



Installation Guide

# NSS-RMS-EWS

RMS Interface for Exchange EWS for RMS v3.x



## **AMX DOMESTIC CHANNEL PARTNER and END CUSTOMER LIMITED WARRANTY, DISCLAIMER AND LICENSE**

(Excerpt from CHANNEL PARTNER TERMS AND CONDITIONS Versions 11.17.2011 with updates for previous version 8.25.2010 [sections 6.1 (a), (b) and (f)])

### **Definitions**

"End Customer" means an authorized end customer with direct in warranty privileges from AMX. Within this limited warranty, disclaimer and license document, "End Customer" shall have the same meaning as "Channel Partner" with the noted exceptions of Sections 6.5 through 6.9 which are not applicable or available to End Customer's directly from AMX. Offerings described in Sections 6.5 through 6.9 are available to End Customer only through their selected authorized AMX Channel Partner.

### **6. LIMITED WARRANTY; RETURN, REPAIR AND REPLACEMENT**

6.1 AMX warrants the Products to be free of material defects in materials and workmanship under normal use for three (3) years from the Shipping Date (or such other period as may be specified below), subject to the following limitations and exceptions ("Limited Warranty"). For any Product, "Warranty Period" means the period during which the Limited Warranty is in effect, as set forth herein.

- (a) LCD and LED panels are warranted for three (3) years from the Shipping Date, except for the display and touch overlay components, which are warranted for a period of one (1) year from the Shipping Date.
- (b) Disk drive mechanisms, pan/tilt heads and external power supplies are warranted for a period of one (1) year from the Shipping Date.
- (c) AMX lighting Products are warranted to switch on and off any load that is properly connected to our lighting Products, as long as the AMX lighting Products are under warranty. AMX also warrants the control of dimmable loads that are properly connected to our lighting Products. The dimming performance or quality thereof is not warranted, due to the random combinations of dimmers, lamps and ballasts or transformers.
- (d) AMX software and firmware included in the Products is warranted for a period of ninety (90) days from the Shipping Date.
- (e) Batteries and incandescent lamps are not covered under the Limited Warranty.
- (f) The Warranty Period for AMX AutoPatch EPICA, Enova DGX, Modula, Modula Series 4, Modula Cat Pro Series and 8Y-3000 Product models will continue for the original installation until five (5) years after the issuance of a PDN with respect to termination of the applicable Product model. However, if the Product is moved from its original installation to a different installation, the Warranty Period will automatically become three (3) years from the Shipping Date and, if more than three (3) years have elapsed since the Shipping Date, the Warranty Period will automatically expire.

DLI-6293353v1

**Note:** Refer to [www.amx.com](http://www.amx.com) to view/download the latest complete AMX Warranty and Return Policies.

# Table of Contents

<b>RMS v3.x Interface for Exchange EWS</b> .....	<b>1</b>
Overview .....	1
Microsoft Exchange Server Requirements .....	1
RMS Version Requirements.....	1
Installation Checklist .....	1
<b>Creating a Room Mailbox (Exchange 2010)</b> .....	<b>3</b>
Overview .....	3
Creating a New Room Mailbox .....	3
<b>RMS Exchange EWS Plug-in Configuration</b> .....	<b>9</b>
Overview .....	9
Registering the Exchange EWS Appointment Interface .....	9
Certificate Validation .....	15
RMS Settings - Synchronization Window and Blackout Period .....	16
Completing the Configuration Wizard.....	16
<b>Associating Exchange Mailboxes with RMS Rooms</b> .....	<b>17</b>
Overview .....	17
<b>Configuring the RMS Service Account (Exchange 2010)</b> .....	<b>21</b>
Overview .....	21
Configuring the RMS Service Account .....	21
Assigning the RMS Account As a Delegate To the Room Mailbox .....	21
Assigning Full-access Permission To the RMS account .....	21
Assigning the Exchange Impersonation Role to the RMS account .....	21
Enabling Impersonation for a Single Account .....	21
Enabling Impersonation for Multiple Accounts .....	21
Adding Accounts to the New RoleGroup.....	21
Create the Impersonation RoleAssignment for the RoleGroup.....	22
Limiting Impersonation to Mailboxes that will be Synchronized with RMS.....	22
<b>Configuring RMS to use Microsoft.NET Framework v4</b> .....	<b>23</b>
Overview .....	23
Specifying the ASP.NET Version for IIS 6 .....	23
<b>Known Issues</b> .....	<b>25</b>
Overview .....	25



# RMS v3.x Interface for Exchange EWS

## Overview

The *RMS Interface for Exchange EWS* (NSS-RMS-EWS) utilizes Microsoft's Exchange Web Services API to communicate with Exchange 2010 and 2007 servers.

NSS-RMS-EWS is intended for use with RMS version 3.x.

If you are using the Appointment Management features of the RMS application to synchronize RMS room schedules with Exchange servers, some additional configuration is needed:

- Each room in the RMS application that has a schedule needs to be associated with an Exchange Room Mailbox.
- In order for RMS to synchronize appointments with Exchange, the account used by RMS must have the ability to add, modify, and cancel appointments in the Exchange Room Mailboxes that will be associated with RMS rooms. This may be accomplished through delegation, full-access permissions, or *Exchange Impersonation*.



NOTE

*The Network Administrator should perform this installation. The RMS Interface for Exchange EWS will not work unless all of the requirements indicated in this document are met.*

## Microsoft Exchange Server Requirements

- Microsoft Exchange 2010 up to and including SP3
- Microsoft Exchange 2007 updated to SP1 or greater



NOTE

*The certificate used for authentication must exist in either the "Personal" or "Trusted People" folders in the **Local Machine Store** (see the *Registering the Exchange EWS Appointment Interface* section on page 9).*

## RMS Version Requirements

- RMS version **3.3.93**

## Installation Checklist

The following requirements must be met in order to ensure a successful deployment of the *RMS Interface for Exchange EWS*:

1. Each RMS room must be associated with an Exchange Room Mailbox. See the *Creating a Room Mailbox (Exchange 2010)* section on page 3, and the *Associating Exchange Mailboxes with RMS Rooms* section on page 17 for details.
2. In order for RMS rooms to synchronize with the Exchange Room Mailboxes, the RMS plug-in must add, modify, and cancel appointments using a domain account with one of the following access methods enabled: *Delegate access*, *Full access permissions*, or *Exchange Impersonation*. See the *Configuring the RMS User Account* section on page 9 for instructions.
3. The RMS website (UI) must be configured to use version 4 of the Microsoft.NET Framework. See the *Configuring RMS to use Microsoft.NET Framework v4* section on page 10 for instructions.
4. The following information must be available to complete initial plugin configuration:
  - The Exchange Server Web Service URL
  - Authentication credentials for the RMS Service Account (Windows domain account) - this can be either of the following:
    - The User ID, Password and Domain of the RMS Service Account
    - A locally-installed X.509 certificate mapped to the RMS Service Account



# Creating a Room Mailbox (Exchange 2010)

## Overview

Microsoft Exchange 2010 provides support for mailboxes that are used to manage meeting room schedules. The instructions in this section describe how to create an Exchange Room Mailbox.



NOTE

Appropriate administrator access is required to perform these tasks.

## Creating a New Room Mailbox

1. Select **Microsoft Exchange Server 2010 > Exchange Management Console** to launch the *Exchange Management Console* utility (FIG. 1).

