to create a room mailbox**) *Note: If you selected the option requiring that booking requests are sent to delegates, use this section to select delegates.* To add a delegate, click **Add**. On the *Select Delegates* page, select a user, click **Add**, and then click **OK** to return to the *New room mailbox* page. To remove a delegate, select the user and then click **Remove**. Assigning Full-Access Permissions: http://technet.microsoft.com/en-us/library/jj919240%28v=exchg.150%29.aspx

Limiting Impersonation to Mailboxes that will be Synchronized with RMS

By default Exchange Impersonation will allow the RMS account to access to every mailbox in the organization. For security purposes the impersonation scope for the RMS account should be limited to the Exchange Room Mailboxes that will be synchronized with RMS. There are numerous options for creating this management scope which are beyond the scope of this document.

- For information about Exchange management scopes see:
  http://technet.microsoft.com/en-us/library/dd335137.aspx
- Enabling Impersonation is explained in detail at:
  http://msdn.microsoft.com/en-us/library/bb204095%28EXCHG.140%29.aspx

Location to Resource Profile Mapping

Overview

Before an RMS Location can synchronize with Exchange, each Location must be associated with a Resource Profile:

1. In the RMS Web UI, select **Management > Configure Locations/Clients > Locations** (FIG. 16):

FIG. 16 RMS Web UI - Management > Configure Locations/Clients > Locations

2. This opens the main Location page. In the *Locations* window, select a Location name from the list and click **Edit** (FIG.17):

FIG. 17 RMS Web UI - Locations Page - Edit button

3. This opens the **Location Edit** page (*Settings* tab).
4. Under **Scheduling Configuration**, open the *Resource Profile* drop-down list to select a Resource Profile to map to this Location (FIG. 18):

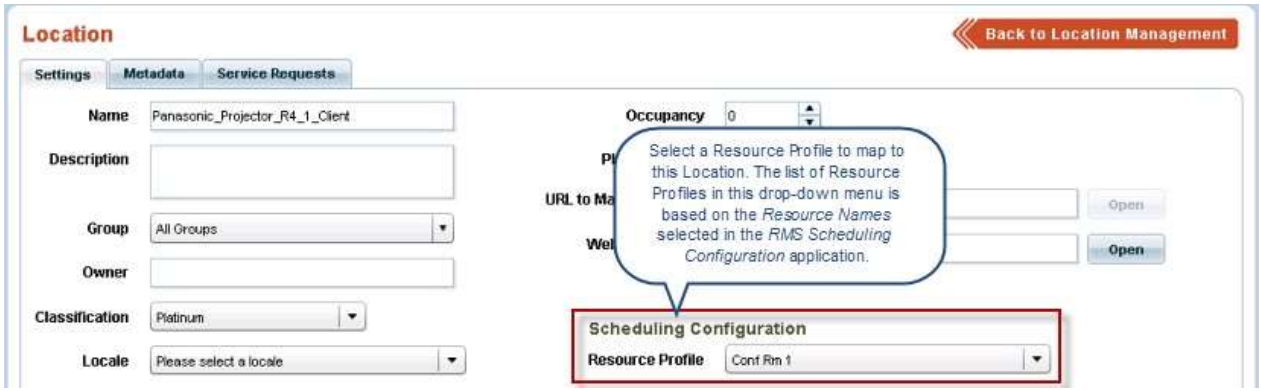


FIG. 18 RMS Web UI - Location Edit Page - Scheduling Configuration drop-down menu

NOTE: *The list of Resource Profiles that are available to select in this menu is based on the Resource Names that were selected in the RMS Scheduling Configuration application - Resource Profiles tab. Note that if any of the names were edited in the RMS Scheduling Configuration application, the edited names are displayed here.*

This will associate the location with the selected Resource Profile (i.e. the Exchange room mailbox).

5. Click **Apply** to save changes.

As Resource Profiles are mapped to Locations, a green checkmark is added to the RMS Scheduling Configuration application - *Resource Profiles* tab (*Mapped* column) to indicate which Locations have been mapped. For example, FIG. 19 on page 21 shows the RMS Scheduling Configuration application, indicating that "*ConfRm1*" is mapped:

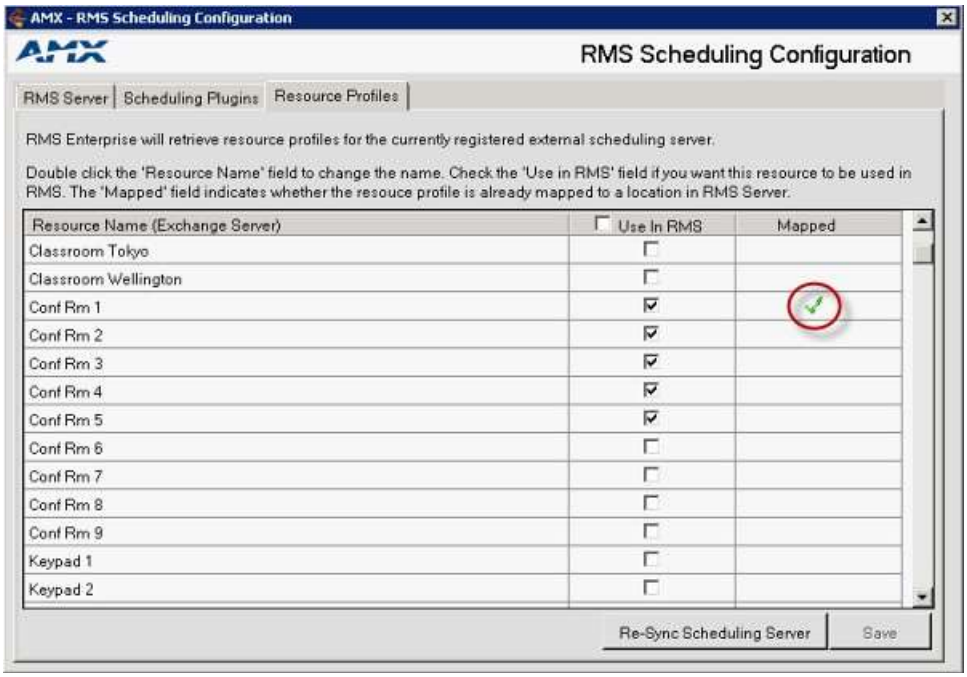


FIG. 19 RMS Scheduling Configuration application (indicating "ConfRm1" mapped)

Appendix

Upgrading From the Legacy RMS Exchange EWS Scheduling Plugin to RMS-SCH-EWS

To upgrade to RMS-SCH-EWS from any version of the legacy RMS Exchange EWS Scheduling Plugin, it is necessary to uninstall both the RMS Exchange EWS Scheduling Plugin and the RMS Scheduling Troller via their respective uninstall programs

- For **Windows 2008 R2 Servers**, referto *Uninstalling the EWS Scheduling Plugin: Windows 2008 R2 Servers* (below).
- For **Windows 2012 Servers**, refer to the *Uninstalling the EWS Scheduling Plugin: Windows Server 2012* section on page 26.

Uninstalling the EWS Scheduling Plugin: Windows 2008 R2 Servers

1) Unregister the Scheduling Plugin

1. Select **Start > All Programs > AMX Resource Management Suite > Scheduler > Scheduling Configuration** (FIG. 20):

FIG. 20 Windows Server 2008 R2 - AMX Resource Management Suite > Scheduler > Scheduling Configuration

2. In the *AMX - RMS Scheduling Configuration* application, open the **Scheduling Plugins** tab (FIG. 21):

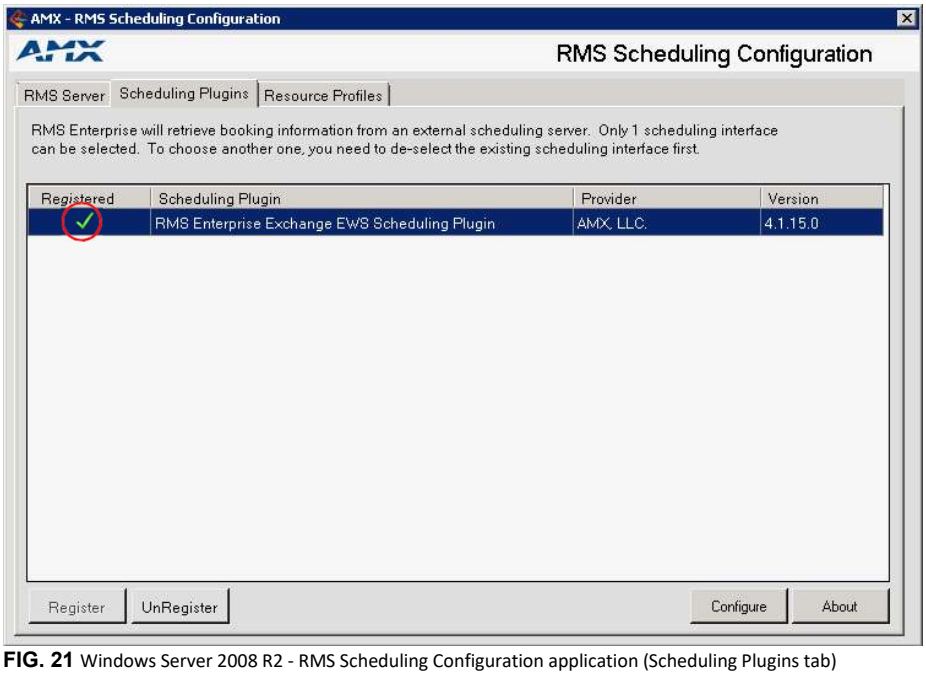


FIG. 21 Windows Server 2008 R2 - RMS Scheduling Configuration application (Scheduling Plugins tab)

