EMS for Outlook

Installation, Configuration, and User Guides

V44

April 2019

Accruent, LLC 11500 Alterra Parkway, Suite 110, Austin, TX 78758 www.accruent.com

Table of Contents

CHAPTER 4: Introduction to the EMS for Outlook Installation Guide

EMS for Outlook is an optional add-in that integrates the EMS room reservation process directly with Microsoft Outlook 2010/2013. Users can view room availability in addition to attendee free/busy information simultaneously and book/manage their meetings directly within Outlook. This document lists the steps you must take to install and configure EMS for Outlook.

The purpose of the section is to answer your questions and guide you through the procedures necessary to install the EMS for Microsoft Outlook application efficiently and effectively for Legacy Versions.

IMPORTANT: To ensure your users are benefiting from the newest features, enhancements, and fixes, EMS Software recommends that you upgrade to the most current release of your EMS product.

- Prerequisites
  - EMS for Outlook Requirements
  - System Architecture
- Plan Your EMS for Outlook Implementation
- Obtain the EMS for Outlook Installation File
- Install or Upgrade EMS for Outlook on a User's PC
- EMS for Outlook Add-In Is Offline
- Silent/Unattended EMS for Outlook Installation
- Where to See Your Exchange Server URL and EMS for Outlook Version Number

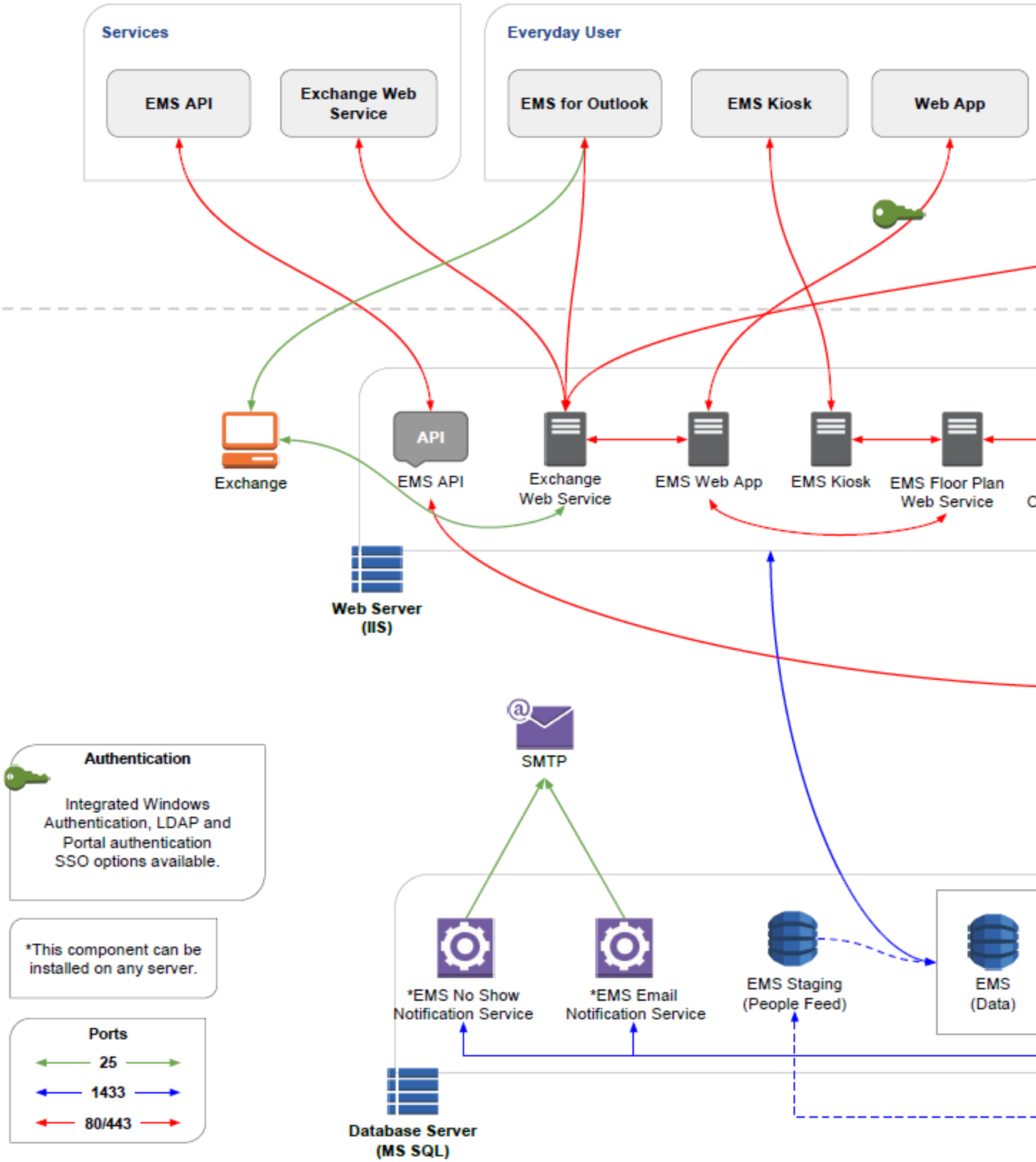
Interested in Upgrading?

Contact EMS Sales at (800) 440-3994. For more information, visit www.emssoftware.com.

CHAPTER 5: System Architecture

EMS for Outlook is one of the Everyday User Applications that is controlled by configurations in EMS Desktop Client.

The EMS Desktop Client is the foundation for a broad range of components, services, web applications, APIs, add-ons, and integrations.


Services
EMS API
Exchange Web Service
Everyday User
EMS for Outlook
EMS Kiosk
Web App
Exchange
API
EMS API
Exchange Web Service
EMS Web App
EMS Kiosk
EMS Floor Plan Web Service
Web Server (IIS)
SMTP
Authentication
Integrated Windows Authentication, LDAP and Portal authentication SSO options available.
*This component can be installed on any server.
Ports
25
1433
80/443
*EMS No Show Notification Service
*EMS Email Notification Service
EMS Staging (People Feed)
EMS (Data)
Database Server (MS SQL)

CHAPTER 6: Prerequisites

1. Uninstall any older versions of EMS for Outlook.
2. The EMS Integration to Exchange Web Service must be installed and operational. For information on how to install and configure this component.

TIP: You can quickly verify if the service has been installed by opening a browser and entering the following: http://[ServerName]/ExchangeIntegrationWebService/Service.asmx (replace [ServerName] with the name of your web server)

The Web Service Address will be required when running the EMSForOutlook.msi (described in Where to See Your Exchange Server URL and EMS for Outlook Version Number).

3. EMS must be configured properly in order to activate EMS for Outlook for each Outlook® user.
4. Verify that the required software is installed on your users' workstations (See Also: EMS for Outlook Requirements).

CHAPTER 7: Plan Your EMS for Outlook Implementation

EMS for Outlook consists of two main components: the Integration with Microsoft Exchange and the EMS for Outlook installation.

Install the EMS Integration for Microsoft® Exchange Web Service

This service (typically installed where your EMS Web App resides) manages all communication/transactions between EMS for Outlook (as well EMS Desktop Client and EMS Web App) and the EMS database, including checking room availability, booking the meeting in EMS, and managing changes. EMSForOutlook.msi will prompt the user for the Integration with Microsoft Exchange Web Service Address during the installation process.

Tip: The URL you enter during this process is stored in the application's configuration file and can be changed by going to Add/Remove Programs > Ems for Outlook > Change Installation > Change URL.

Install EMS for Outlook On Users' Computers (EMSForOutlook.msi)

This add-in should be installed on your users' desktops. This file exposes the EMS Room Scheduling option on the Outlook Calendar Appointment form. By default, the EMSForOutlook.msi installs all of the files required by the EMS for Outlook Add-in in the following locations:

- 32-bit machines – *C:\Program Files\EMS for Outlook*
- 64-bit machines – *C:\Program Files (x86)\EMS for Outlook*

This location can be changed during the installation, but it is recommended that you keep the default.

Configuration Path

1. EMS must be configured properly in order to activate the EMS for Outlook for each Outlook user:
    a. The Outlook user must have an active EMS Everyday User account.
    b. The EMS Everyday User account must be assigned to at least one Everyday User Process Template with the Outlook option enabled.
    c. The EMS Everyday User account must be associated to an active EMS Group record.
    d. The EMS Everyday User must have an associated Contact.

Tip: The Group might have been relabeled to "Client" or "Employee" in your EMS system.

CHAPTER 8: Install or Upgrade EMS for Outlook on a User's PC

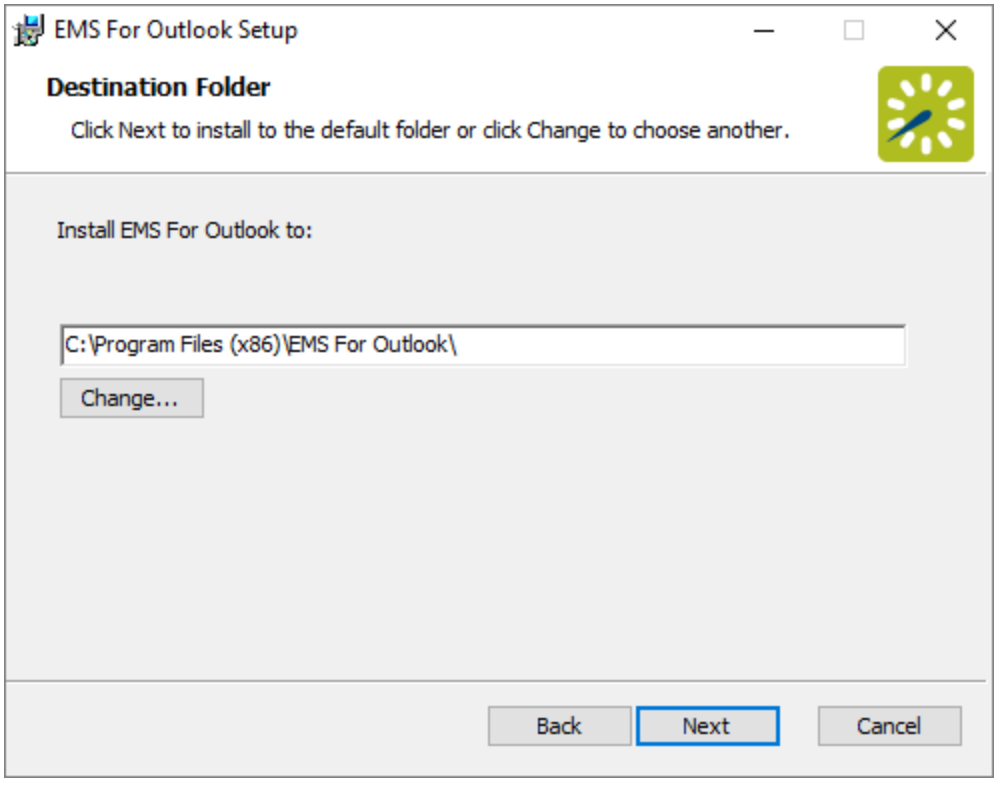
This topic provides information on the following:

- x86 User Installation
- x64 User Installation
- Silent EMS for Outlook User Installation

IMPORTANT: Begin by uninstalling previous versions of the EMS for Outlook application.

x86 User Installation

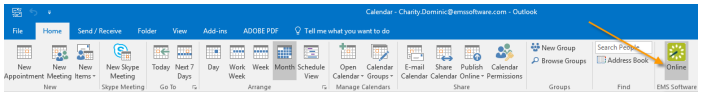
1. Verify that the pre-installation requirements have been met.
2. Download the EMSForOutlook.msi file onto the user's desktop.
3. Close Outlook.
4. Run EMSForOutlook.msi.
5. The first screen welcomes you to the EMS Outlook Add-in Setup Wizard. Click the Next button to begin the installation process. The Destination Folder screen will appear.



6. Specify the Installation Folder.

IMPORTANT: EMS for Outlook only supports the Program Files directory. You should not change this directory during installation.

7. Click the Next button. The Outlook Integration Service Information screen will appear.
8. Enter the Outlook Integration Web Service address your organization uses. (Example - http://[Server-Name]/ExchangeIntegrationWebService/Service.asmx)
9. Click the Next button. The Ready to install EMS for Outlook screen will appear.
10. Click the Install button to complete the installation. Click the Close button to exit.
11. Launch Outlook. The EMS button should display on the user's Outlook toolbar on the Calendar as online.