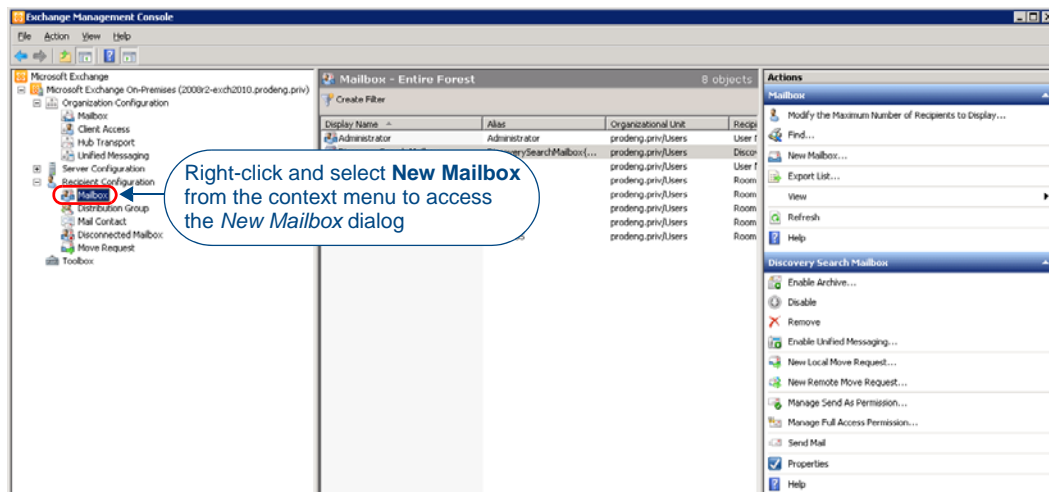


FIG. 1 Exchange Management Console

2. In the left-side window under *Recipient Configuration*, right-click on **Mailbox** and select **New Mailbox** from the context menu (FIG. 2):

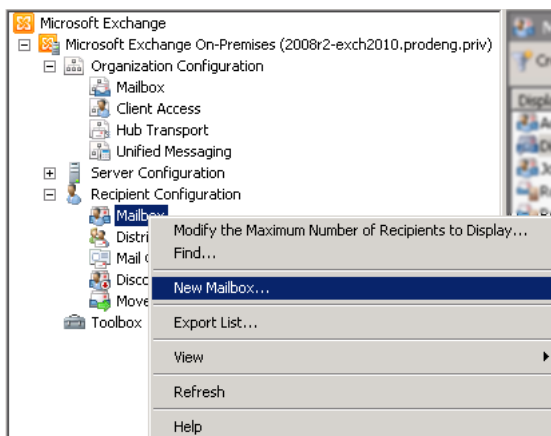


FIG. 2 Exchange Management Console

This selection opens the *New Mailbox - Introduction* dialog (FIG. 3):

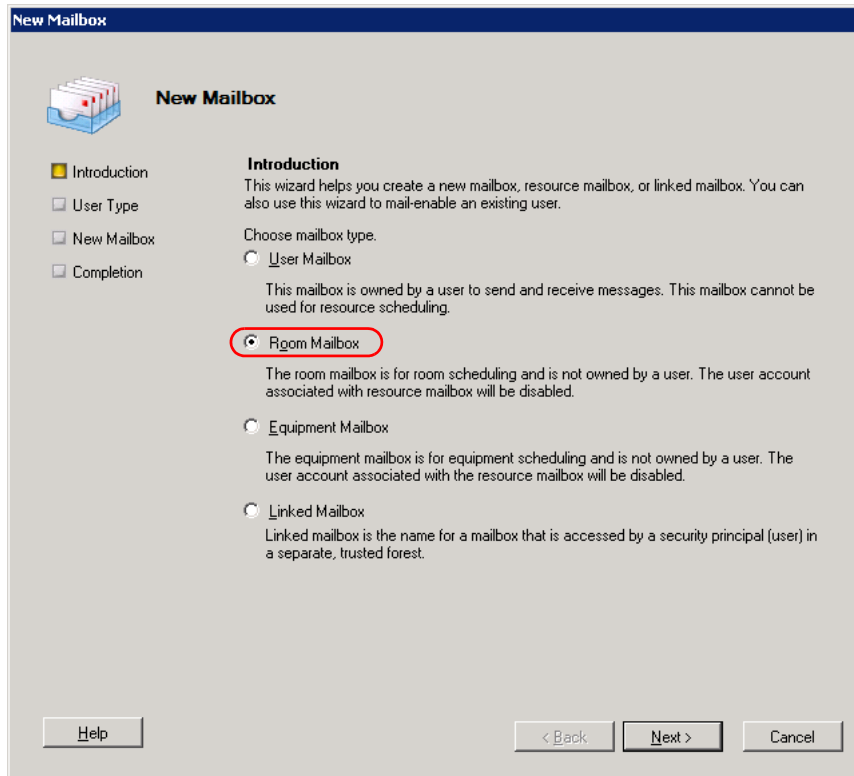


FIG. 3 New Mailbox - Introduction dialog

3. Select **Room Mailbox**, and click **Next** to proceed to the *New Mailbox - User Type* dialog (FIG. 4):

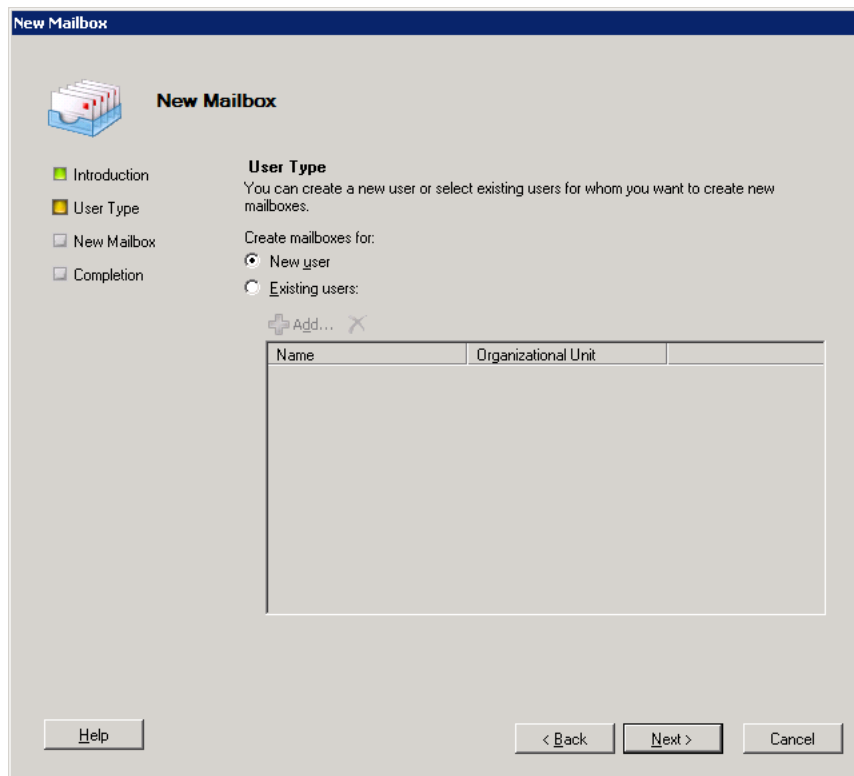


FIG. 4 New Mailbox - User Type dialog



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 (FIG. 5):