3. Select the **RMS Enterprise Exchange EWS Scheduling Plugin** and click **UnRegister**.

4. The system will prompt you to verify this action - click **Yes** to proceed (FIG. 22):

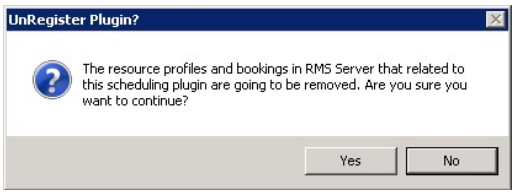
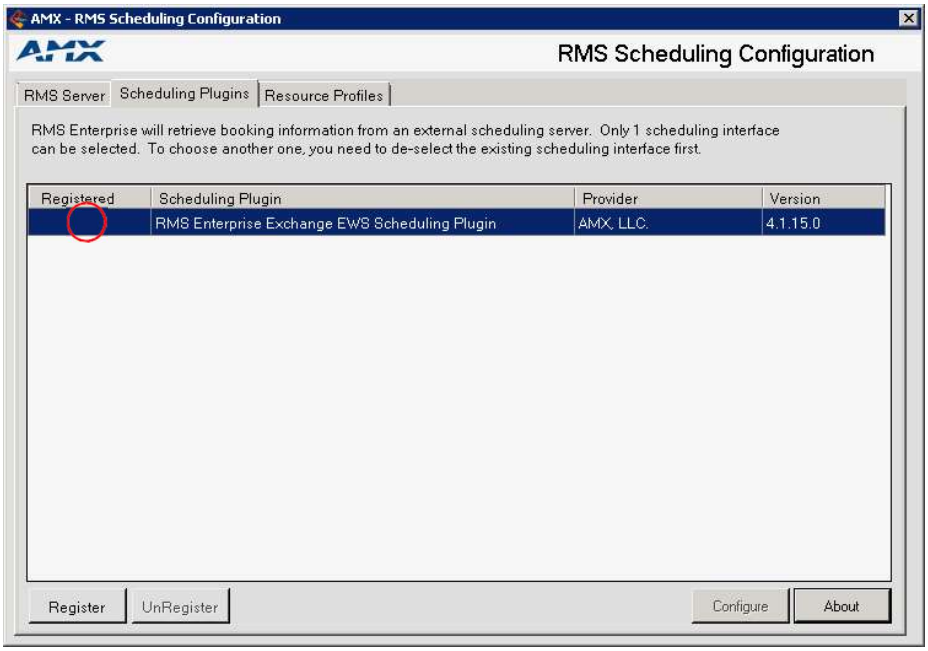


FIG. 22 Windows Server 2008 R2 - Verify Unregister Plugin action

The **RMS Enterprise Exchange EWS Scheduling Plugin** is no longer registered, as indicated in the *Scheduling Plugins* tab (FIG. 23):

FIG. 23 Windows Server 2008 R2 - RMS Scheduling Configuration application (Scheduling Plugins tab, no Plugins registered)



5. Close the *AMX - RMS Scheduling Configuration* application.

2) Uninstall the RMS Exchange EWS Plugin

1. Select **Start > All Programs > AMX Resource Management Suite > Uninstall RMS Exchange EWS Plug-In** (FIG. 24):

FIG. 24 (Windows Server 2008 R2 - Uninstall RMS Exchange EWS Plug-In

2. This launches the *Perform Uninstall* dialog - press **Finish** (FIG. 25):

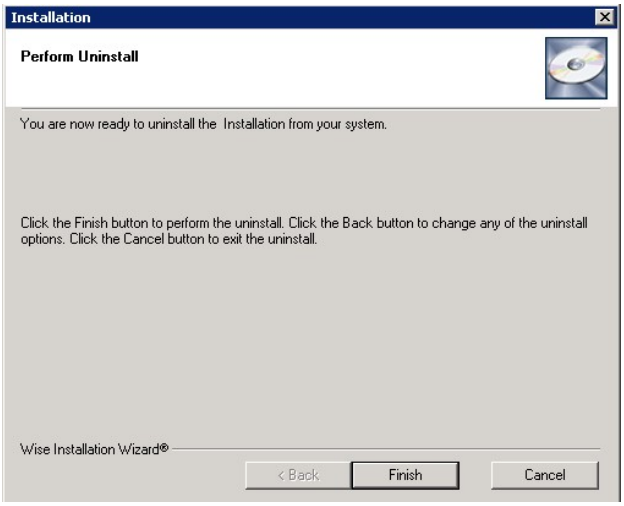


FIG. 25 Windows Server 2008 R2 - Perform Uninstall dialog

3. The system will prompt you to reboot the server to complete the installation (FIG. 26):

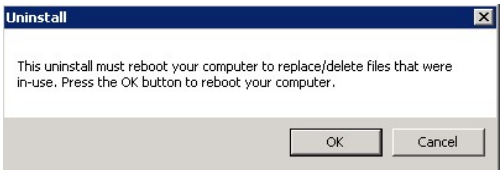


FIG. 26 Windows Server 2008 R2 - Uninstall (reboot) dialog

4. Click **OK** to reboot the server.

3) Uninstall the Troller

1. Select **Start > All Programs > AMX Resource Management Suite > Uninstall RMS Scheduling** (FIG. 27):

FIG. 27 (Windows Server 2008 R2 - Uninstall RMS Scheduling

2. The *Windows Installer* dialog prompts you to verify this action - click **Yes** to proceed (FIG. 28):

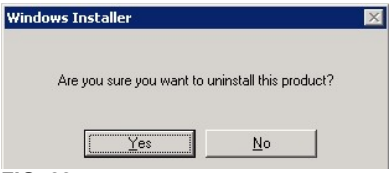


FIG. 28 Windows Server 2008 R2 - Windows Installer

4) Clear Troller Error(s) from the RMS Enterprise Hotlist

1. Open RMS Enterprise to the Classic UI view and look for troller process errors in the Hotlist (FIG.29):

FIG. 29 RMS Enterprise (Classic UI) - Hotlist indicating Troller error

2. Select the troller process error(s) and click the **Dismiss** button to dismiss the selected Hotlistitems.

Uninstalling the EWS Scheduling Plugin: Windows Server 2012

1) Unregister the Scheduling Plugin

1. From the Apps page, locate the **AMX Resource Management Suite** category (FIG. 35):

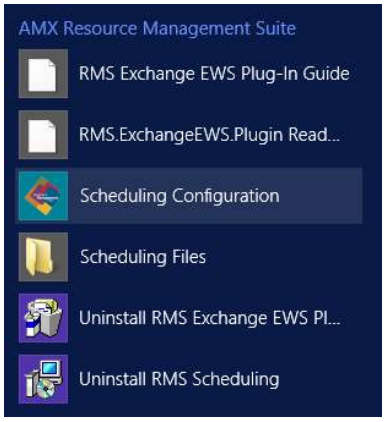


FIG. 30 Windows Server 2012 Apps page - AMX Resource Management Suite apps category

2. Click **Scheduling Configuration** (FIG. 31):

FIG. 31 Windows Server 2012 - Scheduling Configuration

3. In the *AMX - RMS Scheduling Configuration* application, open the **Scheduling Plugins** tab (FIG. 32):

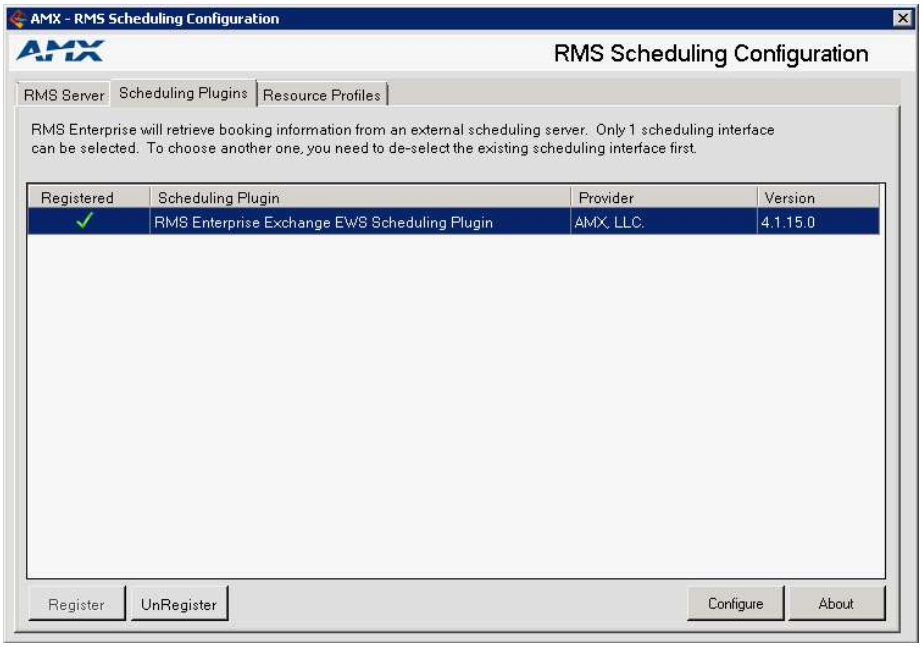


FIG. 32 RMS Scheduling Configuration application (Scheduling Plugins tab)

4. Select the **RMS Enterprise Exchange EWS Scheduling Plugin** and click **UnRegister**.
5. The system will prompt you to verify this action - click **Yes** to proceed (FIG. 33):