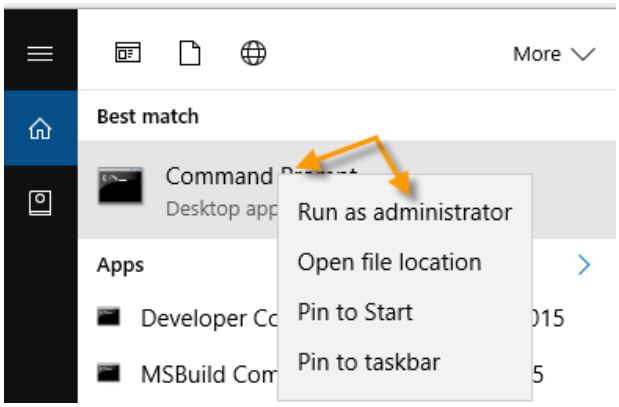


Tip: If the EMS for Outlook displays as Offline, return to Step 8 or see EMS for Outlook Add-In Is Offline.

x64 User Installation

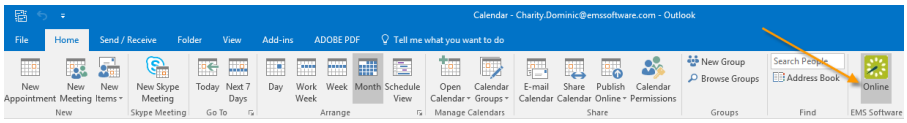
The installer on 64-bit machines with 64-bit Microsoft® Office requires elevated permissions to run. Follow these steps to install with elevated permissions.

1. Verify that the pre-installation requirements have been met.
2. Download the EMSForOutlook.msi file onto the user's desktop.
3. Close Outlook.
4. Run the installer from the command line: from the Windows Start menu, type "cmd."
5. On the Command Prompt application that appears in the menu, right-click and select Run as administrator. This launches the application with elevated permissions.



6. In the Command Prompt window, enter "msiexec "EmsForOutlook.msi".
7. When the file completes, close Command Prompt.

8. Launch Outlook. The EMS button should display on the user's Outlook toolbar on the Calendar as online.



Tip: If the EMS for Outlook displays as Offline, see EMS for Outlook Add-In Is Offline.

Silent EMS for Outlook User Installation

You can push your EMS for Outlook Installation to user machines if your system enables this type of administration.

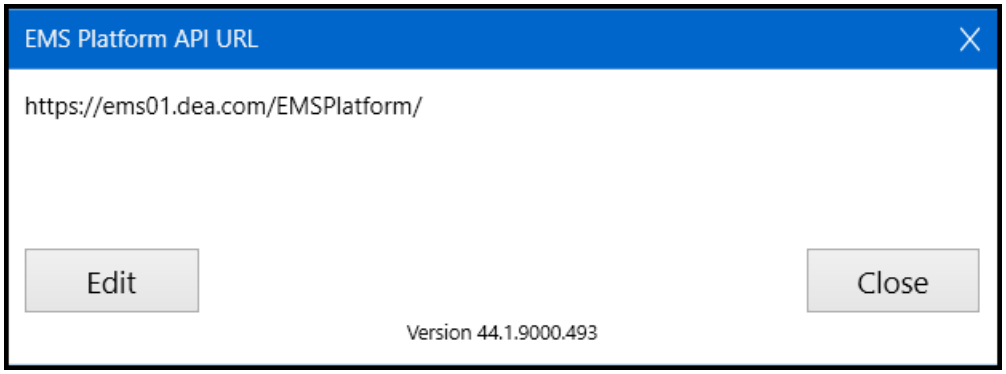
Use the following command to establish an Unattended/Silent installation of the EMSForOutlook.msi (replace [ServerName] with the name of your web server):

msiexec /i "EMSForOutlook.msi" RSURL="http://<url>"

CHAPTER 9: EMS for Outlook Add-In Is Offline

If a user opens Microsoft® Outlook and the EMS for Outlook icon in the Outlook toolbar is "offline," then the Exchange Integration Server URL (typically from your Administrator) needs to be entered so that the application is connected and online as shown below. This might also occur if the network has issues contacting the EMS Platform Services server.

1. To enter or change the Exchange Integration server URL for EMS for Outlook, click the EMS for Outlook icon from the Outlook toolbar. A pop-up shows the status of the add-in.



NOTE: Only your IT System Administrator perform this step.

2. Click the Edit button.
3. Enter the new URL and click the Update button.

CHAPTER 10: Silent/Unattended EMS for Outlook Installation

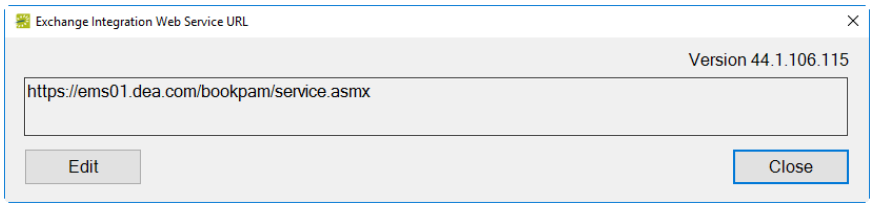
You can push your EMS for Outlook Installation to user machines if your system enables this type of administration.

Use the following command to establish an Unattended/Silent installation of the EMSForOutlook.msi (replace [ServerName] with the name of your web server):

msiexec /i "EMSForOutlook.msi" WSURL="http://<url>"

CHAPTER 11: Where to See Your Exchange Server URL and EMS for Outlook Version Number

Click the EMS for Outlook icon from the Outlook toolbar. A pop-up shows the Version number of the add-in and the Exchange Integration Server URL.



CHAPTER 12: Introduction to EMS Integrated Authentication

The EMS Integrated Authentication component provides single-sign-on capability using Integrated Windows Authentication, your organization's portal, or LDAP. The Integrated Authentication Setup Guide lists the steps you must take to configure these Integrated Authentication options. If you are unsure whether your organization is licensed for Integrated Authentication or you would like to learn more about it, please contact your Account Executive.

The diagram below shows how your organizations' existing security software and systems integrate with EMS software applications through configurations you set in EMS Desktop Client.

Integration Diagram

When configuring integrated authentication using this component, you can use the following methods:

- Integrated Windows Authentication
- Portal or Federated Authentication
- LDAP Authentication

What is Integrated Windows Authentication?

Integrated Windows Authentication (IWA) is a built-in Microsoft Internet Information Services (IIS) authentication protocol that can be used to automatically authenticate and sign-in a user to EMS Web App. Integrated Windows Authentication works only with Internet Explorer and is best used on intranets where all clients accessing EMS Web App are within a single domain. When a domain user who is logged on to a networked PC accesses an EMS Everyday User application, such as EMS Web App, EMS Mobile App, or EMS for Outlook, their Active Directory credentials (Domain\User ID) are compared against corresponding Domain\User ID information recorded in the Network ID and\or External Reference fields of your EMS Everyday User records. If a match exists, the Everyday User will be automatically logged in.

For a more detailed explanation of the authentication methods outlined above, see Integrated Windows Authentication.

What is Portal or Federated Authentication?

The Portal Authentication method provides EMS Web App single sign-on capability using your organization's portal (e.g., CAS, Shibboleth, SiteMinder, Plumtree, uPortal, etc.). When a user logged into your portal accesses EMS Web App, a predefined user-specific variable (e.g., email address, employee/student ID, network ID, etc.) captured by your portal/sign-on page is compared against

corresponding information recorded in the Network ID and/or External Reference fields of your EMS Everyday User records. If a match exists, the Everyday User will be automatically logged-into EMS Web App.

NOTE: The Field Used to Authenticate Everyday User parameter (within System Administration > Settings > Parameters > Everyday User Applications tab) is used by EMS Web App to determine which value should be used for authentication.

Several built-in authentication methods to pass-in credentials are available including:

- Server Variable (Header Variable)
- Session
- Form
- Cookie
- Query String
- Federated (SAML)

For a more detailed explanation of the authentication methods outlined above, see Portal Authentication Methods.

What is LDAP Authentication?

Lightweight Directory Access Protocol (LDAP) is an application protocol for querying directory information. The LDAP Authentication method provides single-sign-on capability using your organization's LDAP environment and can be used in both intranet and internet deployments of EMS Everyday applications such as EMS Web App and EMS Mobile App.

The LDAP Authentication topic covers the following information related to LDAP configuration:

- Configure EMS Web App to Use LDAP Authentication
- Configure EMS Web App Security
- Configure Communication Options
- Core Properties
- Non-AD Config
- LDAP Queries
- Save Your Configuration
- Test Your Configuration
- Configure Authentication for EMS Mobile App

When a user logs into EMS Web App or EMS Mobile App with their User ID and Password, their credentials are authenticated against LDAP and compared against corresponding user information recorded in the Network ID and/or External Reference fields of your EMS Everyday User records. If a match exists, the

Everyday User will be logged in to the application, inheriting any Everyday User Process Template rights to which their LDAP Group has been assigned.

NOTES:

- The EMS Web App LDAP-Process Template assignment process requires that your implementation of LDAP stores group information (e.g., staff, student, department, etc.) as a Directory Service object containing a property (i.e., member) that contains the users that belong to your various groups.
- The Field Used to Authenticate Everyday User parameter (within System Administration > Settings > Parameters > Everyday User Applications tab) is used by the applications to determine which value should be used for authentication.

Contact Customer Support

- **Option 1 (Recommended):** Search the Knowledge Base available in the EMS Customer Portal.
- Option 2: Submit a Case directly via the EMS Customer Portal.
- **Option 3:** Email **support@emssoftware.com**.
- **Option 4 (Recommended for critical issues only):** Phone (800) 288-4565.

Important! If you do not have a customer login, register here.

CHAPTER 13: Integrated Windows Authentication

Integrated Windows Authentication (IWA) is a built-in Microsoft Internet Information Services (IIS) authentication protocol that can be used to automatically authenticate and sign-in a user to EMS Web App. Integrated Windows Authentication works only with Internet Explorer and is best used on intranets where all clients accessing EMS Web App are within a single domain.

This topic provides information on the following:

- Activate Integrated Windows Authentication for IIS 6.0
- Activate Integrated Windows Authentication for IIS 7.x/8.x

NOTE: Integrated Windows Authentication is supported for EMS Floor Plan (V44.1 Update 11).

See Also:

- Integrated Authentication Overview
- For more information, please review the following Microsoft TechNet articles on IWA for IIS 6.0, 7.0, and 8.0.
- Connect Your Database Using Active Directory

When a domain user who is logged on to a networked PC accesses an EMS Everyday User application, such as EMS Web App, EMS Mobile App, or EMS for Outlook, their Active Directory credentials (Domain\User ID) are compared against corresponding Domain\User ID information recorded in the Network ID and\or External Reference fields of your EMS Everyday User records. If a match exists, the Everyday User will be automatically logged in.

NOTE: The Field Used to Authenticate Web User parameter (within System Administration > Settings > Parameters > Everyday User Applications tab is used to determine which value should be used for authentication.

Activate Integrated Windows Authentication for IIS 6.0

1. On the web server that hosts your EMS application's site, open IIS Manager.
2. Locate your EMS application's site.
3. Right-click your EMS application's site and choose Properties. The Properties screen will open.
4. Go to the Directory Security tab and click the Edit button under the Authentication and access control section. The Authentication Methods screen will open.
5. Uncheck the Enable anonymous access option. The Integrated Windows authentication option should be the only option checked.

6. Click OK to exit the Authentication Methods screen. Click OK again to exit the Properties screen. You have completed the necessary IIS configuration steps for IIS 6.0.

Activate Integrated Windows Authentication for IIS 7.x/8.x

1. On the web server that hosts your EMS application's site, open IIS Manager.
2. Locate and highlight your EMS application's site.
3. Double-click the Authentication option in the IIS section.
4. Right-click the Windows Authentication option and select Enable.
5. Right-click the Anonymous Authentication option and select Disable.
6. You have completed the necessary IIS configuration steps for IIS 7.

CHAPTER 14: LDAP Authentication

Lightweight Directory Access Protocol (LDAP) is an application protocol for querying directory information. The LDAP Authentication method provides single-sign-on capability using your organization's LDAP environment and can be used in both intranet and internet deployments of EMS Everyday applications such as EMS Web App and EMS Mobile App.

For example, when a user logs into EMS Web App or EMS Mobile App with their User ID and Password, their credentials are authenticated against LDAP and compared against corresponding user information recorded in the Network ID and/or External Reference fields of your EMS Everyday User records. If a match exists, the Everyday User will be logged in to the application, inheriting any Everyday User Process Template rights to which their LDAP Group has been assigned.