**FIG. 5** 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 (FIG. 6):

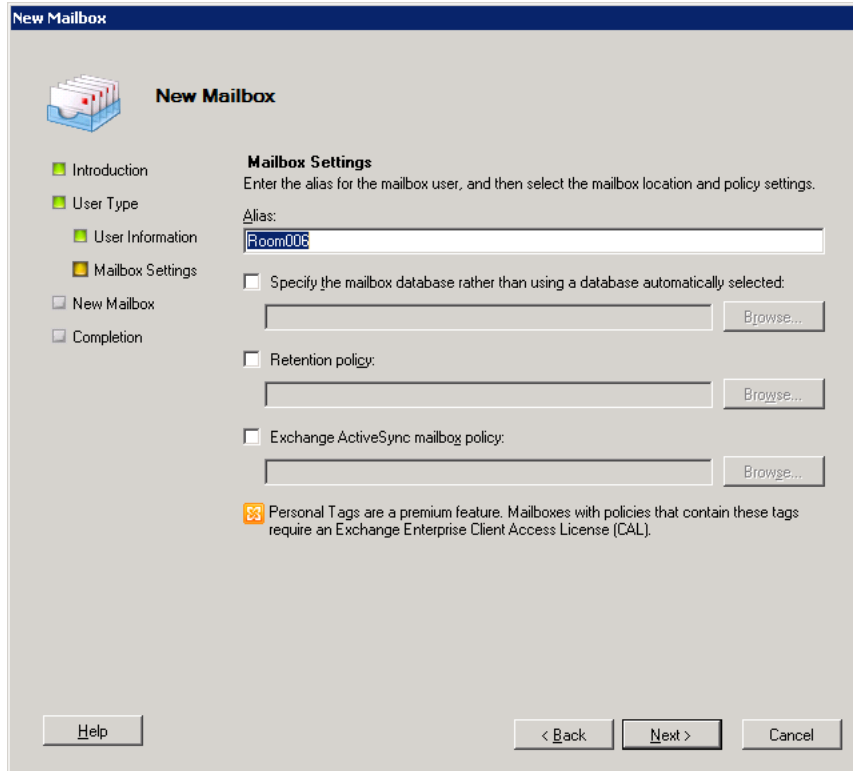


FIG. 6 New Mailbox - Mailbox Settings dialog

7. In most cases, the default settings in this dialog are sufficient - click **Next** to proceed to the *New Mailbox New Mailbox (Confirmation Summary)* dialog (FIG. 7):

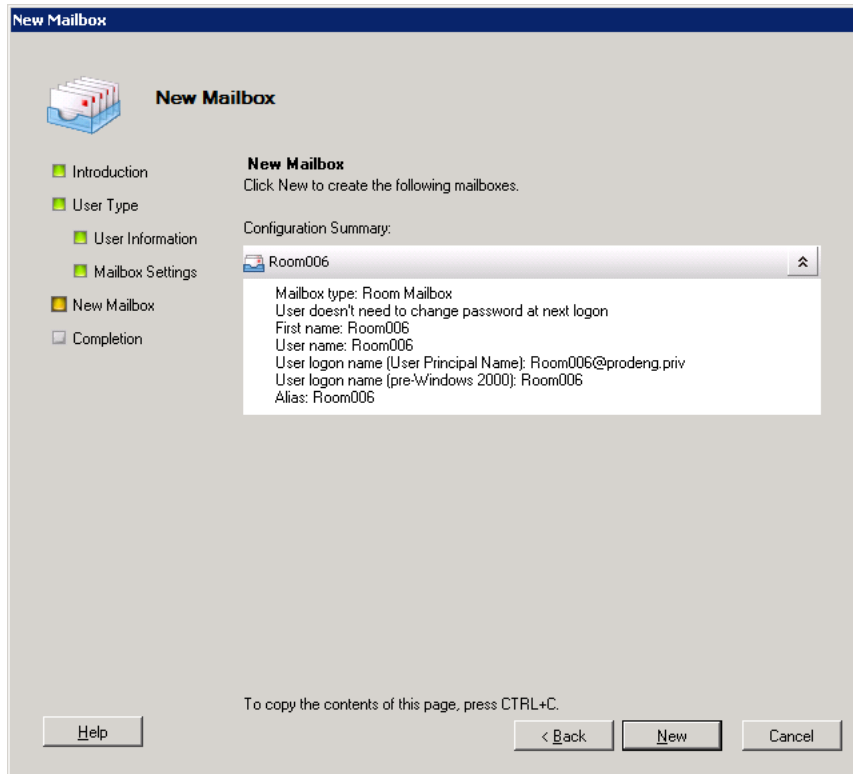


FIG. 7 New Mailbox - New Mailbox (Confirmation Summary) dialog

- Use this dialog to review the information entered.
- To copy the summary information presented on this page, click CTRL+C.

8. Click **New** to create the new Mailbox, and proceed to the *New Mailbox - Completion* dialog (FIG. 8):

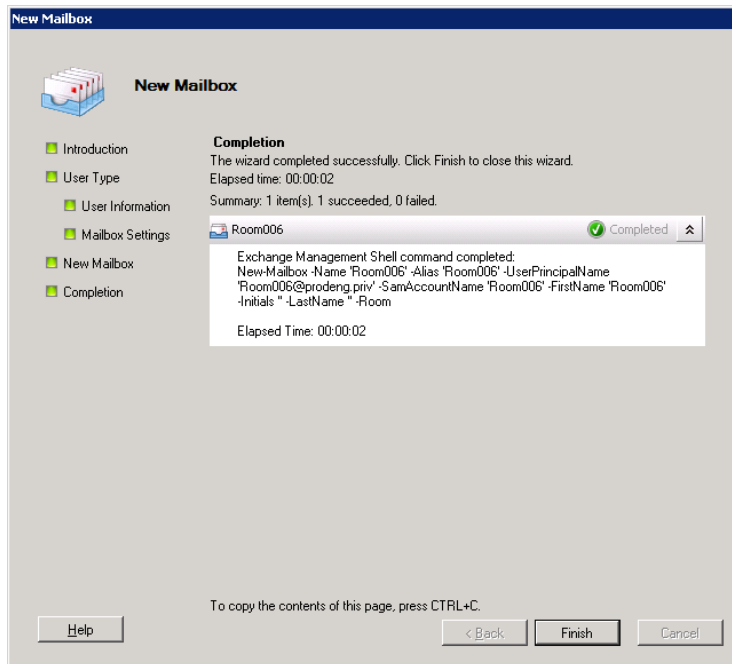


FIG. 8 New Mailbox - Completion dialog

9. Click **Finish**.

Proceed to the next section, and follow all of the instructions for *Configuring the RMS Service Account*.



# RMS Exchange EWS Plug-in Configuration

## Overview

To use the *RMS Interface for Exchange EWS* scheduling plug-in, it must first be registered. Only a single scheduling plug-in should be registered at one time.



NOTE

The RMS application must be configured for External Scheduling Systems for the scheduling plug-in configuration dialog to be displayed.

The plug-in configuration is performed in the Resource Management Configuration Wizard under the *System Settings*, *Scheduling* node of the navigation tree (FIG. 9).

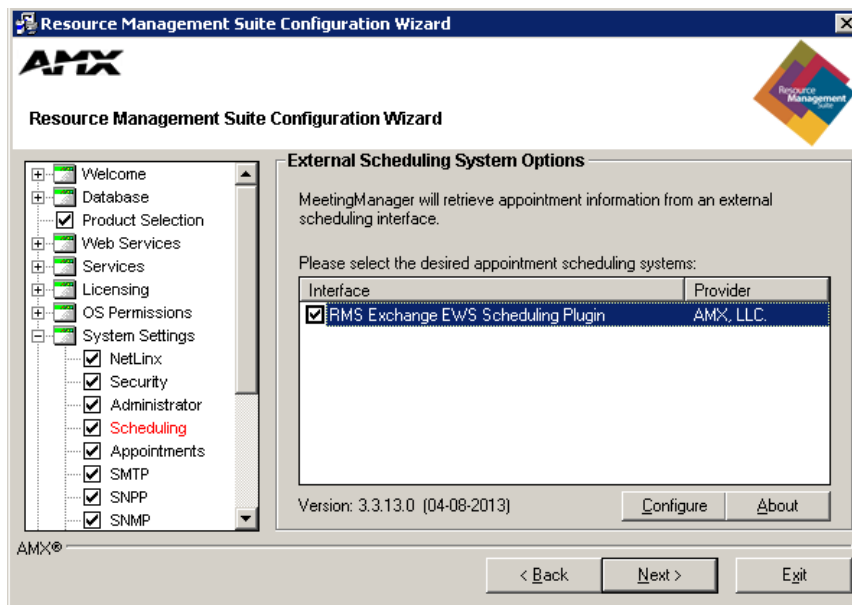


FIG. 9 RMS Configuration Wizard - External Scheduling System Options

## Registering the Exchange EWS Appointment Interface



NOTE

The *RMS Interface for Exchange EWS* communicates with a single Exchange Server.