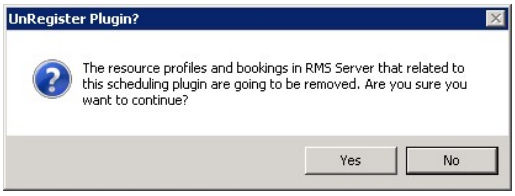
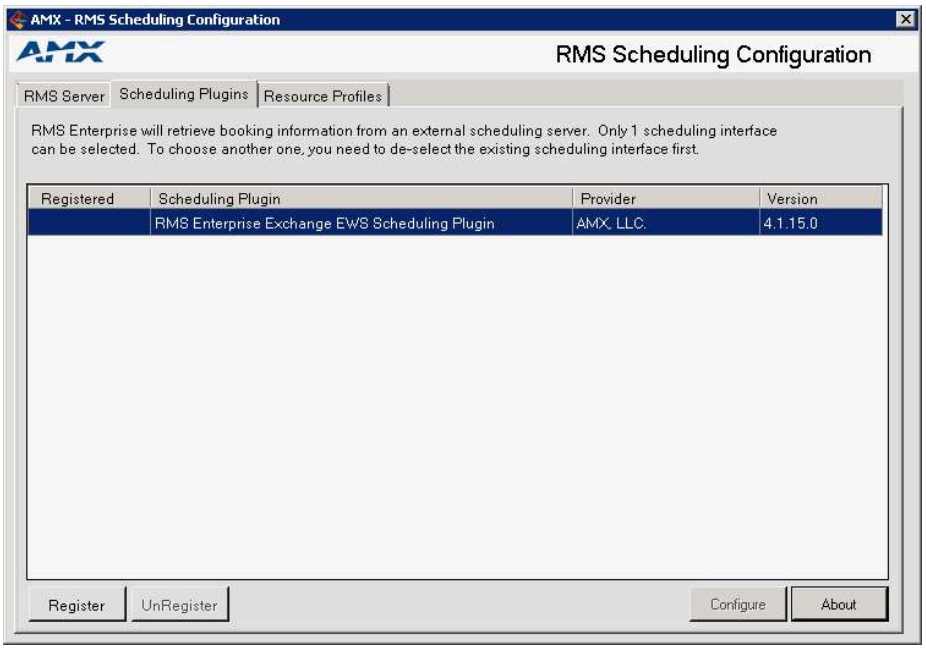


FIG. 33 Verify Unregister Plugin action

The **RMS Enterprise Exchange EWS Scheduling Plugin** is no longer registered, as indicated in the *Scheduling Plugins* tab (FIG. 23):

FIG. 34 RMS Scheduling Configuration application (Scheduling Plugins tab, no Plugins registered)



6. Close the *AMX - RMS Scheduling Configuration* application.

2) Uninstall the RMS Exchange EWS Plugin

1. From the Apps page, locate the **AMX Resource Management Suite** category (FIG. 35):

FIG. 35 Windows Server 2012 Apps page - AMX Resource Management Suite apps category

2. Click **Uninstall RMS Exchange EWS Plug-in** (FIG. 36):

FIG. 36 Windows Server 2012 - Uninstall RMS Exchange EWS Plugin

3. The system will prompt you to verify this action (FIG. 37):

FIG. 37 Windows Server 2012 - Windows Installer

4. Click **Yes** to proceed.

3) Uninstall the Troller

1. In the *AMX Resource Management Suite* apps category, click **Uninstall RMS Scheduling** (FIG. 38):

FIG. 38 Windows Server 2012 - Uninstall RMS Scheduling

2. The system will prompt you to verify this action (FIG. 39):

FIG. 39 Windows Server 2012 - Windows Installer

3. Click **Yes** to proceed.

4) Clear Troller Error(s) from the RMS Enterprise Hotlist

1. Open RMS Enterprise to the Classic UI view and look for troller process errors in the Hotlist (FIG.40):

FIG. 40 RMS Enterprise (Classic UI) - Hotlist indicating Troller error

2. Select the troller process error(s) and click the **Dismiss** button to dismiss the selected Hotlistitems.

Once these steps are complete, the server ready to have the latest version of RMS-SCH-EWS installed. See the *Scheduling Interface for Exchange - Installation and Configuration* section on page 11 for details.

NOTE: *After installing the update, it is necessary to re-configure access to Exchange Room Mailboxes for the RMS Service account. Refer to the Configuring the RMS Service Account on page 20 for details.*

Notes on the configuration of Modern Authentication

NOTE: *Typically, this process will be handled by the IT department in the target organization. The following is provided as an example of how to configure these setting in the absence of such a group, as well as to better communicate the requirements to the IT personnel in the target organization.*

Pre-requisites:

- An active Azure account
- An Azure AD tenant

I. Self-signed Certificate creation

In order to use certificate as credential for the Application, you need to generate a certificate and upload it to Azure AD.

1. Open **Windows PowerShell**

2. Execute the below given command to create a Self-signed Certificate:

```
New-SelfSignedCertificate -CertStoreLocation "Cert:\LocalMachine\My" -Subject
"CN=<ApplicationName>"
```

NOTE: *Replace the ApplicationName with the name of your application that you create on Azure AD.*

II. Export Certificate

Export the Self-signed certificate to use with the application with **Certificate Manager** as explained below:

1. Execute **mmc** command in the **Command Prompt** / **Windows PowerShell**.
2. Open **File** > **Add/Remove Snap-In**.
3. Add the **Certificates** snap-in from the **Available snap-ins** pane to the **Selected snap-ins** pane.
4. Select the **Computer Account** radio button in the **Certificates snap-in** dialog box and click **Next**
5. Select the **Local Computer** radio button in the **Select Computer** dialog box and then click **Finish**
6. Click **OK**
7. Select **Console Root > Certificates (Local Computer) > Personal > Certificates** from the tree view on the left pane.
8. You will see the newly generated application certificate

a. Export Certificate - Without Private Key (.CER)

We need to export the certificate without Private key and Base-64 Encoded X.509 .CER format to upload in Azure AD.

1. Select the application certificate and right click
2. Select **All tasks > Export** option
3. **Certificate Export Wizard** opens.
4. Click **Next** button
5. Select the **No, do not export the private key** radio button and click **Next**
6. Select the **Base-64 encoded X.509 (.CER)** radio button and click **Next**
7. Click **Browse** button and select a folder to place the exported file
8. Key in the **File name** and click **Save** button
9. Click **Next** button
10. You will see **You have successfully completed the Certificate Export Wizard**
11. Click **Finish** button
12. Click **OK** button

b. Export Certificate - With Private Key (.PFX)

We need to export the certificate with Private key and PKCS #12 (.PFX) format to be loaded in RMS EWS Scheduler Interface application.

1. Select the application certificate and right click
2. Select **All tasks > Export** option
3. **Certificate Export Wizard** opens.
4. Click **Next** button
5. Select the **Yes, export the private key** radio button and click **Next**
6. Select the **Personal Information Exchange – PKCS #12 (.PFX)** radio button and click **Next**
7. For **Security,** select the **Password** checkbox
8. Key-in the password and repeat the same in **Confirm password**
9. Accept the default option in **Encryption** dropdown and click **Next** button
10. Click **Browse** button and select a folder to place the exported file
11. Key in the **File name** and click **Save** button
12. Click **Next** button
13. You will see **You have successfully completed the Certificate Export Wizard**
14. Click **Finish** button
15. Click **OK** button

III. Generate the keyCredentials value using PowerShell

Run the following **PowerShell** script to generate the keyCredential value based on your **Base-64 encoded** certificate file.

This will get the values that are to be placed in Azure AD App Manifest.

```
$Cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2

$Cert.Import("C:\RmsSchCert\TestApp_GrpCBA.cer")

$BinaryData = $Cert.GetRawCertData()
$Base64Value = [System.Convert]::ToBase64String($BinaryData)

$BinaryData = $Cert.GetCertHash()
$Base64Thumbprint = [System.Convert]::ToBase64String($BinaryData)

$Keyid = [System.Guid]::NewGuid().ToString()

Write-Host "Base-64 Thumbprint:"
$Base64Thumbprint

Write-Host "Keyid:"
$Keyid

Write-Host "Base-64 Value:"
$Base64Value
```