Note: The EMS Web App LDAP-Process Template assignment process requires that your implementation of LDAP stores group information (e.g., staff, student, department, etc.) as a Directory Service object containing a property (i.e., member) that contains the users that belong to your various groups.

Note: The Field Used to Authenticate Everyday User parameter (within System Administration > Settings > Parameters (Everyday User Applications tab) is used by the applications to determine which value should be used for authentication.

Follow the steps in this section to authenticate your users via LDAP. After successful connection to the platform API, the user will log in following the scenario below:

- The user will enter credentials on the Sign In screen and tap Sign In.
- EMS Mobile App will send credentials to the EMS Platform Services.
- EMS Platform Services will verify credentials against the configured LDAP provider.
- EMS Platform Services will respond to the EMS Mobile App.
- User will be taken to the Home screen.

If the credentials are missing when the user taps Sign In, an error message will display stating that fields are required. If the platform API is unable to verify the credentials, the mobile app will inform the user based on that response.

To use LDAP authentication, you will need to:

1. Configure your LDAP Provider.
2. Test your LDAP Configuration.
3. Test your LDAP Authentication.

This topic covers the following topics related to LDAP configuration:

Configure Your LDAP Provider

1. Navigate to Platform Services admin portal (https://yourcompany.com/ems-platform-api) and select Integrations from the sidebar.
2. Select EMS Mobile and choose LDAP from everyday user authentication method dropdown.

3. Navigate to the EMS Web App > Admin Functions page, listed under your name in the upper right corner of the application.

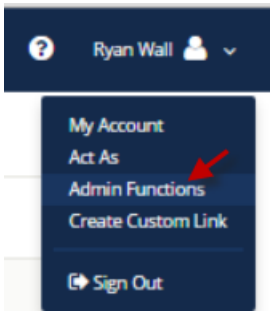
4. Tap the LDAP Configuration tab and complete all required LDAP information, and then Test Your LDAP Configuration.

Tip: This is the same process you use for . The EMS Platform Services API uses the same configuration information.

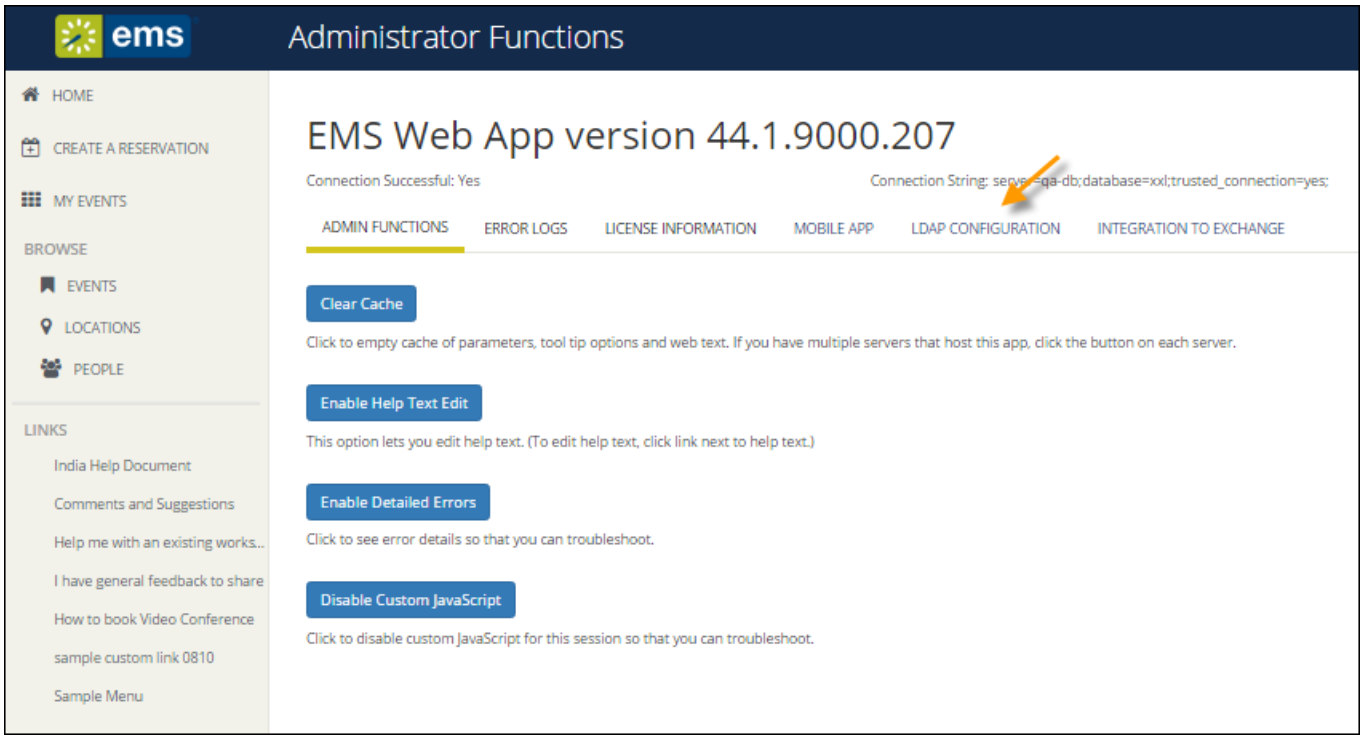
Configure EMS Web App to Use LDAP Authentication

1. Log into EMS Web App with a User that belongs to an Everyday User Security Template containing the Web Administrator role (controlled in the EMS Desktop Client under Configuration > Everyday User Applications > Everyday User Security Templates). See Also: Configuring Security Templates

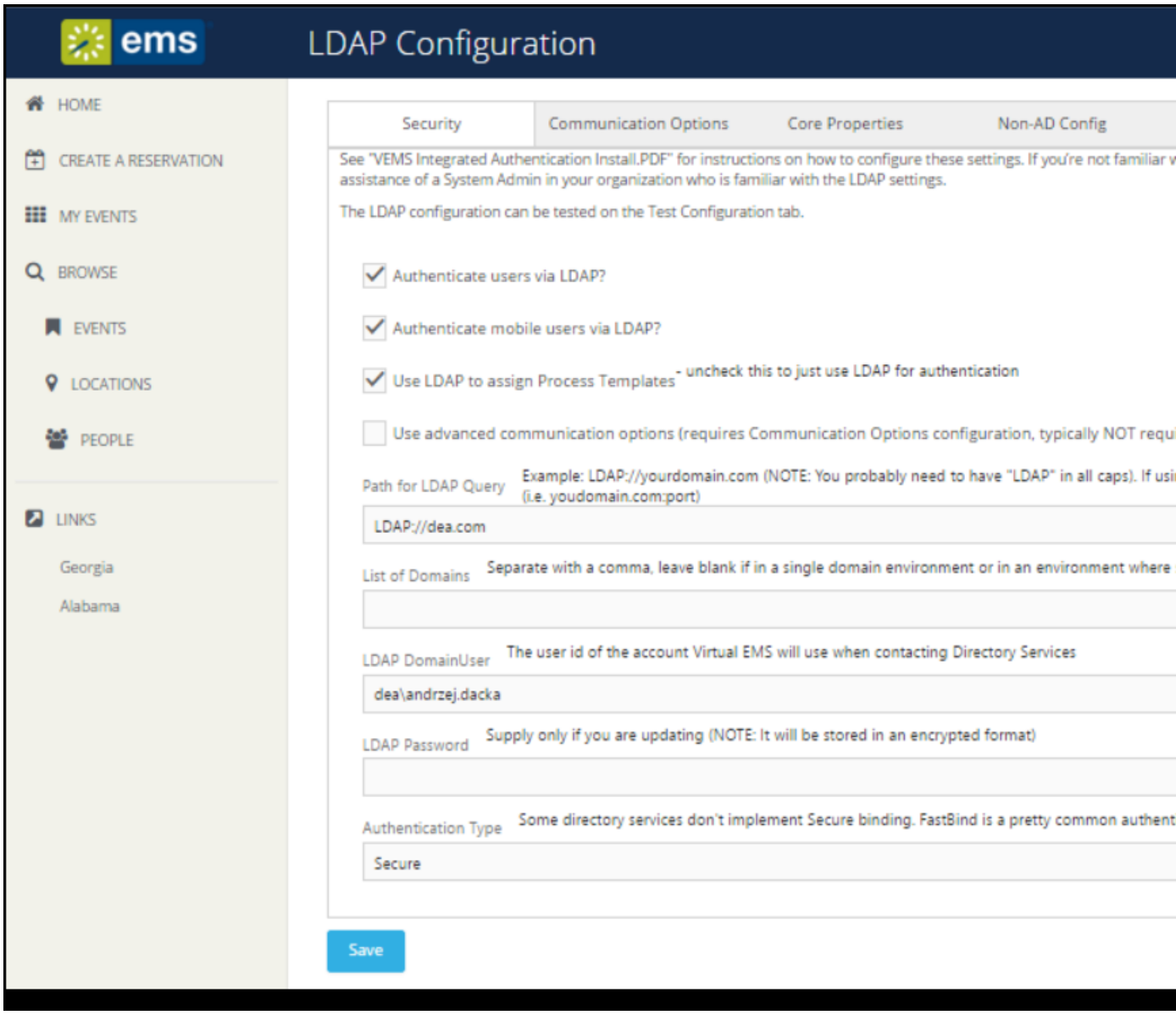
2. From the User Options, select Admin Functions.



3. Click the LDAP Configuration tab.



4. The LDAP Configuration window appears, presenting multiple tabs for various settings.



Configuring EMS Web App Security

1. On the Security tab:
   a. Select the Authenticate users via LDAP checkbox to enable LDAP authentication.
   b. If LDAP will be used to assign Everyday User Process Templates to your Web Users, select the Use LDAP to assign Process Templates checkbox.
   c. Use advanced communication options: Skip this step for Active Directory environments. Enabling this checkbox requires that you complete the settings on the Communication Options tab.

d. In the Path for LDAP Query field, specify a valid LDAP path (example – LDAP://YourCompany.com)
e. List of Domains: Skip this step if your organization uses a single domain. Otherwise, provide a comma separated list of your domains.
f. In the LDAP Domain\User field, enter a Domain User account that has rights to query LDAP (example – YourDomain\User)
g. In the Password field, enter a valid Password for the User Account entered in the previous step.
h. Specify the appropriate LDAP Authentication Type for your environment.

Note: The other tabs (Communication Options, Core Properties, Non-AD Config and LDAP Queries) should only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP.

Configuring Communication Options

Warnings: It is recommended that this tab only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP. If you're not familiar with the LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is familiar with the LDAP settings.

The Communication Options tab includes fields that define how to fetch a Group or a User when sending communications from the EMS Desktop Client. You can also set the SSL configurations, including the Security Certificate Path. Checking the Use SSL box will force communication to use SSL.

- Certificate Path: If there is a specific certification that you want to use to validate your authentication.
- Authentication Type: Type of authentication that your LDAP server will use during the binding process. Basic is the default because it is the most common.
- Search Root: The root is the level at which your search will begin.
- User Search Filter: Specifies the filter to use when performing the user search.
  - Example: (&(objectClass=Person)(SAMAccountName={0})) or (&(objectClass=Person)(uid={0}))
- Group Search Filter: Specifies the filter to use when performing the group search.
  - Example: (&(objectClass=Person)(objectClass=user))
- Protocol Version: Insert the current version number here. The default is 3, as the current version should be 3.

Core Properties

Warnings: It is recommended that this tab only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP. If you're not familiar with the LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is

familiar with the LDAP settings.

Indicate whether your LDAP implementation is Active Directory. These properties are set to the common defaults, but can be changed here if the LDAP properties differ from the defaults displayed.

- LDAP Name Property: The property for user name on the user record in LDAP that will be displayed. Displayname is the default, as it is the most common.
- LDAP Phone Property: The property for the phone number on the user record in LDAP that will be displayed. Telephonenumber is the default, as it is the most common.
- Domain to append to users: This field is unnecessary unless the domain of your user is different from the domain returned from the query.
- Field for LDAP Group Lookup: This identifies the EMS property that should be utilized when performing the search. For example, if you use LDAP solely to assign templates and you want the EMS Web App to look up group membership using a field other than the login name, then you must enter that field's name here.

Non-AD Configuration

Warning: It is recommended that this tab only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP. If you're not familiar with the LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is familiar with the LDAP settings.