To register the *Exchange EWS Appointment Interface*:

1. Place a checkmark in the box to the left of the *RMS Exchange EWS Scheduling Plugin* entry in the scheduling systems plug-in list.
2. Click **Configure** to invoke the *Exchange Web Services Scheduling Plugin Configuration* dialog - **Server connection settings** tab. Use the options in this tab to configure the Exchange Server Web Service URL and Authentication credentials (FIG. 10).

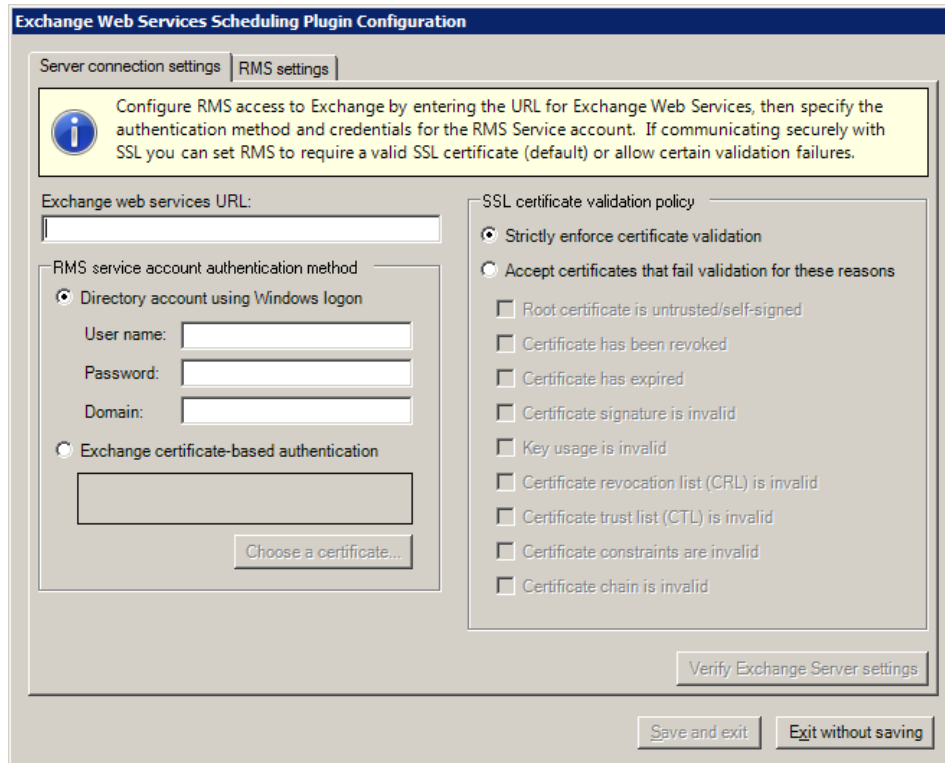


FIG. 10 Exchange Web Services Scheduling Plugin Configuration dialog - Server Connection Settings tab

The RMS service account must be validated with the EWS web services URL prior to saving plugin settings.

FIG. 11 displays how the config dialog should look when the RMS service account uses standard Windows logon to authenticate:

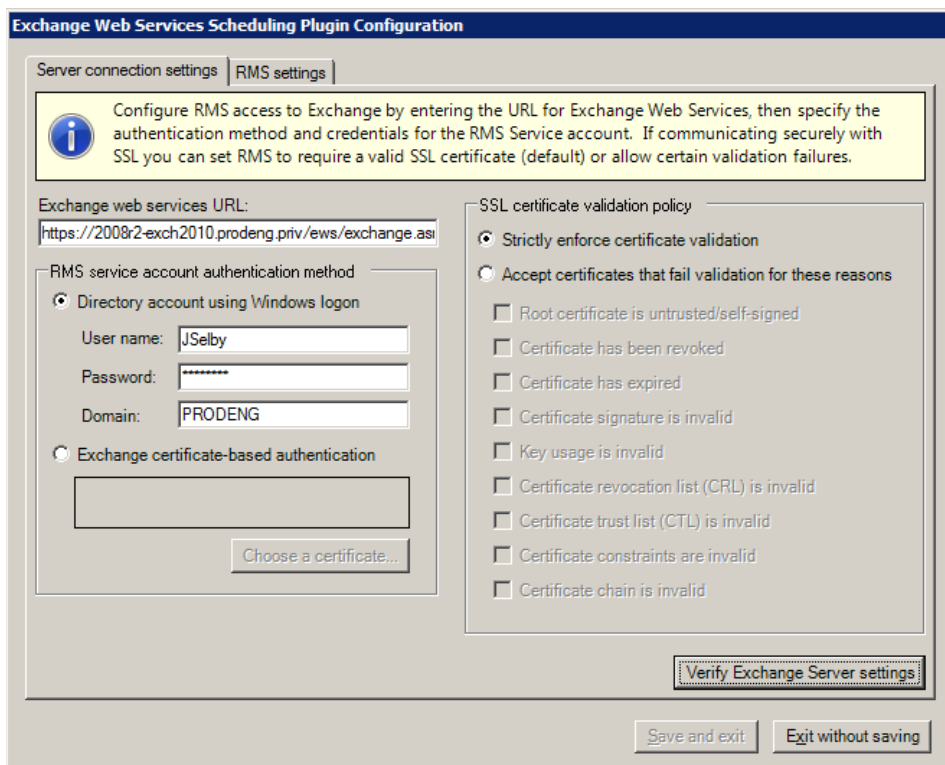


FIG. 11 Exchange Web Services Scheduling Plugin Configuration dialog - Server Connection Settings tab

- The **Save and Exit** button is disabled until all required options have been configured *and validated*.
  - The **Verify Exchange Server settings** button is enabled once the web services URL and logon parameters have been entered.
3. Click **Verify Exchange Server settings** to ensure the Web Service URL and Authentication Credentials are valid. This action invokes the dialog shown below (FIG. 12), and user input to the config dialog is blocked:

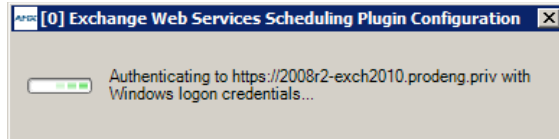


FIG. 12 Exchange Web Services Scheduling Plugin Configuration - Busy: Windows Authentication

4. If authentication succeeds then the plugin checks for the existence of mailbox room lists (FIG. 13):

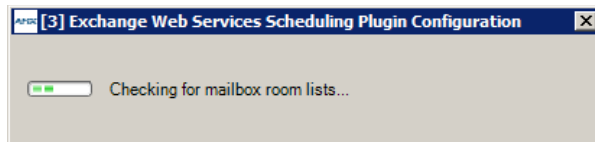


FIG. 13 Exchange Web Services Scheduling Plugin Configuration - Checking for Mailbox Room Lists

- The dialog shown in FIG. 14 is displayed after successful authentication *and detection* of one or more mailbox room lists:

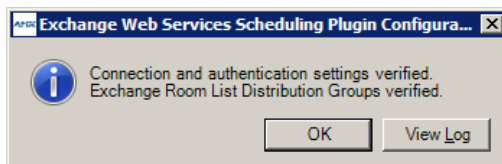


FIG. 14 Exchange Web Services Scheduling Plugin Configuration - Authentication Successful

- The dialog in FIG. 15 is displayed after successful authentication *and failure to detect any mailbox room lists*:

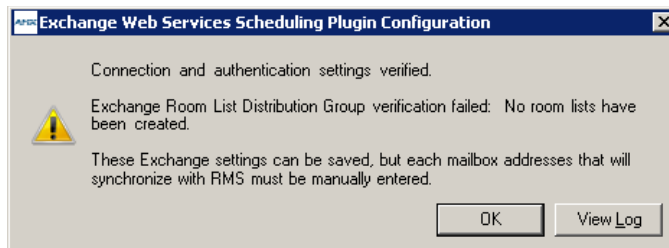


FIG. 15 Exchange Web Services Scheduling Plugin Configuration - Authentication Successful, no Mailbox Room Lists detected



NOTE

*Version 3.3.13 (or higher) of the EWS plugin supports certificate-based authentication.*