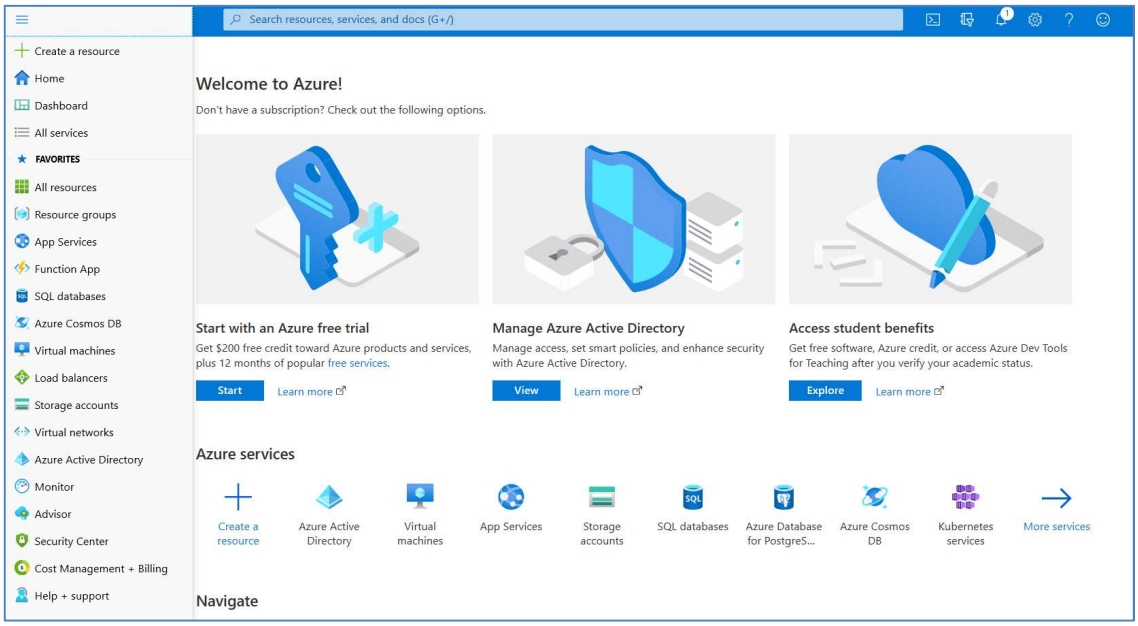
```
PS C:\WINDOWS\system32> C:\TempCert\For ModernAuthentication Testing\TestApp_GraphCert.ps1
Base-64 Thumbprint:
td5HRk2F2BqFUvxXfUsX9PD+tdg=
Keyid:
235dd0e4-7ee5-4468-8a5a-6c6711016e98
Base-64 Value:
MIIDCDCCAfCgAwIBAgIQeZ4VSoqO4Y9CF/uadI86JjANBgkqhkiG9w0BAQsFADAXMRUwEwYDVQQDDAxSbXNTY2hHcnBDQkEwHhcNMjAwODAyMTcwODE5WhcNMjEwODAyMTcxODE5WjAXMRUwEwYDVQQD
DAxSbXNTY2hHcnBDQkEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCXzb7Iqkv4oytnzW7QVuObpTtaANUMk+HY6EHHhpYNT+YdMPpYvoAJtmM2ksLCcZsmeCge8EHj3j7PembipGfnVZa8
G/BHyG5nKYe1k4rkh5IfiYc+vA4YRaQ/hCnzIHzSwSBe4ulzSZz3UtazcbLdTbmG+68+BdzKAjESfa3J81qC6e6iqL1s/uGTpa3i+KCL9cpjvE+pFS5yZsss2D7XDAbHMrFB62Zl/Ldw3jsgOcJ2Klah
t2Q2miAJBO/5Q4Av3S1TxW3R01U8Ho8DCt6hOmY8mUobEg3VB28TnrmjO1EFk6r/HOqxq2i4Tp3MQX1tryxXbOsaw2kiUDs3VCepAgMBAAGjUDBOMA4GA1UdDwEB/wQEAwIFoDAdBgNVHSUEFjAUBggr
BgEFBQcDAgYIKwYBBQUHAwEwHQYDVR0OBBYEFM4cIsWbDwRDCcLMqN4fczOOEacGMA0GCSqGSIb3DQEBCwUAA4IBAQBps8Z0Sxsbvngj DJnlSws4bcFkhoFi1/c6EmSGVYOZdvOyGSIZ+yu1zclHJsBK
AY9hCc/lCB4yCVCn3Qi+2XdaKIJ/9zpha0m/PryNkFtqYRHme7ddVyo2bivIytjLs753l/Owix75OFpfNYC9N9cugKsNUqhi26lRjTBjgsuqC9ghLEhALsUKiVZo7/+YX2/2KPk2KTyvcbGZ8LqzsxGj
FcawECDqwvqMdRED0+qmdLY/9schsb6L2K4cutJZ3GxsDHkdlnscx99i9jyHt4XRXBONpXdE5YOQ8YQXil1k1RsJyEjp9h7+VtzxzicBEfMmgU2ITzwg8Joj2s2XbNVz
```

Copy the value from the PowerShell output terminal into a Text Editor. We will be using **Base-64 Thumbprint** and **Keyid** values in section ***Modify the Manifest of Azure AD Application***

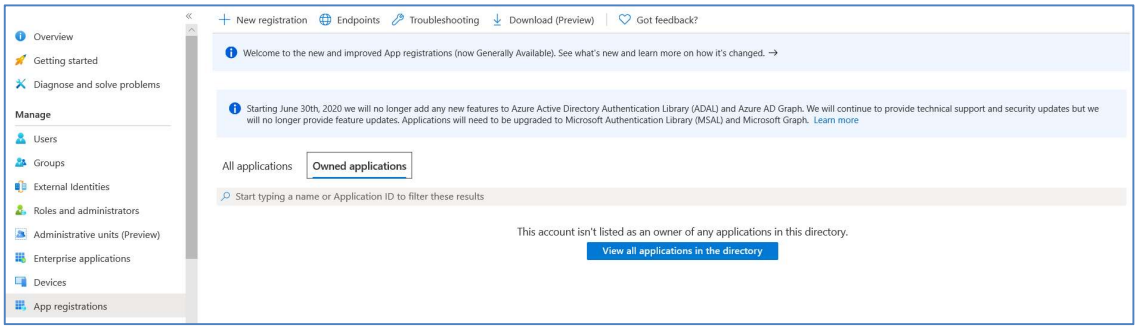
IV. Create your App registration in Azure Active Directory

Access the Azure Portal (https://portal.azure.com) and sign-in with the user ID that has the **Global Administrator** rights

From the Portal Menu, select the **Azure Active Directory option**



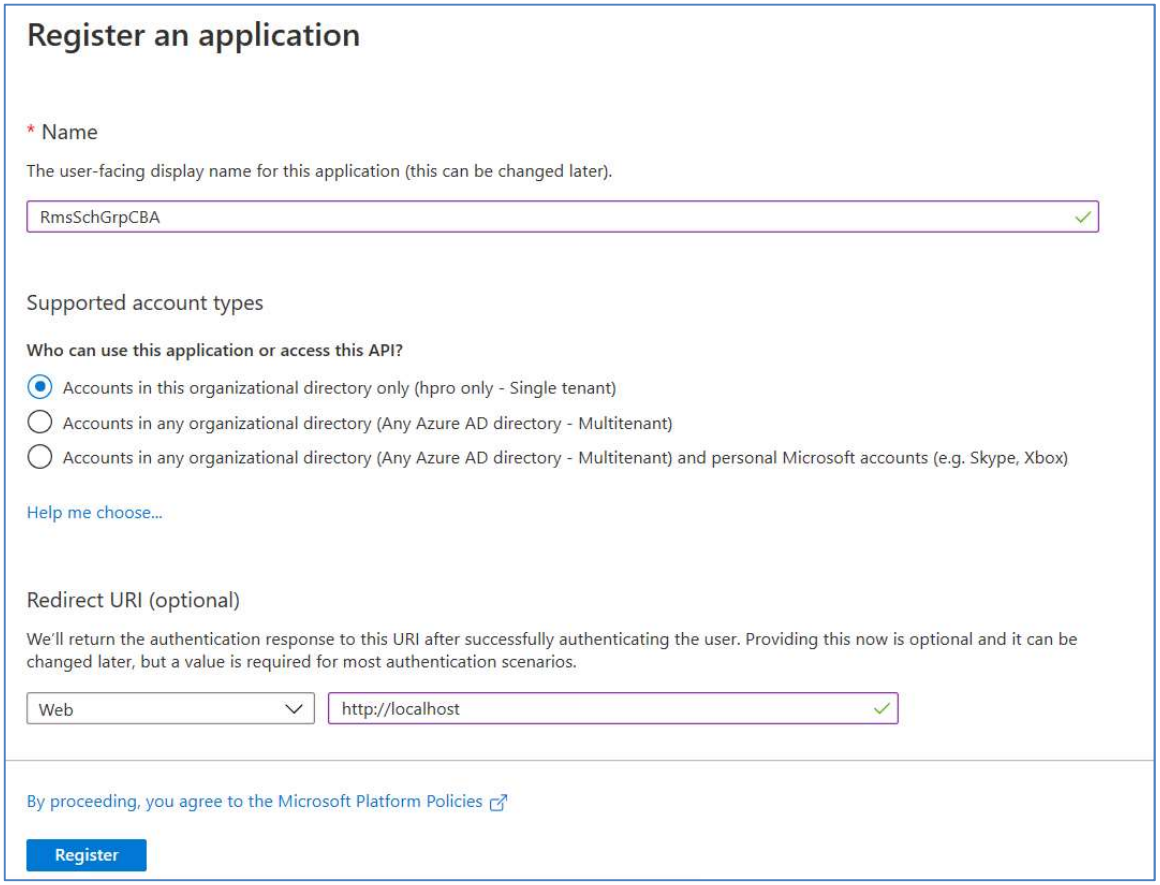
In the left navigation menu, select **App registrations** from **Manage** section **of Active Directory Menu Blade**



Click on the **New registration** option from the top right section.