If your LDAP implementation is not Active Directory, use these fields to redefine the LDAP property names used when searching directory information.

- LDAP Account/User ID Property: The property in your LDAP store that contains the user name.
  - Example: If sameaccountname=xxxx, then enter sameaccountname
- Full LDAP User ID Format: Leave blank unless authentication requires a full path.
  - Example: cn={0},ou=staff,o=yourdomain
- LDAP Group Category: The property in your LDAP store that contains the group category.
  - Example: If filter should be objectClass=groupOfNames, then property should be groupOfNames
- LDAP Group Name: The property in your LDAP store that contains the group name.
- LDAP Group Member Name: The property in your LDAP store that contains the name of a single member in the group.
  - Example: If member property is member=jdoe, then property should be member
- LDAP Group Member User Name Attribute: The property of the user record that corresponds to the group's member property to determine group membership.

LDAP Queries

Warning: It is recommended that this tab only be edited with assistance from our Support Department

when special circumstances arise with unique configurations of LDAP. If you're not familiar with the LDAP settings, it is highly recommended to get the assistance of a System Admin in your organization who is familiar with the LDAP settings.

These are LDAP query overrides to fetch Groups and Users from the domain. These settings rarely need to overridden, but can be used to customize queries.

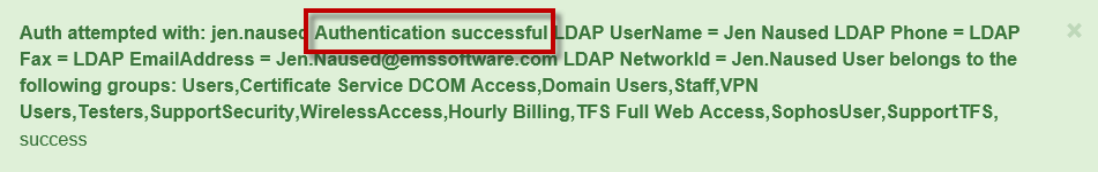
- LDAP query for security groups: Query used to search for security groups in your LDAP store.
- LDAP query to find users: Query used to search for users in your LDAP store.
- LDAP query for find users with space: Query used to search for users that have spaces surrounding their user names in your LDAP store.

Save Your Configuration

1. Click Save.
   Note: If you want Everyday Users to inherit Everyday User Process Templates based on the LDAP Group(s) with which they belong, see LDAP Groups Tab. Otherwise, you have completed the configuration process.
2. Within EMS Desktop Client, go to the Everyday User Process Templates area (Configuration > Web > Everyday User Process Templates).
3. Within an Everyday User Process Template, locate the LDAP Groups tab and select the appropriate LDAP Group(s) to map to that Everyday User Process Template.
4. Click OK.

Test Your Configuration

1. After completing configuration, navigate to the Test Configuration tab in the EMS Web App under LDAP Configuration.
2. Enter your Network UserId Without Domain Name.
3. Enter your Password.
4. Click Test.
   a. If your configuration was successful, you will receive a message in a green box at the top that includes domain information and the words "Authentication successful" (please see example below).



b. If the configuration was unsuccessful, you will receive a prompt stating that LDAP could not be accessed. Check your logs to determine the reason for the failure.

Configuring Authentication for the EMS Mobile App

1. If your organization uses EMS Mobile App, click the Mobile App tab.
2. Choose the LDAP option.

Test Your LDAP Configuration

Assuming you have installed the EMS Platform Services e.g. https://yourcompany.com/ems-platform-api, then you can test the configuration with a simple curl command:

curl -X GET -H 'x-ems-consumer: MobileApp' https://ems.yourcompany.com/endpoint/api/v1/health
Tip: You can also use the API's Swagger interface to accomplish this goal.

You should see a portion of the JSON response that looks like this (unrelated details omitted for brevity):

```
{
  ...
  "additionalProperties": {
    "authConfig": {
      "activities":"ldap"  // <-- these are the critical lines
      "ui":"ldap"
    }
  }
}
```

Test Your LDAP Authentication

Assuming you have installed the EMS Platform Services API at https://ems.*yourcompany*.com/endpoint, you can test the authentication with a simple curl command:

curl -X POST -H 'x-ems-consumer: MobileApp' -H 'Content-Type: application/json' -d '
{"username":"your_username", "password":"your_password"}'
https://ems.yourcompany.com/endpoint...authentication

...where your_*username* and your_*password* are your credentials.

Note: api/v1/authentication is the endpoint within the API where your request must be sent.

CHAPTER 15: Portal or Federated Authentication

This topic provides information on the following:

Portal Authentication Overview

The Portal Authentication method provides EMS Web App single sign-on capability using your organization's portal (e.g., CAS, Shibboleth, SiteMinder, Plumtree, uPortal, etc.). When a user who is logged into your portal accesses EMS Web App, a predefined user-specific variable (e.g., email address, employee/student ID, network ID, etc.) captured by your portal/sign-on page is compared against corresponding information recorded in the Network ID and/or External Reference fields of your EMS Everyday User records. If a match exists, the Everyday User will be automatically logged-into EMS Web App.

NOTE: The Field Used to Authenticate Everyday User parameter (within System Administration > Settings > Parameters > Everyday User Applications tab) is used by EMS Web App to determine which value should be used for authentication.

Several built-in authentication methods to pass-in credentials are available including:

- Server Variable (Header Variable)
- Session
- Form
- Cookie
- Query String
- Federated (SAML)

For a more detailed explanation of the authentication methods outlined above, see Portal Authentication Methods.

Installation/Configuration

1. Within the Everyday User Applications parameters area of EMS (System Administration > Settings > Parameters (Everyday User Applications tab), the following parameters must be set accordingly:

AREA	DESCRIPTION	VALUE
Authentication	Portal Authentication Cookie Key	Required if Portal Authentication Method = Cookie
Authentication	Portal Authentication Method	Server Variable Session Form Cookie Query String
Authentication	Portal Authentication Variable	User variable to be compared against the EMS Everyday User External Reference/Network ID field

2. Direct users to the default EMS Web App page. If the default installation settings were used, the default page is:
(http://[ServerName]/EMSWebApp/Default.aspx)
(replace [ServerName] with the name of your web server)

Redirect User Log In to Your SSO Provider

Administrators can hide the login form on the My Home page and instead, present a single Sign In button that links to the override URL. Open the web.config file and locate the following code to customize the redirect:

<!--<add key="loginOverrideUrl" value=""/>-->

Additionally, you can do the same for user log out:

<!--<add key="logoutOverrideUrl" value=""/>-->

Changing the URL in these areas means that when users log in or out, they will pass through your SSO provider.

Specify a Different Default Home Page for Guest Users

Additionally, you can now specify a different site home page for unauthenticated users.

CHAPTER 16: Portal Authentication Methods

This topic provides information about the following:

NOTE: EMS applications do not natively support SAML. You must use our Portal Authentication to use SAML.

Server Variable Method (Header Variable)

Server Variable/Header Variable is a collection of variables that are set by Internet Information Server (IIS).

Applications like SiteMinder create custom server variables for portal site use.

Set the Portal Authentication Method parameter to Server Variable and type the appropriate variable for the Portal Authentication Variable parameter. Direct users to your EMS Web App Default.aspx page.

Server Variable Method – Federated (SAML)

NOTE: As of Update 23 (March 2018), SAML authentication for the EMS Web App is supported through EMS Platform Services. This is now the recommended method for configuring SAML. See Also: SAML Authentication.

SAML can be leveraged for authentication with your EMS applications by leveraging our portal authentication method and a service provider of your choosing.

Method 1: Locally installed Service Provider

Using this method, you install a service provider of choice on the webserver hosting the EMS web applications. All traffic is routed through that service provider (typically via an ISAPI filter). This service provider will manage all of the authentication for the user. Once the user has successfully authenticated, it

will pass an identifier for the user to the EMS application using one of our portal methods. In this scenario typically the Server Variable (Header) method is used.

Method 1 configuration Steps

1. Install and configure a service provider on the EMS web server
2. Set the service provider to protect the specified EMS web applications
3. Configure the service provider to pass the required user attributes
4. In EMS Desktop Client, configure the EMS Web App parameter "Portal Authentication Method"
5. In EMS Desktop Client configure the applicable Portal Authentication Variables.

Method 2

This method can be common if there is already a server configured with a service provider in your environment, handling authentication for other applications. In EMS Desktop Client, you can configure your application to re-direct any login requests to the other server to be authenticated. Once the user is authenticated, the server with your service provider installed sends the user back to the EMS Desktop Client with an identifier for the user in the header, or within a cookie. The EMS application reads this header, or cookie value, and leverages portal authentication to sign the user in with the matched credentials.

Method 2 Configuration Steps

1. Install and configure a service provider on the EMS web server
2. Set the service provider to protect the specified EMS web applications
3. Configure the service provider to pass the required user attributes
4. In EMS Desktop Client configure the EMS Web App parameter "Portal Authentication Method"
5. In EMS EMS Desktop Client, configure the applicable Portal Authentication Variables.
6. In EMS EMS Desktop Client, change the Login URL under Configuration > Everyday User Applications > Web App Menus.
    a. Select Login.aspx and click Edit
    b. Enter in the URL to your Remote Service Provider
7. Configure your remote Service provider to send the user back to the default.aspx page of the web application that the request originated from.

EMS Desktop Client Configuration

Please reference our Portal Authentication section for further details around the configuration required within EMS. There are a number of different options available. You will need to know the method that the

user identifying value will be passed and the name of that value. Other values can also be passed (ie: email address and phone number) to aid in automatic web user account provisioning as well.

Session Method

A session is a way to provide/maintain user state information in an inherently stateless environment. It provides access to a session-wide cache you can use to store information.

In order to use the session method, set the Portal Authentication Method parameter to Session and type the appropriate variable for the Portal Authentication Variable parameter. Then you must create an asp.net web page and name it with the .aspx extension similar to the example below. The asp.net web page created must be copied into the EMS Web App root web directory. It must be copied there in order for EMS Web App to read the session variable.

You will need to pass through the user's email address or external reference to your asp.net web page.

Code example in vb.net:

```
<%@ Import Namespace="System" %>

<script runat="server" language="vb">

    Sub Page_Load(ByVal sender As System.Object, ByVal e As System.EventArgs)

        Session.Item("EMS Web AppSession") = "test@emssoftware.com"

        Response.Redirect("Default.aspx")

    End Sub

</script>
```

Form Method

Forms enable client-side users to submit data to a server in a standardized format via HTML. The creator of a form designs the form to collect the required data using a variety of controls, such as INPUT or SELECT. Users viewing the form fill in the data and then click Submit to send the data to the server.

To use the form method, set the Portal Authentication Method parameter to Form and type the appropriate variable for the Portal Authentication Variable parameter. To create portals through a form, create a web page with a form similar to below. Once the user logs on through the portal, the form below can be submitted to log the user on to EMS Web App.

Code example in HTML:

```
<Form name="form1" method="Post" action=" http://[ServerName]/ EMSWebApp/Default.aspx ">
```

```
<input type="hidden" id="EMS Web AppFORM" name="EMS Web AppFORM"
value="test@emssoftware.com>

<input type="submit" value="submit">

</form>
```

Cookie Method

A cookie is a small piece of information stored by the browser. Each cookie is stored in a name/value pair called a crumb—that is, if the cookie name is "id" and you want to save the id's value as "this", the cookie would be saved as id=this.

You can store up to 20 name/value pairs in a cookie, and the cookie is always returned as a string of all the cookies that apply to the page. This means that you must parse the string returned to find the values of individual cookies. Cookies accumulate each time the property is set. If you try to set more than one cookie with a single call to the property, only the first cookie in the list will be retained.

To use the cookie method, set the Portal Authentication Method parameter to Cookie and type the appropriate variable for the Portal Authentication Cookie Key parameter. Then create a web page with code similar to below. Once the user logs on through the portal, take their user logon information and create a cookie. After the cookie is created send the user to your EMS Web App Default.aspx page.

Code example in Active Server Pages 2.0:

```
<%@LANGUAGE="VBSCRIPT" %>

<%

    Response.Expires = -1

    Response.Cookies("EMS Web AppCookie")("CookVal") = "test@emssoftware.com"

    Response.Cookies("EMS Web AppCookie").Path = "/"

    Response.Cookies("EMS Web AppCookie").Expires = DateAdd("m", 3, Now)

    Response.Redirect("http://[ServerName]/ EMSWebApp/Default.aspx ")

%>
```

Query String Method

A query string is information appended to the end of a page's URL. An example using portal authentication is below.