5. To choose a certificate, click **Choose a certificate...** (FIG. 16):

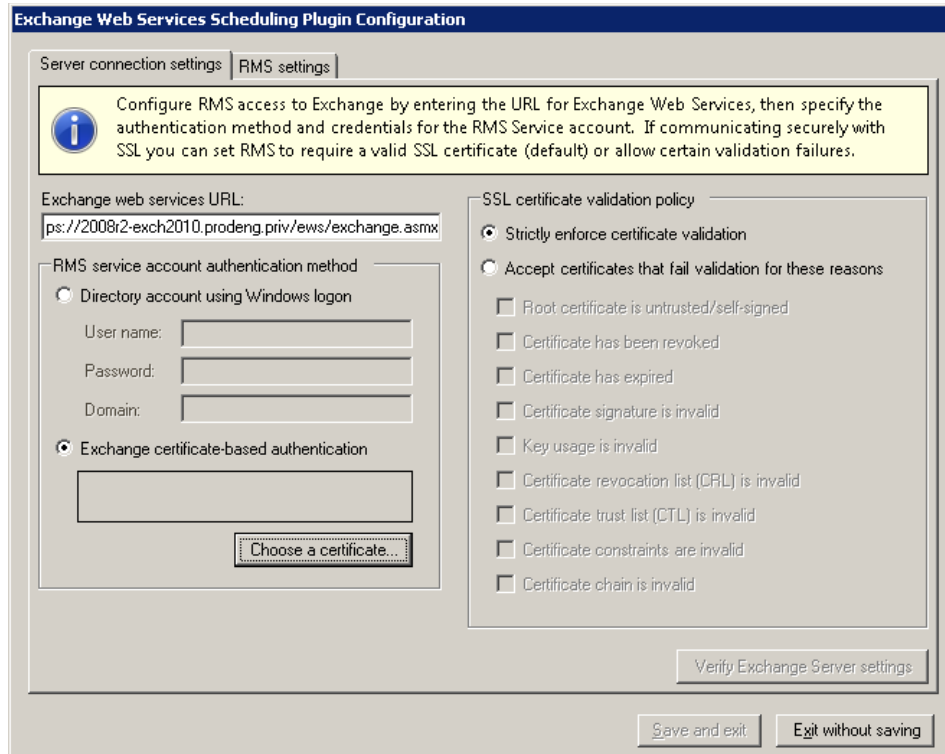


FIG. 16 Exchange Web Services Scheduling Plugin Configuration dialog - Server Connection Settings tab

- All certificates installed in the "Personal" and "Trusted People" folders in the Local Machine Store will be available for selection.
- The certificate used for authentication must exist in either the "Personal" or "Trusted People" folders in the Local Machine Store.
- The *Exchange Web Services Scheduling Plugin Configuration* dialog **will not manage certificate requests or installation**; certificate management is built in to Windows.

6. Select a Certificate in the *Certificate Selection* dialog (FIG. 17):

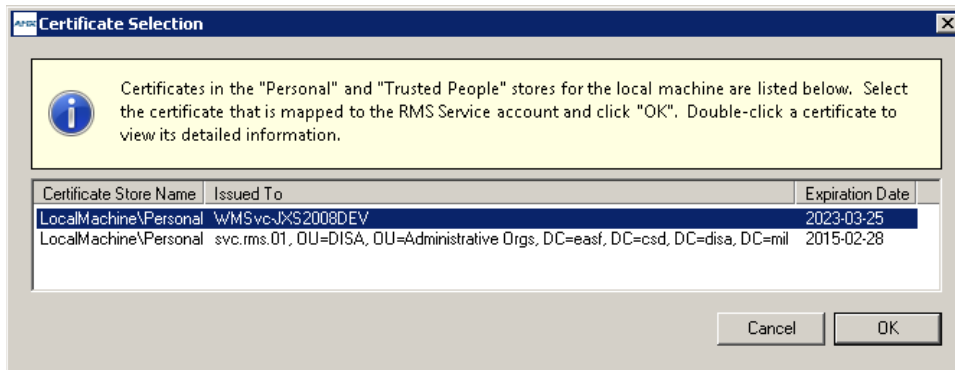


FIG. 17 Certificate Selection dialog



*Only one certificate at a time can be selected.*

7. Double-click a certificate to display its details in the *Certificate* dialog (FIG. 18):



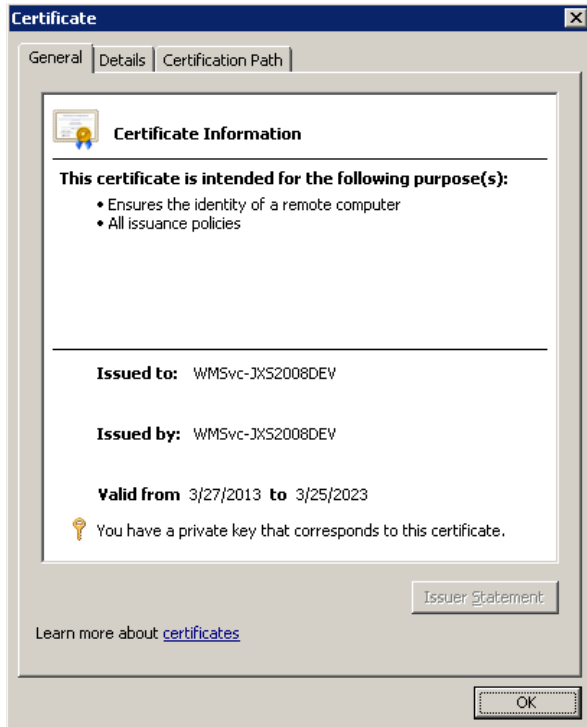


FIG. 18 Certificate dialog

8. Click **OK** to select a Certificate and close the *Certificate Selection* dialog.

When a certificate has been chosen its store path is displayed in the *Exchange Web Services Scheduling Plugin Configuration* dialog - **Exchange Services URL** field (FIG. 19):

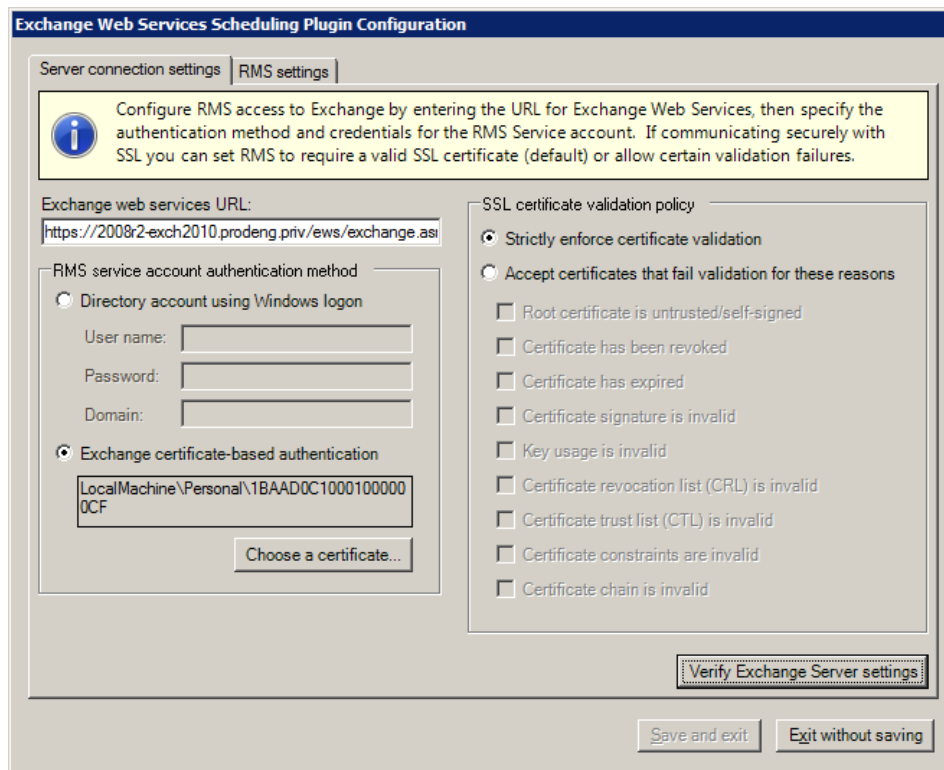


FIG. 19 Exchange Web Services Scheduling Plugin Configuration dialog - Server Connection Settings tab



The config dialog does not export to disk or otherwise store a binary copy of the selected certificate - only the path into the computer's certificate store is saved. When the plugin is loaded it will use this path to extract the actual certificate from the cert store.