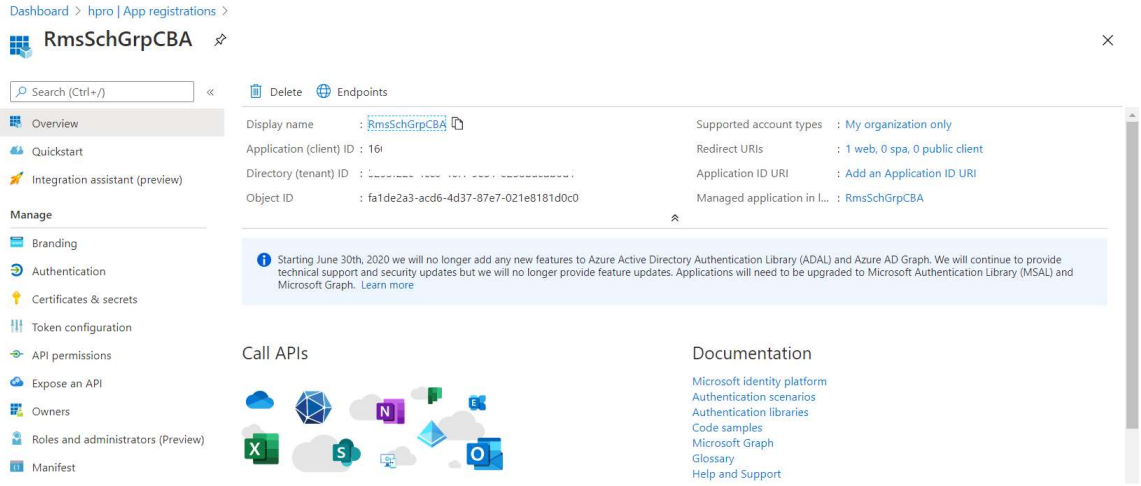
In the 'Register an application' page:

a. Fill in **Name** for the application.
b. Select the **Supported account types** as "Accounts in this organization directory only"
c. Set the **Redirect URI (optional)** as "Web" and URI as http://localhost



Click **Register** button.

Overview page opens for the newly created application

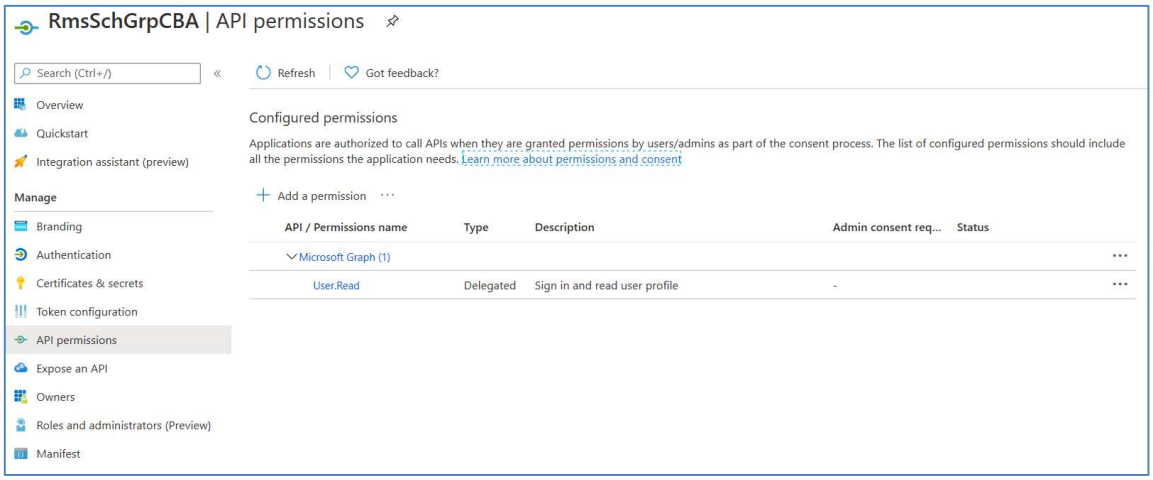


Make note of the **Tenant ID**, **Client ID** values. We will be using them while configuring the **RMS Scheduler Interface Exchange** for Modern Authentication

V. Add Graph API permissions to the RMS Scheduler app

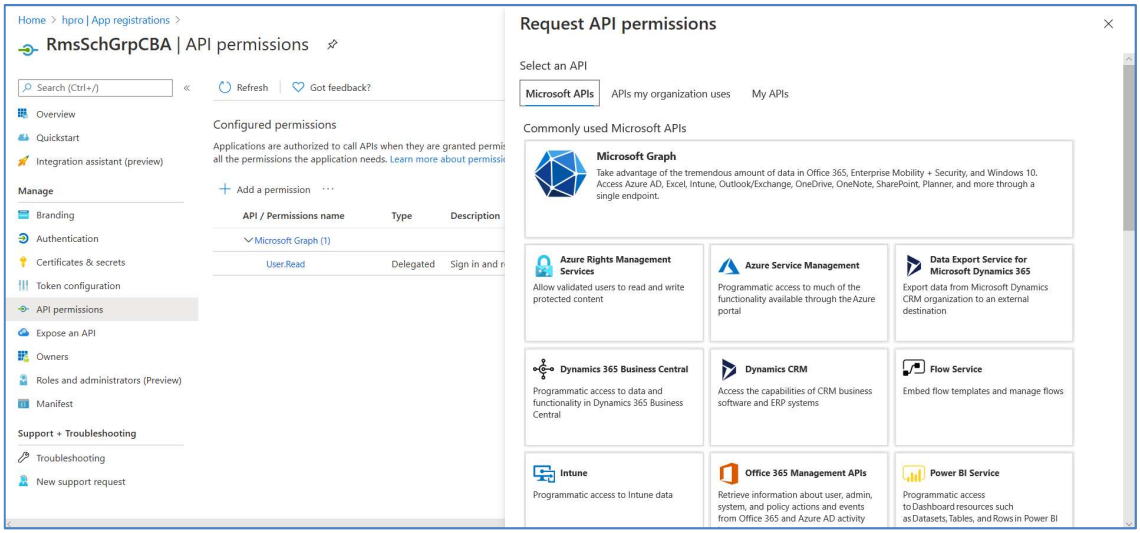
In the left navigation menu, select **API Permissions** from **Manage section of Application Menu Blade**

API Permissions page opens

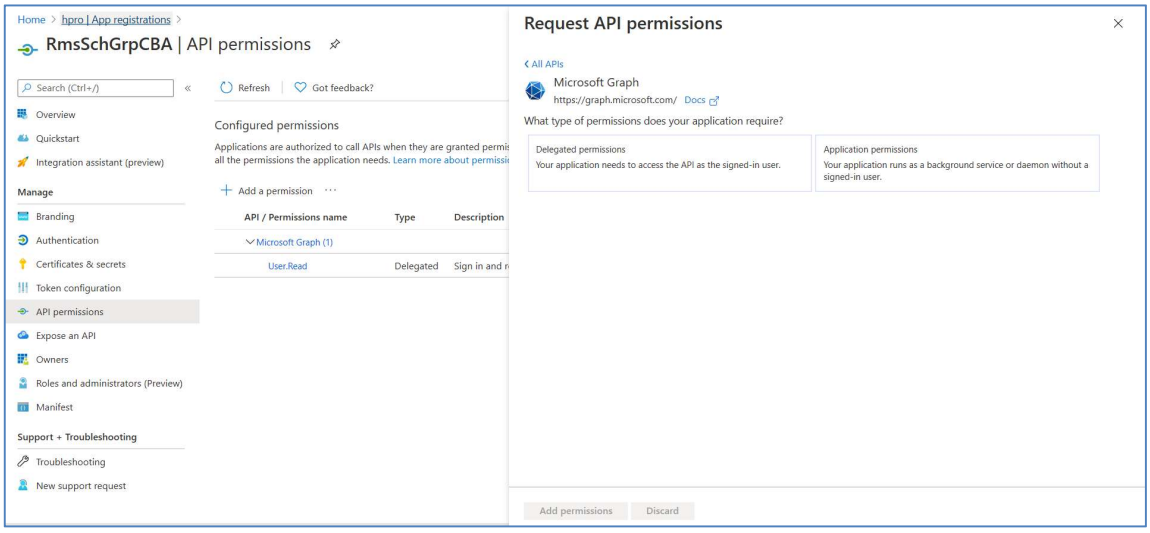


Click on the **Add a permission** option from the **Configured permissions** section.

Request API permissions page opens



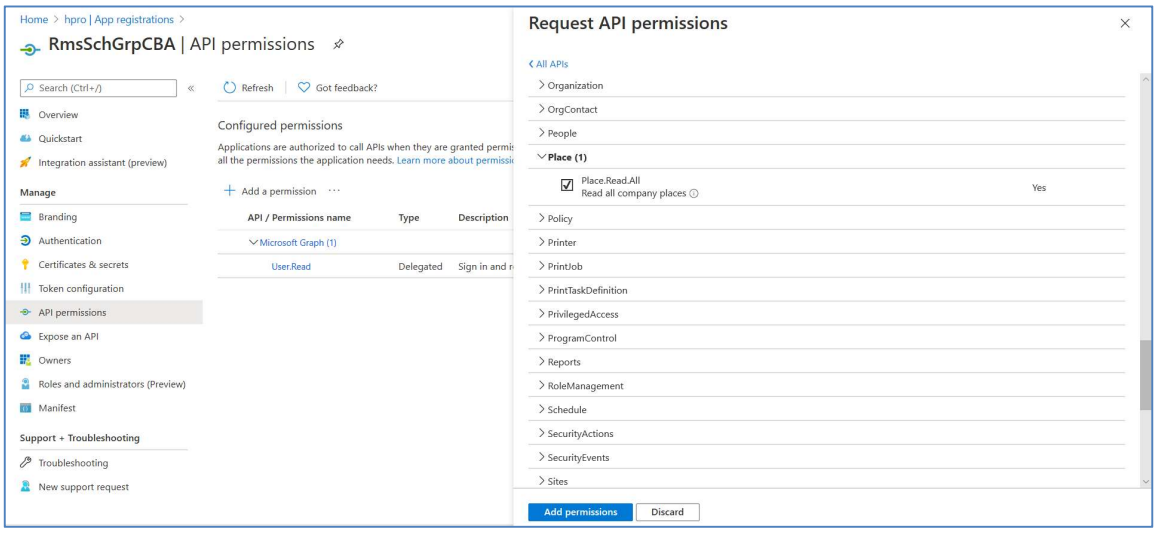
Click on **Microsoft Graph** option from the **Commonly used Microsoft APIs** section



Select the **Application Permissions** option for 'What type of permissions does your application require?'