Code example:

```
http://[ServerName]/ EMSWebApp/Default.aspx?MCQS=test@emssoftware.com
```

To use the query string method, set the Portal Authentication Method parameter to Query String and type the appropriate variable for the Portal Authentication Variable parameter.

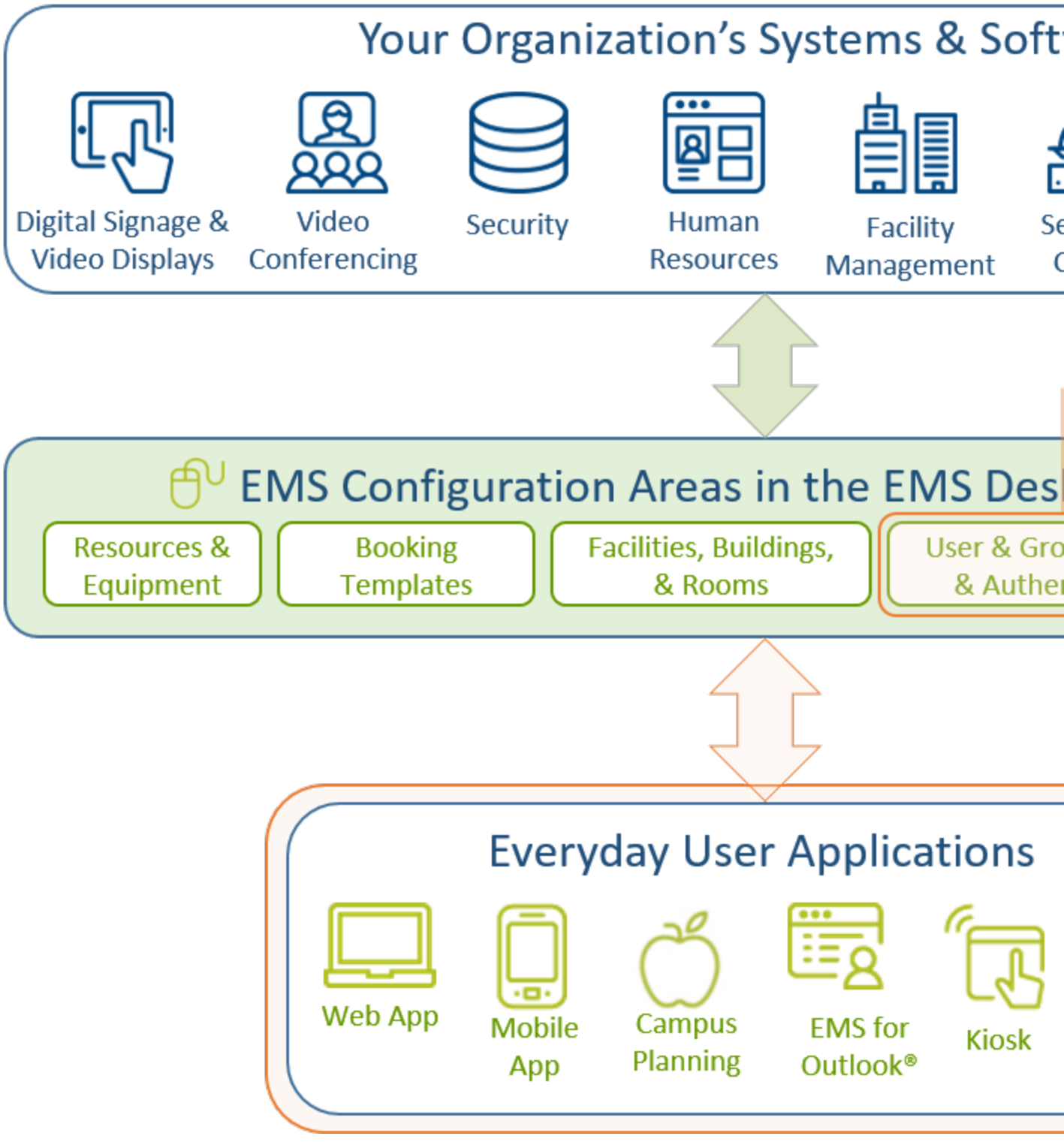
CHAPTER 17: Introduction to EMS Integration to Microsoft® Exchange

EMS Integration to Microsoft® Exchange is a component that integrates EMS Everyday User applications, such as EMS Mobile App, EMS for Outlook and EMS Web App, with Microsoft® Exchange. This module enables everyday users to view the availability of both meeting rooms *and* attendees, and send Outlook® meeting invitations, all from within EMS Everyday User applications.

This guide provides instruction for installing Integration to Microsoft® Exchange for System Administration and IT users. The following information is included in this guide:

- System Requirements for Integration to Microsoft® Exchange
- Install or Upgrade the Exchange Integration Web Service
- Configure Integration to Microsoft® Exchange
- Use Application Pool Identity for Integration for Exchange Service Account
- Configure EWS Impersonation for Microsoft® Exchange
    - Learn More About Exchange Web Services (EWS) Impersonation

Exchange Integration Flow



You must be licensed for EMS, EMS Web App, and Integration to Microsoft® Exchange in order to configure and use this feature. If you are unsure if your organization is licensed for Integration to Exchange, or if you would like to learn more about it, please contact your Account Executive.

To install and configure Integration to Exchange, you will:

- Install the Exchange Integration Web Service
- Configure EMS Integration to Exchange
- Configure EWS Impersonation for Exchange Online (Office 365)

The following requirements must be met to install and configure Integration to Microsoft® Exchange. See Also: System Requirements for Integration to Microsoft Exchange.

- EMS and/or EMS Web App Installed
- EMS must be installed and operational
- Valid Outlook Integration License

CHAPTER 18: System Requirements for Integration to Microsoft® Exchange

You must be licensed for EMS Desktop Client, EMS Web App, and Integration to Microsoft® Exchange to configure and use this module. If you are unsure if your organization is licensed for Integration with Exchange, or if you would like to learn more about it, please contact your Account Executive.

The following requirements must be met to install and configure Integration to Exchange:

- System requirements must be met for the following:
  - EMS Web Server
  - EMS Web App
  - EMS Platform Services
  - EMS for Outlook and Integration to Exchange
- EMS Desktop Client and/or EMS Web App Installed
- EMS Desktop Client must be installed and operational
- Valid EMS for Microsoft Outlook License

Web Server Requirements

EMS Web App Requirements

IMPORTANT: Integration with Exchange configuration issues often relate to access rights with this account. Please ensure that the account has the necessary permissions.

EMS Platform Services

EMS for Microsoft Outlook Requirements

CHAPTER 19: Install or Upgrade the Exchange Integration Web Service

Prior to Install or Upgrade

IMPORTANT: Before beginning the installation process, complete the following steps.

1. Install or upgrade your EMS databases as outlined in the EMS Desktop Client Installation Guide.
2. Manually uninstall any previous versions of the Exchange Integration Service on your web server.
3. If you are upgrading from previous versions, update your parameter settings for "PAM Web Service URL" to "Exchange Integration Web Service URL"
   (i.e., http://server/ExchangeIntegrationWebService). See Also: EMS Web App Parameters.

Install or Upgrade Instructions

1. Verify that the requirements outlined in the System Requirements section have been met.
2. Download ExchangeIntegrationWebService.msi onto the web server that will be running the service.
3. Run ExchangeIntegrationWebService.msi.
4. The first screen welcomes you to the Exchange Integration Service Setup Wizard. Click Next to begin the installation process. The Destination Folder screen will appear.
5. Select the destination folder. The installation process will create a new physical directory on your web server based on the destination folder path entered ("ExchangeIntegrationService" in the example above.) Click Next.
   NOTE: The Exchange Integration Service should not be installed in the same physical directory as other EMS web-based products.
6. The SQL Server and database information screen will appear.
7. Enter your EMS SQL Instance Name.
8. Enter your EMS Database Name, typically named "EMS".
9. Click Next. The Virtual Directory information screen will appear.
10. The Virtual Directory Name will default to the destination folder specified in Step 5. It is recommended that you keep the default setting. The installation process will create a virtual directory on your web server based on the virtual directory entered ("ExchangeIntegrationWebService" in the example above.) Click Next.
    NOTE: The Exchange Integration should not be installed in the same virtual directory as other EMS web-based products.

11. The Ready to Install Exchange Integration Web Service screen will appear. Click Install to install the Exchange Integration.
12. The Completed the Exchange Integration Web Service Setup Wizard screen will appear. Click Finish.
13. After following the steps above, verify your installation by opening a browser and entering the following:
    http://[ServerName]/ExchangeIntegrationWebService/Service.asmx
    (replace [ServerName] with the name of your web server)
    IMPORTANT: A standard installation requires that the Exchange Integration be published without any authentication methods in place (e.g., Integrated Windows Authentication or Portal Authentication). If you require the Exchange Integration to be secured with authentication, additional configuration is necessary. Contact your implementation consultant for further details.

CHAPTER 20: Configure Integration to Microsoft Exchange

NOTE: As of 44.1, Update 24, the testing function on pamconfig.aspx will test the FindItems, GetUserAvailability, Create, Edit, and Cancel EWS calls used by the EMS integration. Previously, only FindItems was tested. There is not necessarily a 1:1 guide as to what would cause a failure for each specific call, however this does not mean that scenarios exist where 'create' would succeed but 'cancel' would fail for example. The 'GetUserAvailability' call does not leverage ApplicationImpersonation, so if this is succeeding and the create/edit/cancel calls are failing then the issue is likely around permissions for the service account. Testing will be logged in the logfile, which has a default location of ExchangeIntegrationWebService\LogFiles and can be modified in the web.config file.

Configuring EMS to work with Exchange Online (Office 365) or Exchange 2013 is the same as configuring EMS to work with a 2007/2010 Exchange environment that is hosted on your network. See Configure EWS Impersonation for Microsoft® Exchange for information on configuring impersonation on Exchange Online (Office 365). If you need additional assistance configuring this, please contact support@emssoftware.com.

NOTE: Integration to Exchange requires the use of a mail-enabled service account that has the Application/Impersonation role in Exchange for all users who will be accessing EMS. See Also: Configure Exchange Web Service Impersonation.

This topic provides information on the following:

Configure Integration to Exchange Instructions

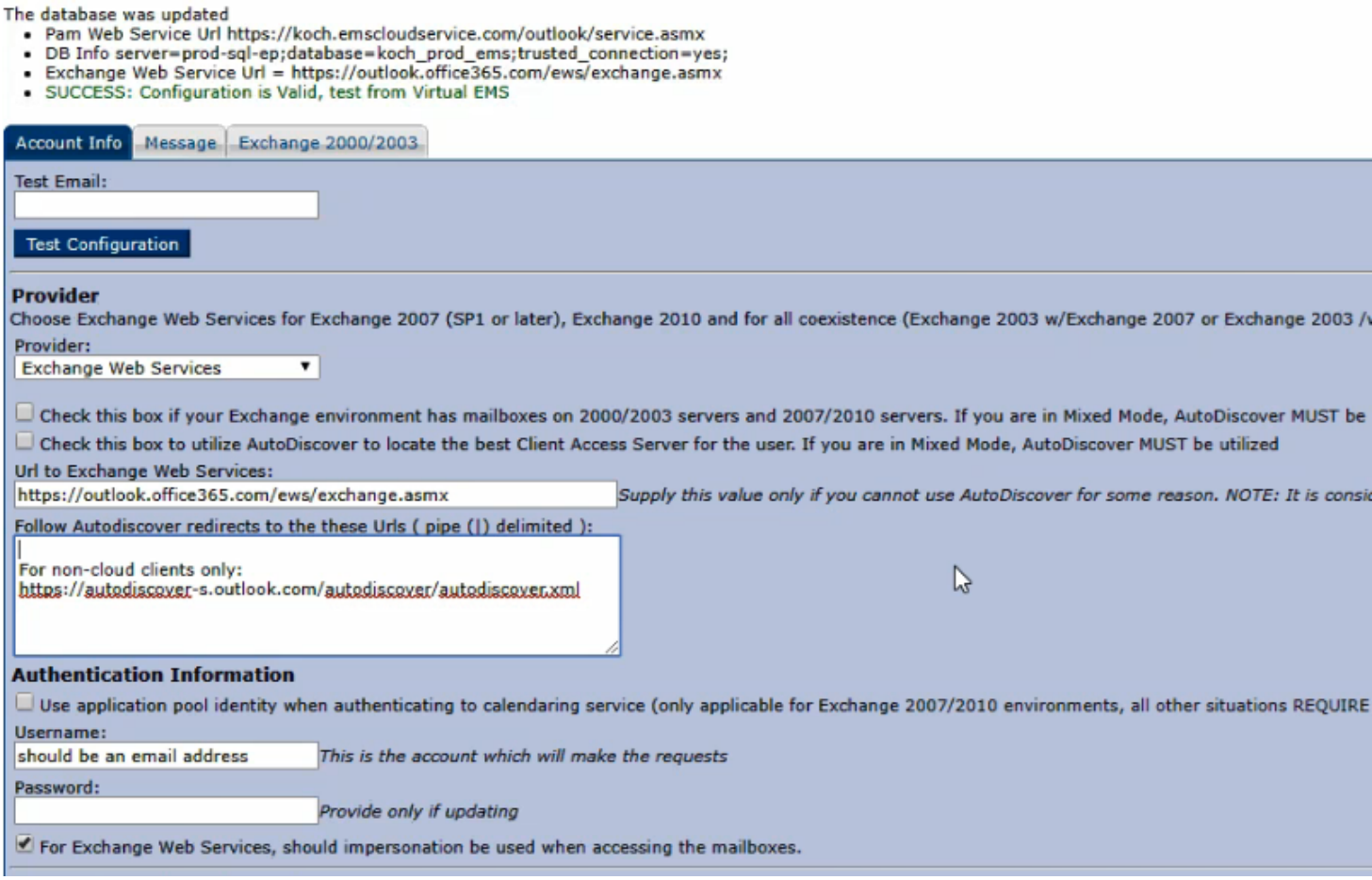
Important: As of Update 28, access to the PAMconfig.aspx page is restricted by default. Customers who do not enable Windows Authentication in IIS for the Exchange Integration Web Service should comment out the following section in order for EIWS to work properly:

```
<remove users="*" roles="" verbs=""/>

<add accessType="Allow" roles="Users"/>”
```