- Click **Verify Exchange Server settings**. This action invokes the following dialog (FIG. 20), and user input to the config dialog is blocked.

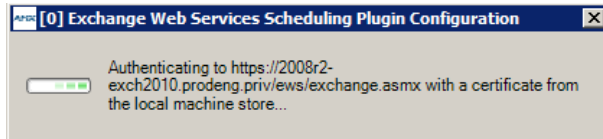


FIG. 20 Exchange Web Services Scheduling Plugin Configuration dialog - Authenticating

- If authentication succeeds then the plugin checks for the existence of mailbox room lists (FIG. 21):

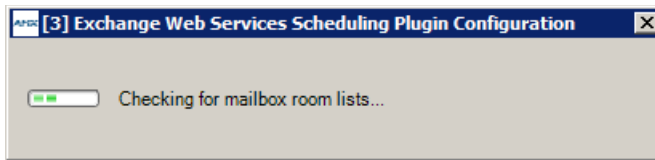


FIG. 21 Exchange Web Services Scheduling Plugin Configuration dialog - Checking for Mailbox Lists

- The following dialog is displayed after successful *authentication and detection* of one or more mailbox room lists (FIG. 22):

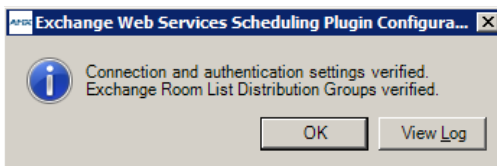


FIG. 22 Exchange Web Services Scheduling Plugin Configuration dialog - Authentication Successful

- The following dialog is displayed after successful *authentication and failure to detect* any mailbox room lists (FIG. 23):

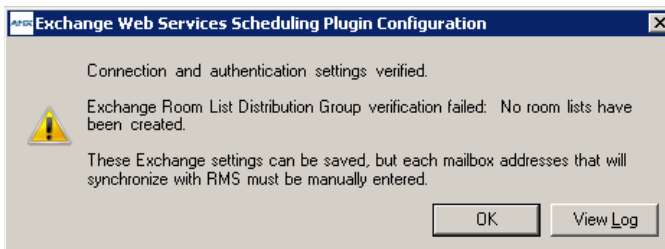


FIG. 23 Exchange Web Services Scheduling Plugin Configuration dialog - Authentication Failed

## Certificate Validation

By default, the RMS Interface for Exchange EWS requires strict validation of the Exchange server's SSL certificate for encrypted connections. If the certificate fails validation for any reason then the RMS Interface for Exchange EWS will immediately disconnect and log the specific failure(s).

The most common certificate validation failure - *"Root certificate is untrusted/self-signed"* - is caused by installing a self-signed SSL certificate on the Exchange server. If self-signed certificates are acceptable then this validation failure may be ignored by checking the *"Root certificate is untrusted/self-signed"* option as shown in FIG. 24:

The screenshot shows the 'Exchange Web Services Scheduling Plugin Configuration' dialog box with the 'RMS settings' tab selected. A yellow information box at the top states: 'Configure RMS access to Exchange by entering the URL for Exchange Web Services, then specify the authentication method and credentials for the RMS Service account. If communicating securely with SSL you can set RMS to require a valid SSL certificate (default) or allow certain validation failures.' Below this, the 'Exchange web services URL' field contains 'https://2008r2-exch2010.prodeng.priv/ews/exchange.asi'. The 'RMS service account authentication method' section has 'Directory account using Windows logon' selected, with 'User name' set to 'JSelby', 'Password' masked with asterisks, and 'Domain' set to 'PRODENG'. The 'Exchange certificate-based authentication' option is unselected. The 'SSL certificate validation policy' section has 'Accept certificates that fail validation for these reasons' selected, and the 'Root certificate is untrusted/self-signed' checkbox is checked. Other checkboxes for 'Certificate has been revoked', 'Certificate has expired', 'Certificate signature is invalid', 'Key usage is invalid', 'Certificate revocation list (CRL) is invalid', 'Certificate trust list (CTL) is invalid', 'Certificate constraints are invalid', and 'Certificate chain is invalid' are all unselected. At the bottom right, there are buttons for 'Verify Exchange Server settings', 'Save and exit', and 'Exit without saving'.

**FIG. 24** Exchange Web Services Scheduling Plugin Configuration dialog - Allowing self-signed SSL certificates

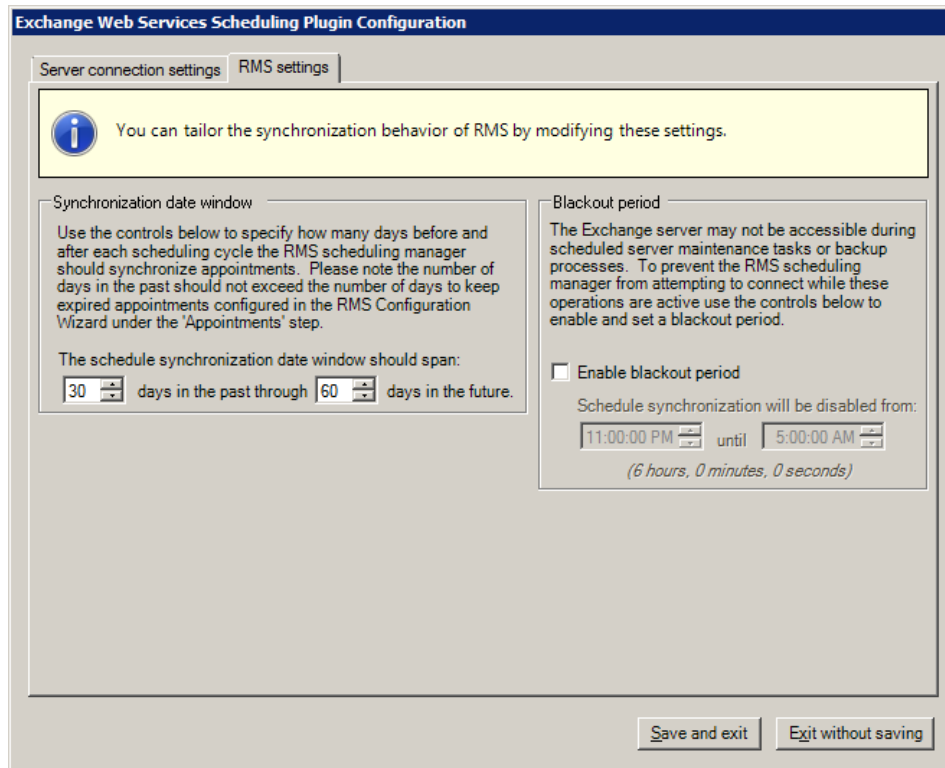


NOTE

*Ignoring failure(s) other than "Root certificate is untrusted/self-signed" or disabling certificate validation altogether (by allowing all failures) is not recommended. These options should only be enabled when troubleshooting occasional SSL connection issues.*

## RMS Settings - Synchronization Window and Blackout Period

1. Open the *Exchange Web Services Scheduling Plugin Configuration* dialog - **RMS settings** tab (FIG. 25):



**FIG. 25** Exchange Web Services Scheduling Plugin Configuration dialog - RMS Settings tab

2. Use the options under *Synchronization Data Window* to configure the date window for RMS to synchronize Exchange appointments:
  - **Number of days in the past:** Set the number days (prior to the current date) that RMS should query and synchronize Exchange appointments.  
Note that this number should not exceed the number of days to keep appointments configured in the RMS Configuration Wizard (under the *Appointments* step).  
Default = 30
  - **Number of days in the future:** Set the number of days after the current date that RMS should query and synchronize Exchange appointments.  
Default = 60
3. Use the options under *Blackout Period* to configure a scheduled synchronization/trolling blackout period. 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.
  - This option is enabled by default and is recommended.
  - You may change the time frame to accommodate your specific environment.