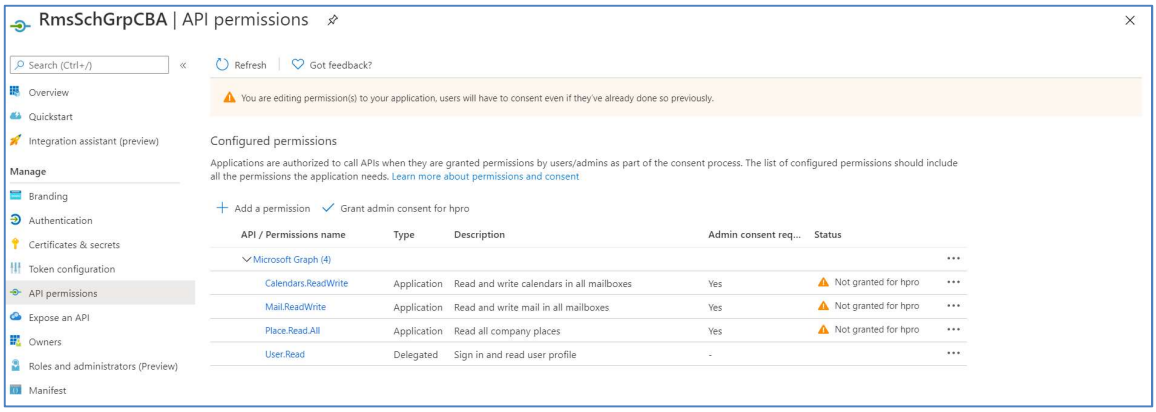
Select the following Permissions:

Calendars > Calendars.ReadWrite
Mail > Mail.ReadWrite
Place > Place.Read.All

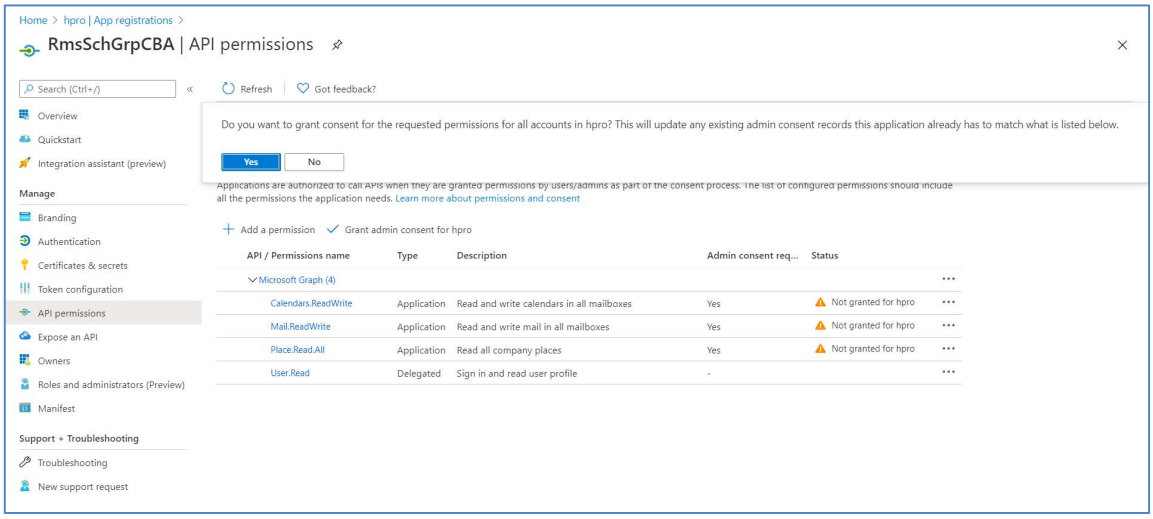


Click **Add Permissions** button

The newly added permissions are saved and listed in **Configured permissions**

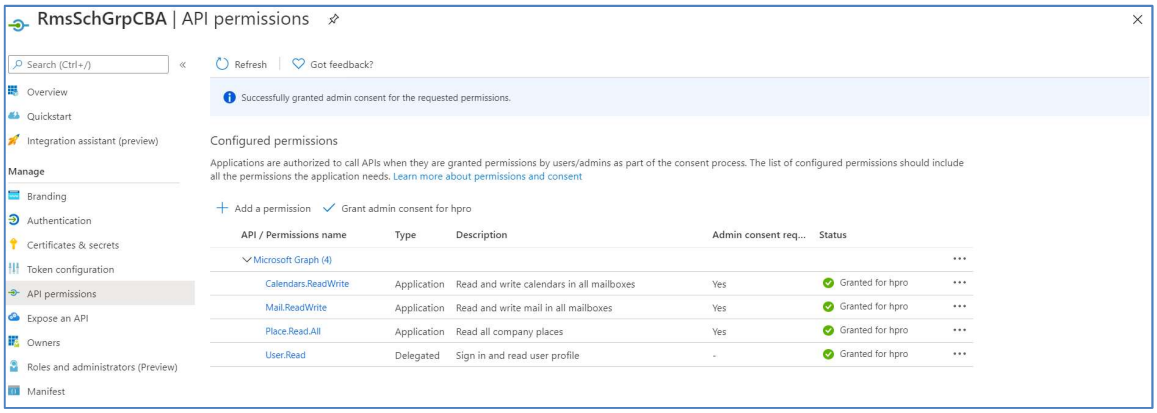


Now, grant admin consent for the requested permissions by clicking **Grant admin consent for <domain name>** button



Click **Yes** button for the confirmation message

Notice that the **Admin consent** granted for the requested permissions



VI. Application Credentials

Credentials enable applications to identify themselves to the authentication service when receiving tokens.

You can use either **Client Secret** or **Certificate** to achieve this, but not both. Section **VII** and **VIII** describes both methods. **Make sure to use anyone.**

VII. Adding Credentials to the Application (Client Secret)

Important NOTE:

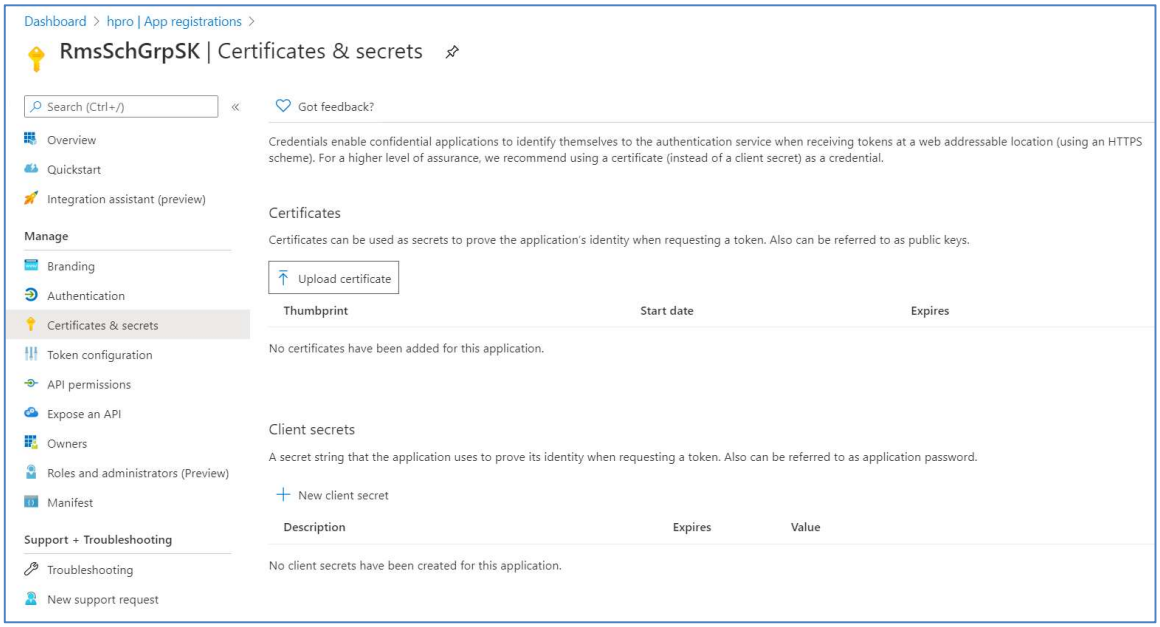
*Skip this step and go to **Adding Credentials to the Application (Client Certificate)** section below to use Certificate based authentication*

For a higher level of assurance, recommended to use a certificate (instead of a client secret) as a credential.