1. After following the installation instructions, access the Integration to Exchange configuration area by opening a browser and entering the following: http://[ServerName]/ExchangeIntegrationWebService/PamConfig.aspx (replace [ServerName] with the name of your web server)
2. Go the Account Info tab.

Office 365 Configuration Example



3. Select your email system in the Provider drop-down list using the instructions provided on the page.
4. Check the box "... utilize AutoDiscover to locate the best Client Access Server for the user..." NOTE: If you do not check this box, you must fill in the Url to Exchange Web Services field.
5. Within the Authentication Information section, enter your Integration to Exchange Account User Name and Password. The User Name should be prefixed with your domain (example – YourDomain\Integration to Exchange Account, or Integration to Exchange Account@YourDomain) . TIP: Make a note of this URL for use later in this topic.

6. (*Optional*) The "Use application pool identity…" option allows you to set the Integration to Exchange Account credentials at the Application Pool level instead of storing the credentials in the EMS database. See the Use Application Pool Identity for Integration for Exchange Service Account topic for more information about this option. If this option is selected, you must check the box to use Impersonation.
7. If you selected "Exchange Web Services" as your Provider, select the checkbox if the account specified has Exchange Impersonation access to all mailboxes in your Exchange mailbox store.
8. Select the Authentication Type:
   - Anonymous – No authentication
   - Specify Account – Relies on a custom account (not the Integration to Exchange Account) that you create and manage. Please contact Customer Support (or a member of the Professional Services group if you are working with one) to discuss the configuration process for this option.
   - Default Credentials – Relies on security context of EMS application calling the Integration with Exchange Web Service. If using this option, Integrated Windows Authentication should be enabled for the Integration with Exchange Web Service.
   - For MS Exchange 2007/2010 environments, click Save.

   NOTE: When testing Integration to Exchange, the email account that is being used (either on the Test Settings tab or in the Testing Integration to Exchange section below) MUST exist in the Exchange environment being tested. If you are testing Integration with Exchange in a development environment, please verify that a mailbox for the email being used exists in that domain/environment.
9. Click Test Configuration. If any errors are encountered, please verify your configuration. Otherwise, your Integration to Exchange configuration is complete.

Test Your Exchange Integration

To test your configuration, you will need to log into EMS Web App with a user account (configured with the user's primary email address) belonging to a Everyday Application Process Template (within the EMS client application) that has the Enable Integration to Microsoft Exchange option checked.

1. Log into EMS Web App. Begin making a reservation and selecting a room.
2. Select the Add to my calendar checkbox. If this option is not available, please verify (within the EMS client application) that your user account belongs to a Everyday User Process Template that has the Allow Invitations option checked.
3. Find and add an attendee using the Find Attendee field.
4. Complete necessary information on the Details tab and click Submit Reservation.
5. Verify that an appointment was added to your Outlook Calendar and that your attendee received an invitation.

Optional Messaging Settings

The options on the Message tab (as reached above in Step 2) shown below guide you in further configuring your integration.

Message Tab Fields

FIELD	DESCRIPTION
Message To Append	Message appended to the bottom of the appointment body. This message is seen by all users.
To view the details of this reservation click the below link	Message added to the appointment body, above a link that takes a user to a view-only EMS Web App page for the appointment. This message is seen by all users.
If you are the meeting organizer click the below link to	Message added to the appointment body, above a link that takes the meeting organizer to the EMS Web App Reservation Summary page for that reservation. This message is seen by all users, but only the meeting organizer can access the Reservation Summary page to make changes.

FIELD	DESCRIPTION
edit the reservation	
Allow Attachments	Allows users to add attachments within EMS Web App when making an appointment.
Maximum Attachment Size	If attachments are allowed, set the maximum file size allowed for an attachment.

Concept: The default installation allows file attachments up to 4MB.
If your implementation needs file attachments that are larger, follow the two procedures below:

1. Update the config file.
2. Update the database.

NOTE: File sizes larger than 2 GB are not allowed at this time.

Enable Larger File Attachments On The Config File

By default, Exchange Integration attachments will only accept files 4MB or less. If your implementation needs to allow files of larger sizes to be attached to reservations, the following config updates will be required, both in EMS Web App and in the Exchange Integration Web Service.

IMPORTANT: The maximum file size is 2 GB.

1. In the <system.webServer> section, include this xml node:

```
<security>
      <requestFiltering>
        <requestLimits maxAllowedContentLength="51200000"/> <!--
maxAllowedContentLength in bytes, 50MB=51200000-->
      </requestFiltering>
    </security>
```

2. In the <httpRuntime element, add these highlighted attributes with the end result looking like this:

```
<httpRuntime targetFramework="4.5" requestLengthDiskThreshold="214-
7483644"
maxRequestLength="51200"  />  <!--requestLengthDiskThreshold in
bytes, & maxRequestLength in KB, 50MB-->
```

3. Under the <appSettings> look for the "MaximumUploadSizeInBytes" key. Update this value to the number of bytes allowed. For instance, 50MB would look like this:

```
<add key="MaximumUploadSizeInBytes" value="52428800000"/>  <!--
in bytes50MB-->
```

Enable Larger File Attachments in the Exchange Integration Web Service

By default Exchange Integration attachments will only accept files 4MB or less. If your implementation needs to allow for Exchange message attachments larger than 4MB, the config updates above will need to be applied in the Exchange Integration Web Service.

NOTE: Due to the size of the xml sent, we recommend adding 5MB to the desired file upload size. (i.e., if you want to allow a max of 20MB files, calculate a total of 25MB worth of Kilobytes and bytes.

In addition to these web.config settings above, a web administrator will need to update the file size in the Exchange Integration Web Service as follows:

1. Navigate to the Exchange Integration Web Service/PAMConfig.aspx
2. Click the Message tab
3. Update the Maximum Attachment Size text box and Save.

WARNING: For Externally Exposed Web App sites

If your EMS Web App site is externally exposed, some of the web.config settings above could make the site vulnerable to DoS site attacks. We highly recommend setting network-level protection to prevent DoS attacks.

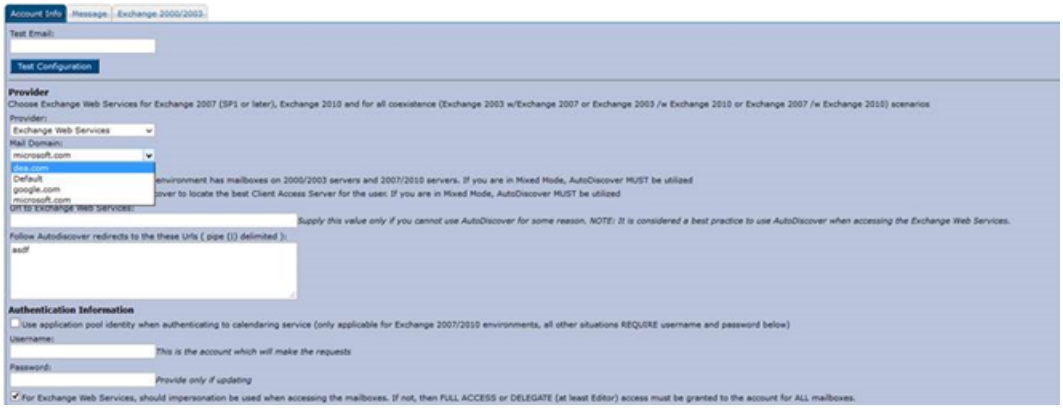
CHAPTER 21: Configure Multiple Mail Domains

To configure multiple mail domains, you must edit the web.config file. This will enable the Mail Domain drop-down that allows Administrators to specify different EWS URLs, AutoDiscover settings, and authentication options based on the domain.

When an EIWS booking is made through EMS for Outlook or the EMS Web App, it will automatically pull the domain from that user's email address. It will then use the corresponding Mail Domain option.

1. Open the web.config file.
2. Navigate to the mail domains line at the top under the Configuration section.

3. Remove the comment marks (<!-- -->) and add your domains to the value (e.g., `<add key="mailDomains" value="dea.com|google.com|microsoft.com"/>`
4. Save your web.config file. You will now see the Mail Domain drop-down menu on the pamconfig.aspx screen. Each menu item will have its own Provider area.



5. Test your Exchange Integration.

NOTE: These settings are stored in the tblPamSettings table.

CHAPTER 22: Use Application Pool Identity for Integration for Exchange Service Account

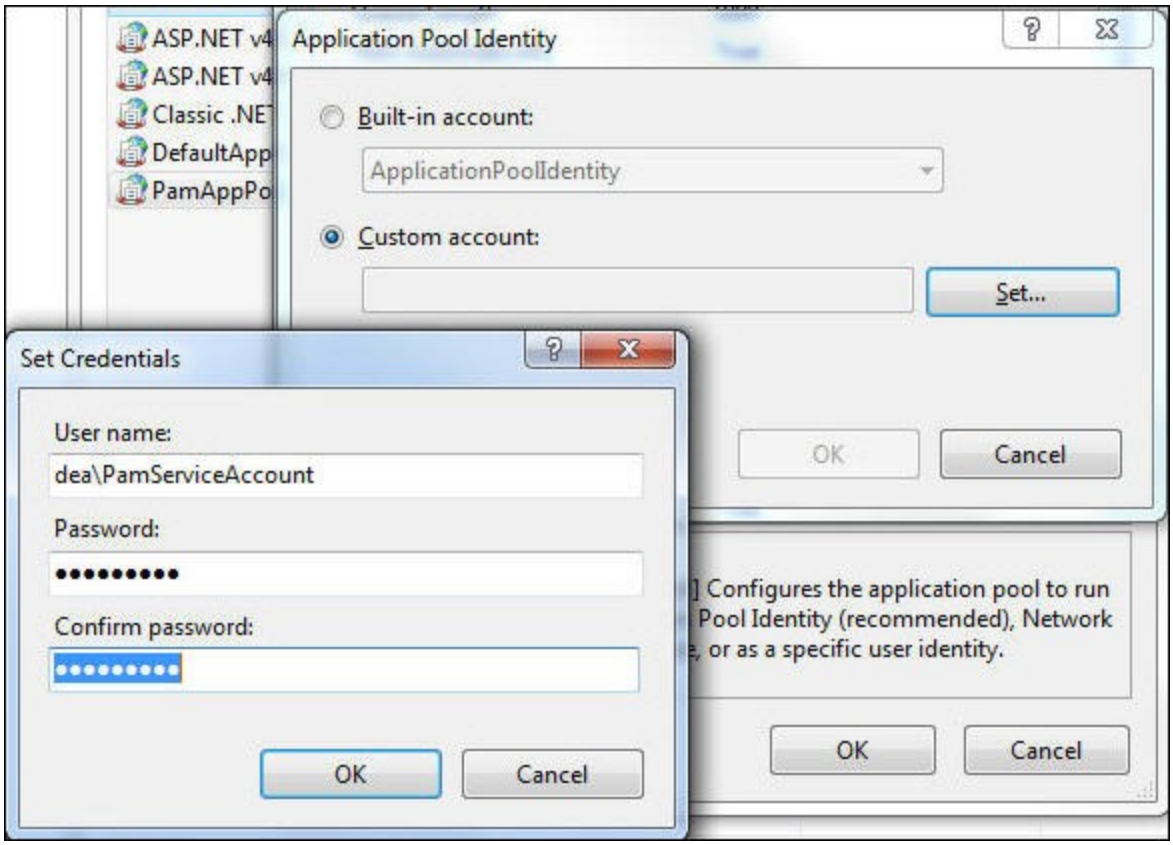
Rather than entering the Integration for Exchange account credentials on the PAMConfig.aspx page (as in V44 and previous releases), credentials can be maintained at the Application Pool level. This allows your organization to maintain absolute control—only IIS applications running in the newly created application pool can run as the Integration to Exchange Account.