### Completing the Configuration Wizard

After you set all the appropriate plug-in settings, click **OK** to complete the plug-in configuration. You can return to this configuration at any time using the Configuration Wizard, selecting this plug-in from the list, and clicking the **Configure** button.

# Associating Exchange Mailboxes with RMS Rooms

## Overview

Before an RMS room can synchronize with Exchange, the room must be associated with an Exchange Room Mailbox. In the web administrative interface, when you add a new room or modify an existing room, you are provided with *Exchange EWS Scheduling Configuration* options (FIG. 26)

**Modify Room Settings**

**Room Information**

Name: Joe's Place  
 Group: (Default Group)  
 Location: AMX Dallas  
 Owner: AMX Corp.  
 System: Joe's Place

**Room Properties**

Timezone: (GMT-06:00) Central Time (US & Canada)  
 Use Daylight Savings: Yes  
 Prestige Level: Platinum  
 Number of Seats: 0  
 Phone Number: 214.349.2112  
 Equipment List:  
 URL to Map of Room: Open  
 Web Control URL: 192.168.243.91 Open

**Licensing Information**

Asset License: 1234-56-78-9AB-100-FG3002-18 (99 remaining)  
 Scheduling License: 1234-56-78-9AB-100-FG3002-19 (99 remaining)

**Exchange EWS Scheduling Configuration**

Mailboxes in Room Lists: RMS Room List/MeetingRoom003@prodeng.priv  
 Room Mailbox Email Address: Test

Save Cancel

**FIG. 26** Room Scheduling Settings



*The RMS application will not access emails, tasks, notes, etc.*

The Exchange room mailbox may be chosen in one of two ways:

1. Room mailboxes that are members of a room distribution list may be selected from the *Mailboxes in Room Lists* drop-down list (FIG. 27):

**Modify Room Settings**

**Room Information**

Name: Joe's Place  
 Group: (Default Group)  
 Location: AMX Dallas  
 Owner: AMX Corp.  
 System: Joe's Place

**Room Properties**

Timezone: (GMT-06:00) Central Time (US & Canada)  
 Use Daylight Savings: Yes  
 Prestige Level: Platinum  
 Number of Seats: 0  
 Phone Number: 214.349.2112  
 Equipment List:  
 URL to Map of Room: Open  
 Web Control URL: 192.168.243.91 Open

**Licensing Information**

Asset License: 1234-56-78-9AB-100-FG3002-18 (99 remaining)  
 Scheduling License: 1234-56-78-9AB-100-FG3002-19 (99 remaining)

**Exchange EWS Scheduling Configuration**

Mailboxes in Room Lists: RMS Room List/MeetingRoom003@prodeng.priv  
 Room Mailbox Email Address: RMS Room List/MeetingRoom001@prodeng.priv  
 RMS Room List/MeetingRoom002@prodeng.priv  
 RMS Room List/MeetingRoom003@prodeng.priv  
 RMS Room List/MeetingRoom004@prodeng.priv

Save Cancel

**FIG. 27** Modify Room Settings - "Mailboxes in Room Lists" drop-down list

2. In Exchange 2007 organizations or for Exchange 2010 organizations not using room distribution lists the room mailbox SMTP address must be manually entered in the *Room Mailbox Email Address* text field (FIG. 28):

**Modify Room Settings**

**Room Information**

Name: Joe's Place  
 Group: (Default Group)  
 Location: AMX Dallas  
 Owner: AMX Corp.  
 System: Joe's Place

**Room Properties**

Timezone: (GMT-06:00) Central Time (US & Canada)  
 Use Daylight Savings: Yes  
 Prestige Level: Platinum  
 Number of Seats: 0  
 Phone Number: 214.349.2112  
 Equipment List:  
 URL to Map of Room: Open  
 Web Control URL: 192.168.243.91 Open

**Licensing Information**

Asset License: 1234-56-78-9AB-100-FG3002-18 (99 remaining)  
 Scheduling License: 1234-56-78-9AB-100-FG3002-19 (99 remaining)

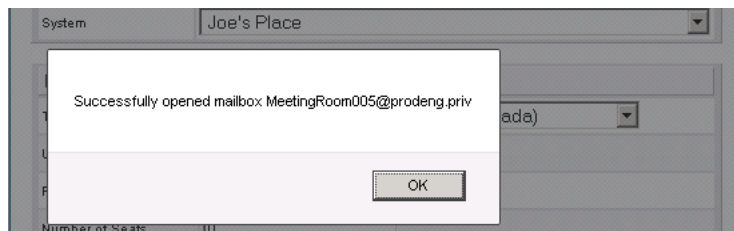
**Exchange EWS Scheduling Configuration**

Mailboxes in Room Lists: RMS Room List/MeetingRoom003@prodeng.priv  
 Room Mailbox Email Address: MeetingRoom005@prodeng.priv  
 Test  
 Save Cancel

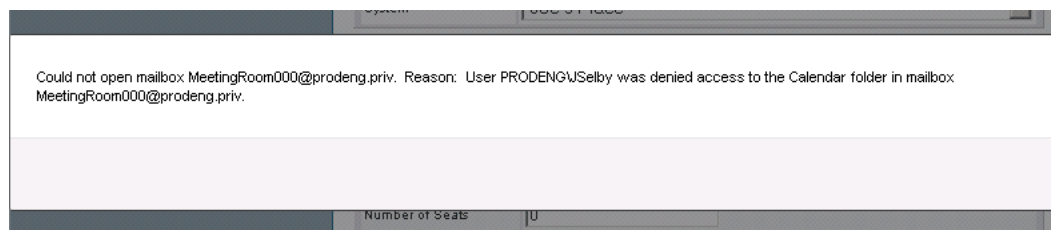
Click to verify that the RMS service account can access the room mailbox email address

**FIG. 28** Modify Room Settings - "Room Mailbox Email Address" field

After choosing a room mailbox verify the RMS service account can access it by clicking the **Test** button (FIG. 29):



**FIG. 29** Modify Room Settings - Test (Success)



**FIG. 30** Modify Room Settings - Test (Failed)





# Configuring the RMS Service Account (Exchange 2010)

## Overview

This section provides instructions for configuring the RMS user account's access to Exchange Room Mailboxes.

## Configuring the RMS Service Account

A single domain account is used by RMS to access all room mailboxes on the Exchange server. This account must meet the following requirements:

1. The account must have an associated Exchange Mailbox.
2. The account must have rights to add, modify, and cancel/delete appointments in each Exchange Room Mailbox RMS will synchronize with. This may be accomplished via one of the following three methods:
  - a. Delegate access to the mailbox.
  - b. Full-access permissions on the mailbox.
  - c. Impersonating the mailbox owner using *Exchange Impersonation*.

### Assigning the RMS Account As a Delegate To the Room Mailbox

1. Open the *Exchange Management Console*.
2. Navigate to the **Recipient Configuration** leaf in the *Exchange* tree.
3. Right-click on the desired *Room Mailbox*.
4. Click **Properties**.
5. Click the **Resource Policy** tab.
6. Add the RMS account to the delegates list.



NOTE

*On Exchange 2007 servers if the RMS user account is set as a delegate on the room mailboxes then full-access permissions must also be granted.*

### Assigning Full-access Permission To the RMS account

1. Open the *Exchange Management Console*.
2. Navigate to the **Recipient Configuration** leaf in the *Exchange* tree.
3. Right-click on the desired *Room Mailbox*.
4. Select the **Manage Full Access Permission** menu option.
5. Add the RMS account to the full access permission list.