Make sure to create a new application by following the steps defined in **Create your app registration in Azure Active Directory**

In the left navigation menu, select **Certificates & Secrets** from **Manage section of Application Menu Blade**

Certificates & Secrets page opens

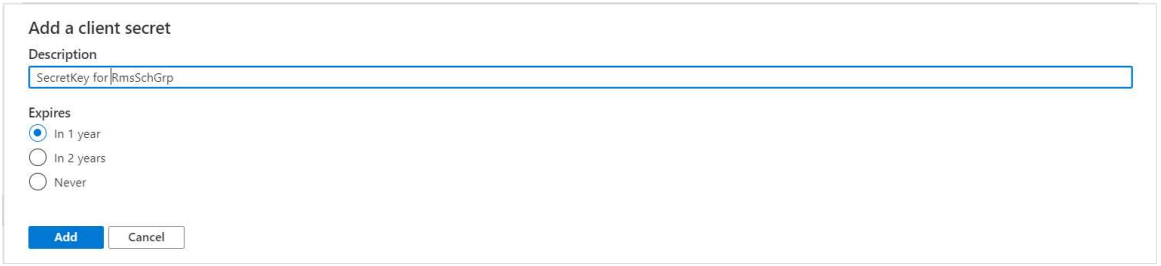


Click **New Client secret** button

Add a client secret dialog opens

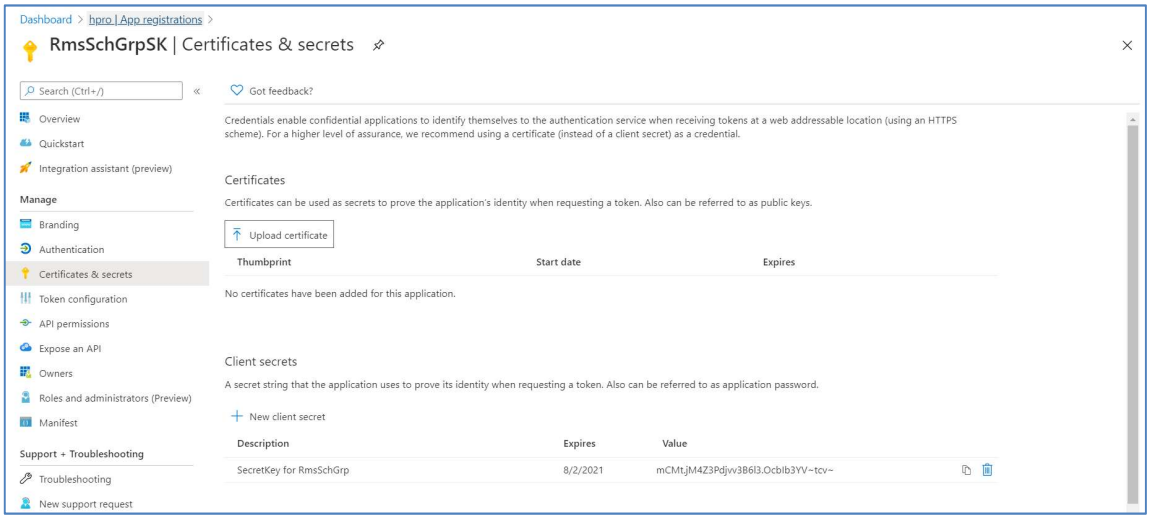
Key-in **Description** for the client secret

Select a value from the **Expires** section as per your need



Click **Add** button

Once the settings are saved, the key is displayed.



Important NOTE:

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this screen.

VIII. Adding Credentials to the Application (Client Certificate)

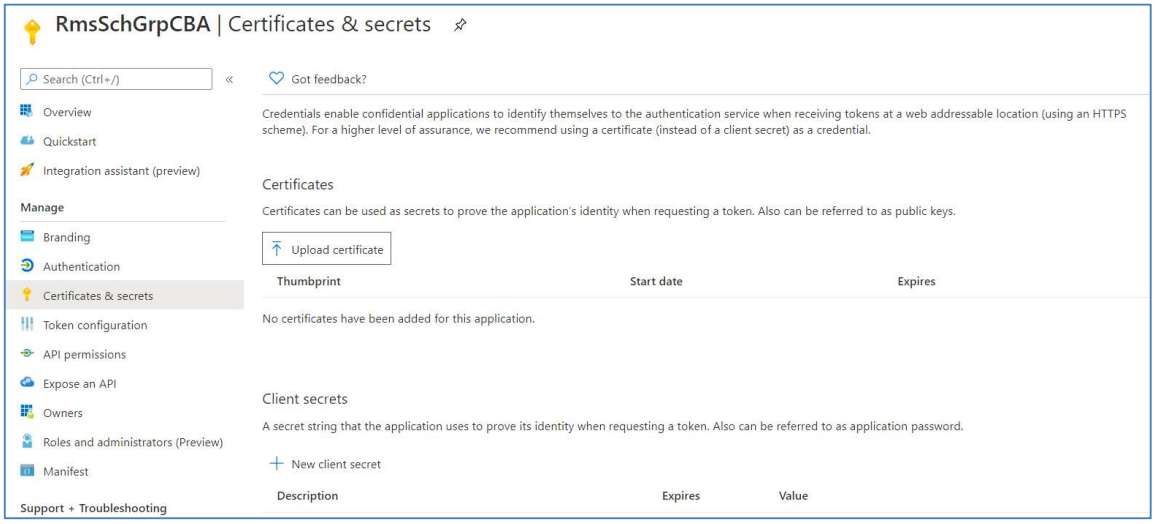
Important NOTE:

*If you have already configured **Adding Credentials to the Application (Client Secret)**, Please skip this step.*

Make sure to create a new application by following the steps defined in **Create your app registration in Azure Active Directory**

In the left navigation menu, select **Certificates & Secrets** from **Manage section of Application Menu Blade**

Certificates & Secrets page opens



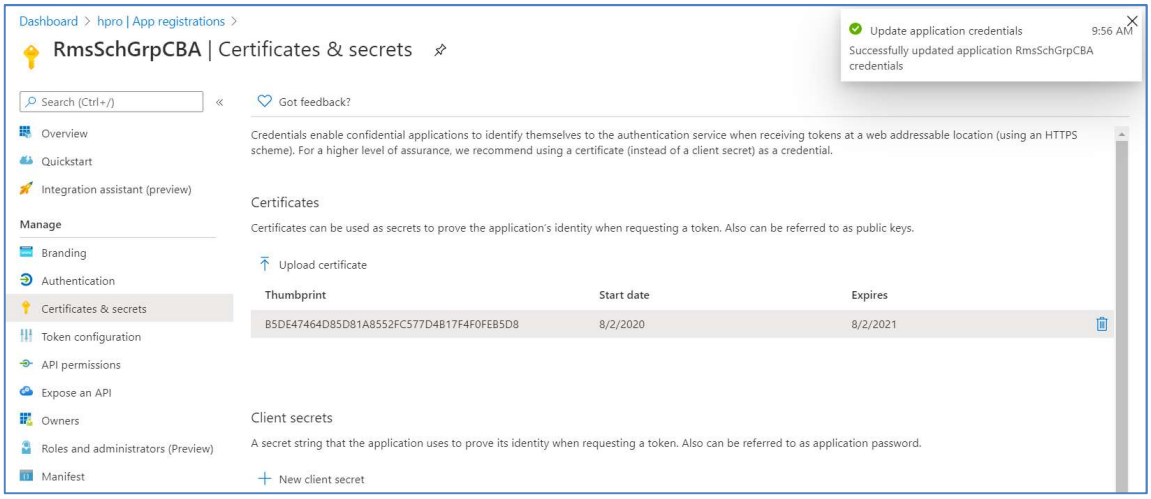
Click **Upload certificate** button

Upload certificate dialog opens. Click on the **Folder** icon to select a certificate file

Select the **.CER** file that exported in section ***Export Certificate - Without Private Key (.CER)***

Click **Add** button

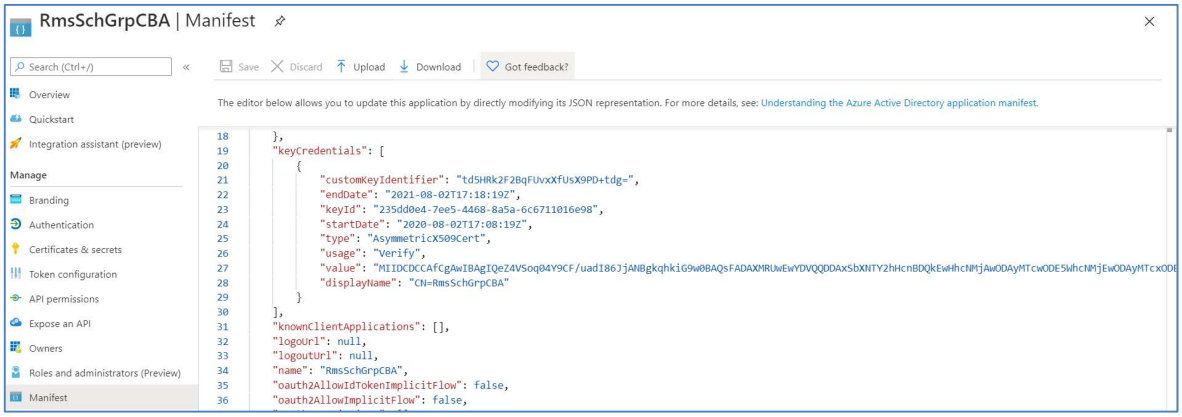
Notice that the uploaded certificate listed under **Certificates** section



IX. Modify the Manifest of Azure AD Application

In the left navigation menu, select **Manifest** from **Manage section of Application Menu Blade**

The editor shown on right side with JSON elements



The editor shown on right side with JSON elements. In the `"keyCredentials":` section, replace the following with the value that we got from section III

```
"customKeyIdentifier": <Base-64 Thumbprint value got from PowerShell Script>
"keyId": <Keyid value got from PowerShell Script>
```