This functionality requires the following:

- Microsoft Exchange 2007 (SP1) or Exchange 2010.
- Microsoft Exchange Impersonation Account (your EMS Integration to Exchange account). This account must be using Exchange Web Services (EWS) Impersonation, not full access to the mail-box store.

Configure the Application Pool

1. Open IIS Manager
2. Open the Application Pools panel
3. Click Add Application Pool…
4. The Add Application Pool window opens. Enter a unique name and ensure the correct .NET Framework is selected. Managed pipeline mode should be Integrated. Click OK
5. Find the Application Pool you just created. Right-click it and select Advanced Settings.
6. The third section in the list is Process Model. Highlight Identity and then click the (…) button to con-figure.
7. Choose Custom Account and then click Set. Enter the username and password for your EMS Integ-ration to Exchange account. Confirm the password and click OK on any remaining dialogs (see fol-lowing image).



8. Within IIS Manager, navigate to the Virtual Directory containing the Integration for Exchange Web Service. This is under the Default website by default, but can be installed to a different website.
9. With the IntegrationExchangeWebService Virtual Directory highlighted in the left pane, select Basic Settings… under Actions in the right pane.
10. Click the Select button and then choose your newly created application pool from the list.
11. Click OK on all remaining dialogs.

Configure Integration for Exchange to Use the Application Pool Account

1. Navigate to the Integration for Exchange configuration area by opening a browser and entering the following:
   http://[ServerName]/PAMWebService/PAMConfig.aspx (replace [ServerName] with the name of your web server)
2. From the Account Info tab, find the Authentication Information section, check the box for Use application pool identity when authenticating to calendaring service (see following image).
3. With this option enabled, you can leave the Username and Password fields blank in the Authentication Information section.

4. Click Save button at the bottom of the page.

CHAPTER 23: Configure EWS Impersonation for Microsoft® Exchange

NOTE: The service account requires a mailbox and must be mail enabled. EMS Software recommends disabling the password expiration for these accounts.

1. Log in to the Office 365® Exchange Administration Center. For Microsoft Exchange 2010, please see here.
2. Create a Service Account User within your Office 365 Environment.
   OR
   Configure a already migrated account.
3. Select Exchange > Admin Roles from the navigation tree.
4. Click the + icon to add a new role
5. In the role group dialog box, provide a name for your Role Group (e.g. "EMS_Exchange_Impersonation"). It is also helpful to enter a Description.
6. Under Role, click the + icon to add the "Application Impersonation" Role.
7. Under Members, click the + icon and find your Exchange Service Account.

TIP: For more information on EWS Impersonation, see What is EWS Impersonation?

CHAPTER 24: Learn More About Exchange Web Services (EWS) Impersonation

EMS offers two Exchange integration options to enable seamless room, resource, and attendance scheduling:

1. EMS Integration to Exchange offers users the convenience of scheduling rooms, resources, and services, confirming attendee availability, and managing Outlook invitations via EMS Web App (our web-based reservation tool). See Also: Installation Overview.
2. EMS for Outlook lets users find available rooms, review their details, reserve them and book any necessary resources (equipment, etc.) without ever leaving Microsoft® Outlook.

To achieve this seamless interaction between everyday users, Outlook hosts, and EMS administrators, an account with Exchange impersonation access to all mailboxes in your Exchange mailbox store is required.

See Also: Configure EWS Impersonation for Microsoft® Exchange

FAQs

Why is this account necessary?

Meetings created via EMS Integration for Exchange either on EMS Web App or EMS for Outlook are owned by the host and associated with a specific Exchange account. That Exchange user can move, update, or cancel the event. However, these meetings can also be moved, changed, or canceled by IT admins and expert users in EMS Desktop Client. When a reservation is moved, changed or canceled in the client, EMS must be able to update the record on the host's Exchange account. Co-ownership of events between the meeting host and the EMS administrators necessitates an account that can read and write to all Exchange accounts being used for booking.

Can we exclude people from impersonation? (For example, remove CEO, Board of Directors, etc. from being impersonated.)

Microsoft Exchange Server supports a CustomRecipientScope parameter when defining the impersonation role. You can define a scope of included users by implementing this parameter.

Is there any way that we could use a delegation feature (like allowing office admins delegate rights) instead of impersonation to notify hosts of updates/changes?

Delegation is possible, here are some things you should know:

- The account needs Editor w/Folder owner (so a custom rights set).
- Custom rights, at least through exchange 2010, are not scriptable. This means the delegation account will get set to owner, which is the only built in (read scriptable) option that has all the necessary permissions.
- EMS for Outlook creates a custom property on the Calendar folder, which allows you to programmatically search the folder for items that have the custom property. Once that custom property is created, then Editor will be enough. It is the creation of the custom property at the folder level that requires owner permission.
- While you can use PowerShell to script the permissions and loop through the users and set the permissions (owner), you would need to make sure that the script got applied to any new users and reapplied to any users that have changed the permissions of the delegation account
- Rights are granted to ANY mail client (Outlook, OWA, etc): when using the impersonation account, rights are only granted to Exchange Web Services, so nobody could type in the service account into Outlook and gain the same permissions.
- These rights are visible to the end user. For example, if an account, "EMSExchangeAccount", has been granted, delegation rights (any level) to User1's calendar, and User1 goes to the Permissions tab of his calendar, he will see the EMSExchangeAccount and the rights it is assigned. Additionally, User1 would be able to change the rights, which would essentially disable the Exchange integration.
- This restricts access only to the calendar

By contrast, EWS impersonation provides the following alternatives to delegation:

- Allows access ONLY through Exchange Web Services
- Does grant permission to do anything the impersonated user could do (assuming it is available as part of EWS)
- End users do not see (and cannot change) the permissions

Additional Reading

The links below provide additional information from Microsoft® about Exchange Web Services (EWS).

- The Importance of EWS Impersonation
- Authentication and EWS in Exchange
- Impersonation and EWS in Exchange

  With Impersonation, a service account has full access to a defined set of mailboxes. What it can access in those mailboxes (such as specific folders) cannot be filtered or defined. Only an Exchange Admin can configure an EWS Impersonation account for impersonation and configure its mailboxes to allow the impersonation.

- Delegate Access and EWS in Exchange

  Delegate access allows a user to access certain folders in another user's mailbox Delegate permissions can be set by a mailbox owner or administrator using an app or other app code.

CHAPTER 25: EMS for Microsoft® Outlook (Legacy) Configuration Guide

Additional configuration tasks are required in order to enable your Microsoft® Outlook users to access EMS for Outlook functionality.

This guide provides information on the following:

CHAPTER 26: Introduction to EMS for Outlook Configuration Guide

This guide provides information on configuring EMS for Microsoft Outlook Add-in. EMS for Outlook is an optional add-in that integrates the EMS room reservation process directly with Microsoft® Outlook 2010/2013.

Additional configuration tasks are required in order to enable your Microsoft® Outlook users to access EMS for Outlook functionality.

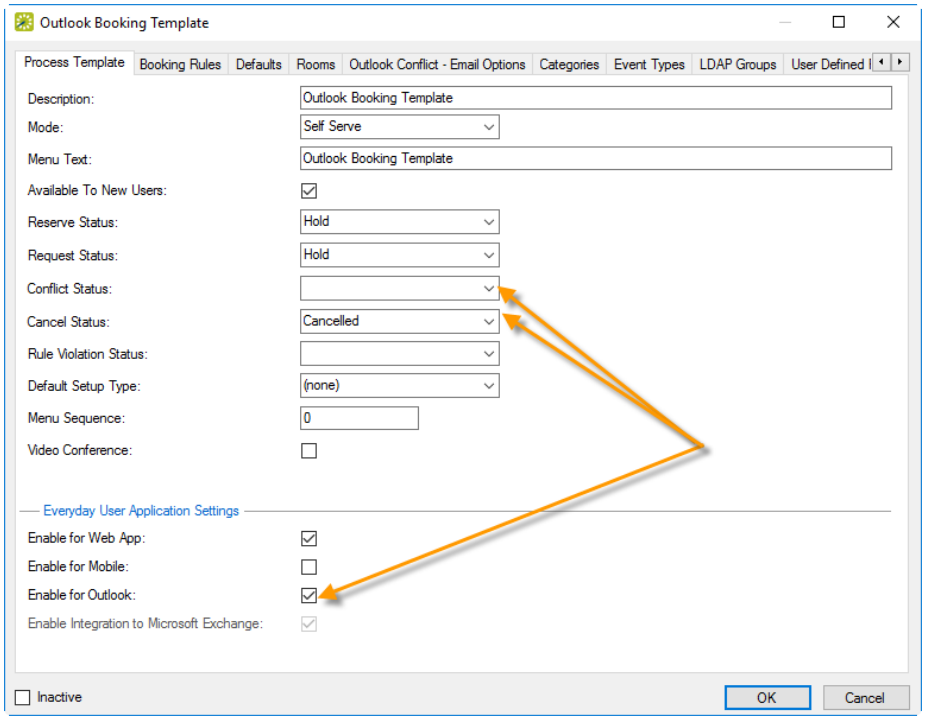
In this section:

CHAPTER 27: Establish Outlook Booking Templates and Conflict Behavior

When you configure Everyday User process templates in the EMS Desktop Client, several options are specific to Outlook functionality. Once you have defined Everyday User Process templates as part of EMS Desktop Client setup, you can make some adjustments in order to fully enable and customize the EMS for Outlook add-in.

1. When defining a Everyday User Process template in EMS Desktop Client setup, select the Outlook option. Below is an example of a new booking template being created for EMS for Outlook bookings.

Note: During the booking process, EMS for Outlook users will be prompted to resolve schedule conflicts by selecting a different space. If they do not select an alternative, the booking enters a conflict status as set below and will not appear on the users' My Events or bookings calendar. If users are unable to find meetings they thought they booked, they might have skipped the conflict resolution step.

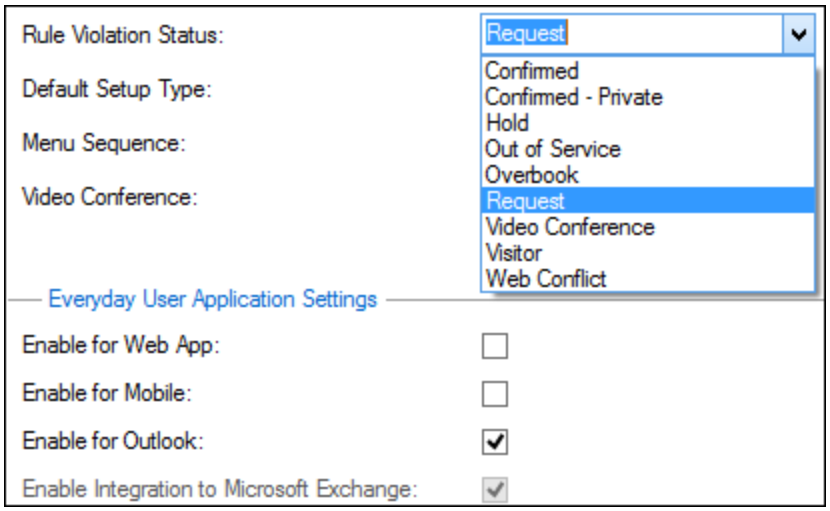


Tip: Use the Outlook Conflict – Email Options tab to control behavior for the notification email sent to the Outlook user if a booking conflict arises during the process of booking through Outlook.