### Assigning the Exchange Impersonation Role to the RMS account

Impersonation may be enabled for an individual account or on multiple accounts using a RoleGroup:

#### Enabling Impersonation for a Single Account

Create the impersonation RoleAssignment for the specific account:

```
New-ManagementRoleAssignment -Name:EWSImpersonation -Role:ApplicationImpersonation
-User: jdoe@company.com
```

#### Enabling Impersonation for Multiple Accounts

Create a RoleGroup for impersonation:

```
New-RoleGroup -Name: "EWS Impersonators"
```

#### Adding Accounts to the New RoleGroup

```
Add-RoleGroupMember -Identity:"EWS Impersonators" -Member:jdoe@company.com (use as many times as
necessary)
```

### **Create the Impersonation RoleAssignment for the RoleGroup**

New-ManagementRoleAssignment -Name:EWSImpersonation -Role:ApplicationImpersonation  
-SecurityGroup:"EWS Impersonators"

### **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>

Proceed to the next section, and follow all of the instructions for *Configuring RMS to use Microsoft .NET Framework v4*.

# Configuring RMS to use Microsoft.NET Framework v4

## Overview

This section describes configuring the RMS website (UI) to use version 4 of the Microsoft.NET Framework.

- IIS 6 - See *Specifying the ASP.NET Version for IIS 6* below
- IIS 7 - Detailed instructions for this procedure are available online from Microsoft: <http://technet.microsoft.com/en-us/library/cc754523%28WS.10%29.aspx>



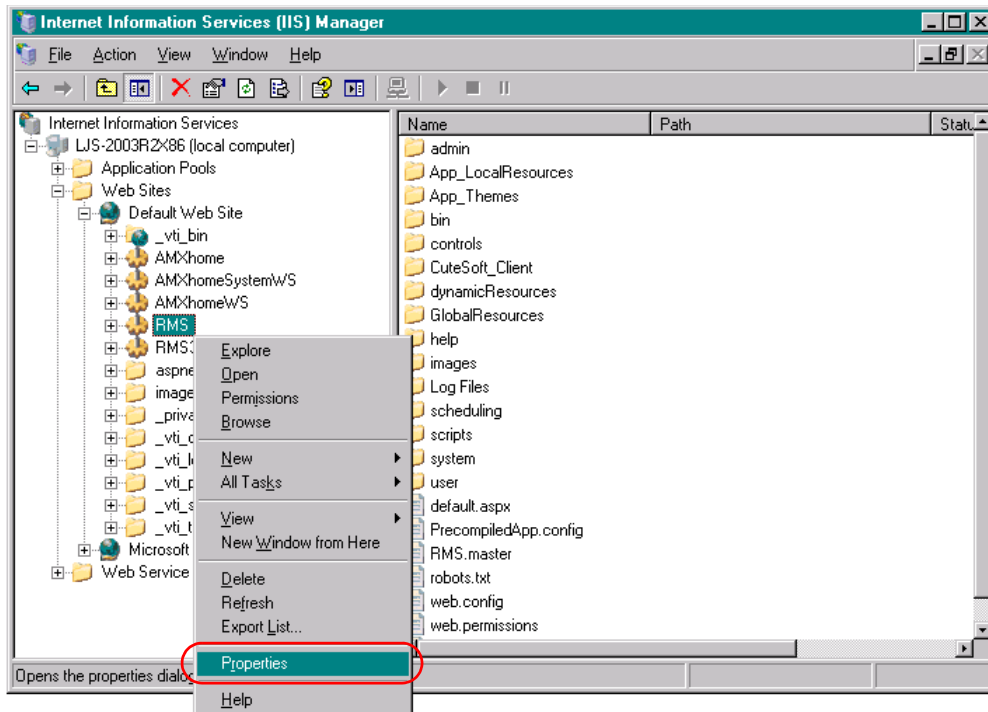
NOTE

If the .NET framework was installed after IIS, then `aspnet_regiis.exe -i` must be executed from the .NET framework directory.

When the requirements in this section have been met, proceed to the next section, and follow all of the instructions for *Exchange 2010 Scheduling Configuration*.

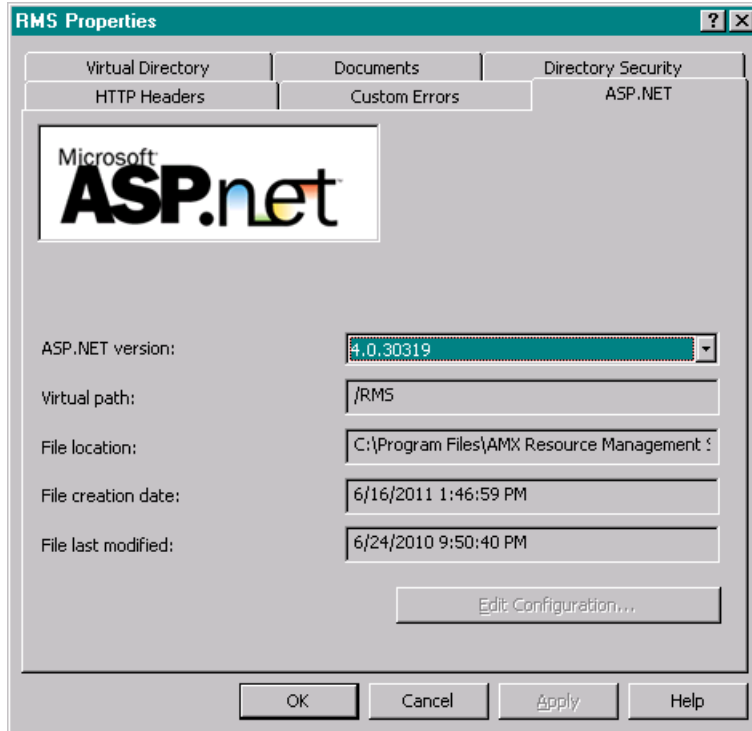
## Specifying the ASP.NET Version for IIS 6

1. Start the IIS 6 management application:
  - a. Select **Start > Programs > Administrative Tools > Internet Information Services**
  - b. Select **Start > Programs > (IIS) Manager**
2. Navigate to the RMS web site, right-click, and select **Properties** from the context menu (FIG. 31):



**FIG. 31** Internet Information Services > Web Sites > Default Web Sites > RMS - *Properties* selected in the context menu

3. This opens the *RMS Properties* dialog.
4. Select the *ASP.NET* tab and ensure "ASP.NET version:" is **4.0.30319** (FIG. 32):



**FIG. 32** RMS Properties - ASP.NET tab

5. Click **OK**.
6. Exit Internet Information Services (IIS) Manager.

# Known Issues

## Overview

This section provides information on known issues relative to the RMS Interface for Exchange EWS.

- The RMS Interface for Exchange EWS communicates with a single Exchange Server.
- Appointments deleted from the RMS schedule in the RMS User Interface will be restored during the next schedule synchronization cycle. The delete option on the appointment context menu should not be enabled. Its availability is a known anomaly.
- Welcome text, macros, and images associated with an instance in a recurring series will not be propagated to the other meeting instances in the series.
- When using Windows Authentication in IIS7, *Anonymous Authentication* must be disabled.
- The RMS Interface for Exchange EWS will synchronize with Exchange 2007 servers at or greater than Service Pack level 1. However, Exchange Distribution Lists are only available in Exchange 2010 and later, which will require the email address for each Exchange Room Mailbox to be manually entered in the web administrative interface.



**Increase Your Revenue  
through education + knowledge**

In the ever-changing AV industry, continual education is key to success. AMX University is dedicated to ensuring that you have the opportunity to gather the information and experience you need to deliver strong AMX solutions. Plus, AMX courses also help you earn CEDIA, NSCA, InfoComm, and AMX continuing education units (CEUs).

Visit AMX University online for 24/7/365 access to:

- *Schedules and registration for any AMX University course*
- *Travel and hotel information*
- *Your individual certification requirements and progress*