Click **Save** button to save the changes

X. Configuring RMS Scheduling Interface for Exchange – Modern Authentication (Client Secret Key)

Install the latest RMS Scheduler Interface v1.1.2

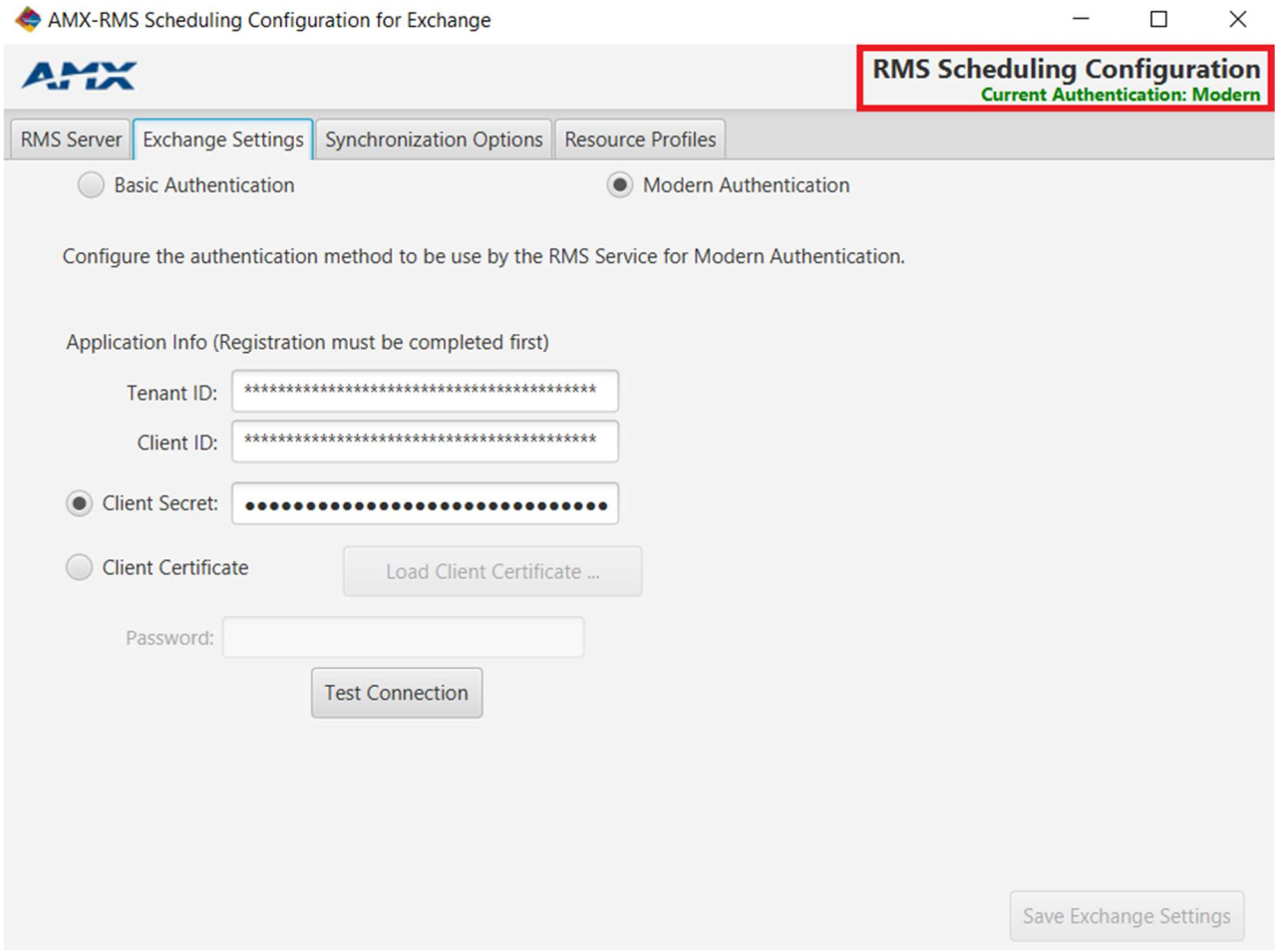
After installation is completed, configure the RMS Server and click **Save RMS Server Setting** to save the settings

Select the **Exchange Settings** tab and choose the **Modern Authentication** radio button option

Key-in the **Tenant ID, Client ID** values that you noted down from the Azure AD App Overview (Refer to section ***Create your App registration in Azure Active Directory***)

Key-in the **Client Secret** key that you copied when you generated (as per the instruction of section ***Adding Credentials to the Application (Client Secret)***)

Click **Test Connection** button. You should see **Connect to Exchange account successfully** message.



Click the **Save Exchange Settings**

When you select **Resource Profile** tab, you should be able to enable the resource profile

Once the **RMS Scheduling Interface** settings are saved and configuration window is closed, you should be able to schedule the meeting by using the Modern Authentication.

XI. Configuring RMS Scheduling Interface for Exchange - Modern Authentication (Certificate Based)

Install the latest RMS Scheduler Interface v1.1.2. After installation is completed, configure the RMS Server and click **Save RMS Server Setting** to save the settings

Select the **Exchange Settings** tab and choose the **Modern Authentication** radio button option

Key-in the **Tenant ID, Client ID** values that you noted down from the Azure AD App Overview (Refer to section ***Create your App registration in Azure Active Directory***)

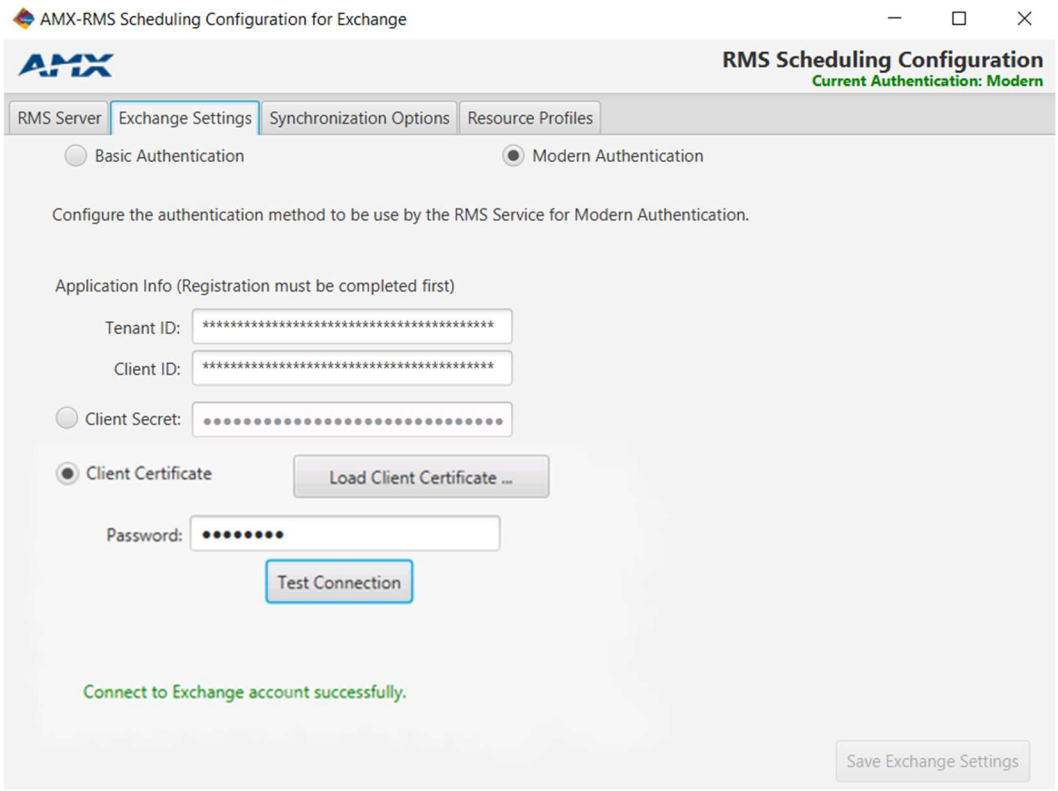
Choose the **Client Certificate** radio button option

Click **Load Client Certificate** button

Select the **.**PFX certificate file that was exported in section ***Export Certificate - With Private Key (.PFX)***

Key in the certificate password that were used during export in **Password** field

Click **Test Connection** button. You should see **Connect to Exchange account successfully** message.



Click the **Save Exchange Settings**

When you select **Resource Profile** tab, you should be able to enable the resource profile

Once the **RMS Scheduling Interface** settings are saved and configuration window is closed, you should be able to schedule the meeting by using the Modern Authentication.

RMS-SCH-EWS Known Issues

The following are known issues relative to RMS-SCH-EWS *RMS Enterprise Scheduling Interface for Exchange*:

- Hybrid Modern Authentication is not currently supported
- Streaming Notifications for Modern Authentication are not supported at this time
- If Exchange Settings are already configured, saving Exchange settings again will re-sync resource profiles from Exchange Server and remove existing mappings from RMS Server.
- For Modern Authentication, newly configured rooms do not immediately report in the Resources tab, as they do not report in a Microsoft Graph query of the rooms. It may take up to 24 hours for Microsoft Graph API to report the new room.
- Each meeting instance in an Exchange recurring meeting series is treated as an individual meeting in RMS.
- Recurring appointments in Exchange that have "No End Date" specified are limited to two years of occurrences synchronized into RMS. After the two years elapses, no further bookings for that series will be synchronized into RMS. It is recommended that recurring appointments either have a specific end date or a number of occurrences defined.
- The RMS Exchange Appointment Organizational Form (used with some previous versions of the Scheduling Interface) is not compatible with the *RMS Enterprise Scheduling Interface for Exchange*.

3000 RESEARCH DRIVE, RICHARDSON, TX 75082 AMX.com | 800.222.0193 | 469.624.8000 | +1.469.624.7400 | fax 469.624.7153
AMX (UK) LTD, AMX by HARMAN - Unit C, Auster Road, Clifton Moor, York, YO30 4GD United Kingdom • +44 1904-343-100 • www.amx.com/eu/

Last Revised:
03/04/2020