- Enable for Outlook Option—This checkbox enables the template to display to associated everyday users in the EMS for Outlook add-in and enables the Rule Violation Status field available on this

screen.

- Conflict Status—Selections on this drop-down list determine the type of conflict status assigned to bookings made with this template that are in conflict.
- Rule Violation Status—Selections in this drop-down list determine the status of bookings made using to this template that are in conflict. This option is only available Enable for Outlook is selected. When you activate this option and a user in EMS for Outlook request a booking that violates a booking restriction, then the booking is changed to this status. For example, if a EMS for Outlook user requests a room that is already booked and overrides the conflict warning, then the booking is set to the status you specify in this field (such as Overbook or Web Conflict).



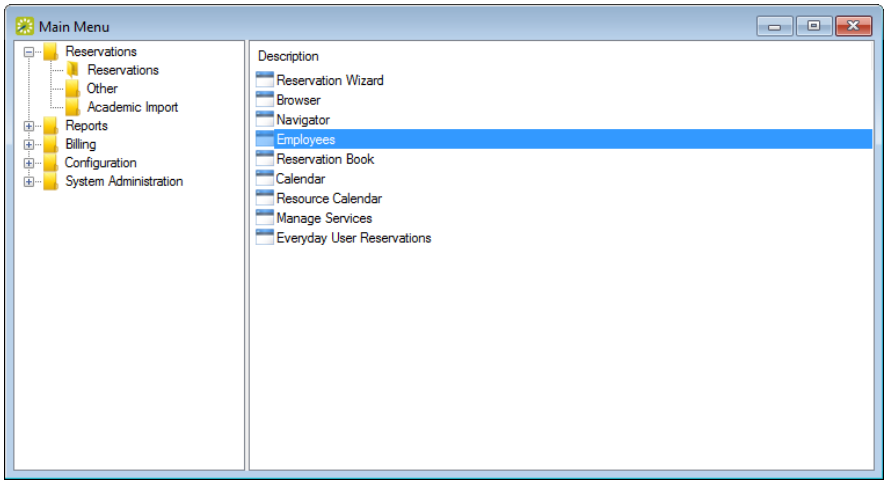
Tip: The values in this drop-down list come from settings in the booking Statuses area of EMS Desktop Client.

2. Complete the remaining tabs.
3. Once you have defined your Outlook Everyday User Process template(s), assign it to your User Account(s).

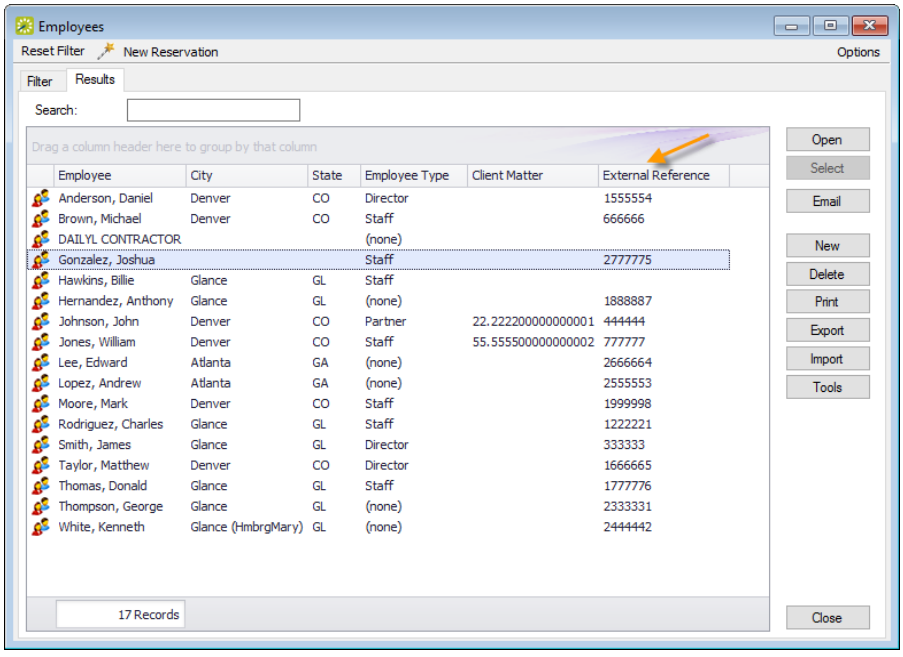
CHAPTER 28: Assign EMS Users to Groups

You assign users to see groups in EMS by modifying their Everyday User accounts via the External Reference field.

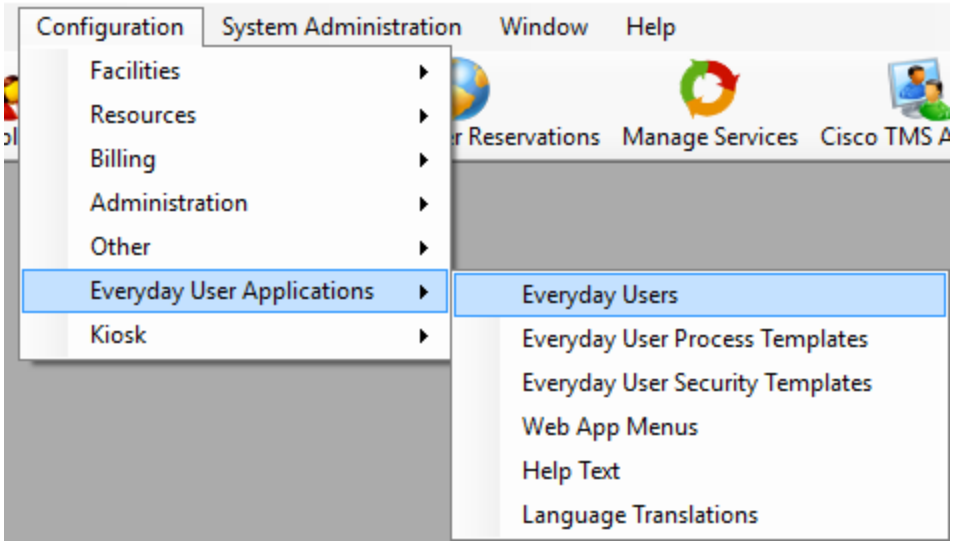
1. Navigate to Billing Information tab within Reservations > Reservations > Employees.



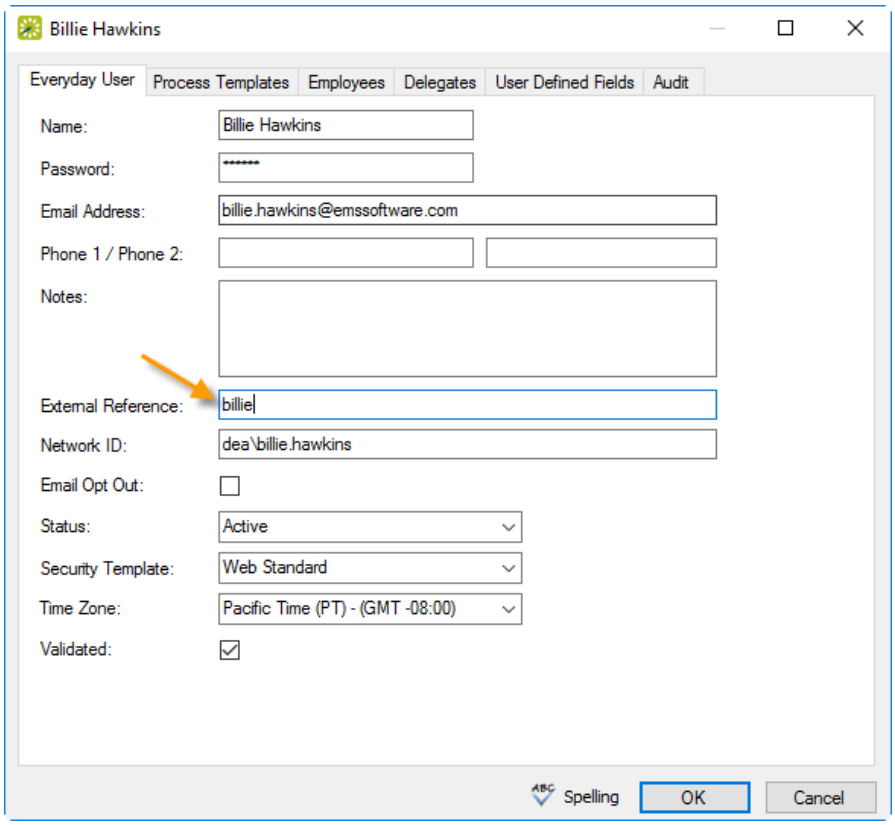
2. Make a note of the value in the External Reference field.



3. Navigate to the Everyday User's account, which is on the Everyday User tab within Configuration > Everyday User Applications> Everyday Users.



4. Open the Everyday User's account by clicking the Edit button. On the Everyday User tab, compare the value above to the value in the External Reference field.

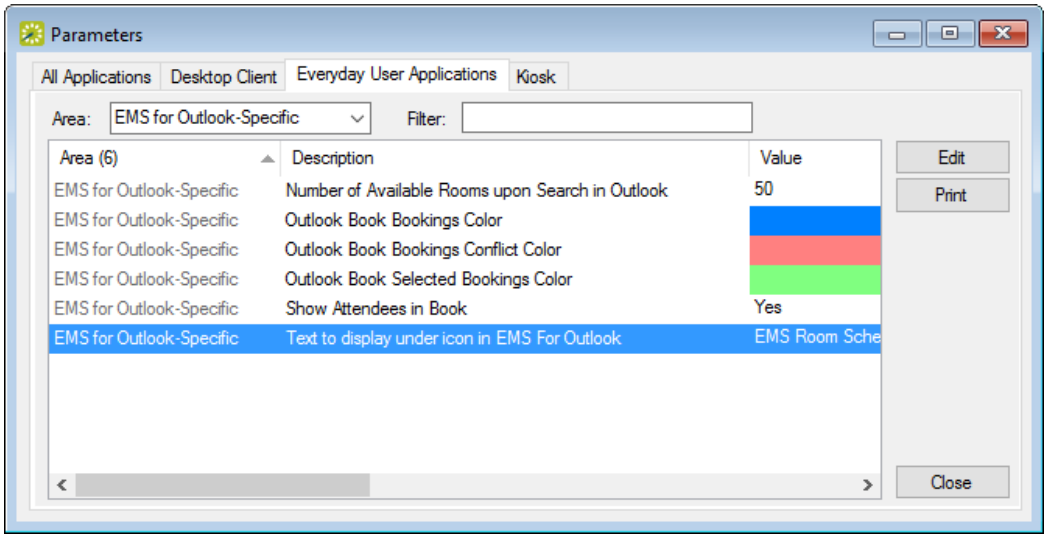


IMPORTANT: These values can be set automatically by administrators if your organization is using the HR Toolkit module. Please see the HR Toolkit Installation Instructions for more information.

CHAPTER 29: Customize the Desktop Application Label

To customize the desktop application label:

1. Log into EMS Desktop Client.
2. Navigate to System Administration > Settings > Parameters and select the Everyday User Applications tab.
3. In the Area drop-down, select EMS for Outlook.
4. Select Text to display under icon in EMS for Outlook and click Edit.



5. Make your changes and click OK. Click Close.

Tip: You can customize other field labels under the All Applications tab (which means your customizations will apply to all EMS applications you deploy); filter the list by selecting "Labels" in the Area field.

Change the EMS for Outlook Icon (hidden future functionality)

- Secure your new icon file. The icon must be of file type BMP, GIF, JPG, or PNG. The new icon should have a resolution of 32 x 32 pixels.
- Name the new logo file CustomLogo.bmp (or other extension listed above).
- Drop the new custom icon into the EMS for Outlook installation directory (e.g. *C:\Program Files (x86)\EMS for Outlook*). This step must be performed after the EMS for Outlook plug-in has been installed on the workstation.

IMPORTANT: Microsoft® Outlook needs to be restarted for either of these changes to take effect. The logo file must be installed on all users' machines.

CHAPTER 30: Enable User Access to EMS for Outlook

Introduction

IMPORTANT: User Access to EMS for Outlook is set in the EMS Desktop Client.

You will need to configure special settings in EMS Desktop Client in order to activate the EMS for Outlook toolbar button for Outlook users. The add-in uses each Outlook user's EMS Everyday User account to establish their room booking privileges based on the Process Template(s) to which the Everyday User is assigned and EMS Group(s) for which the appointment can be booked.

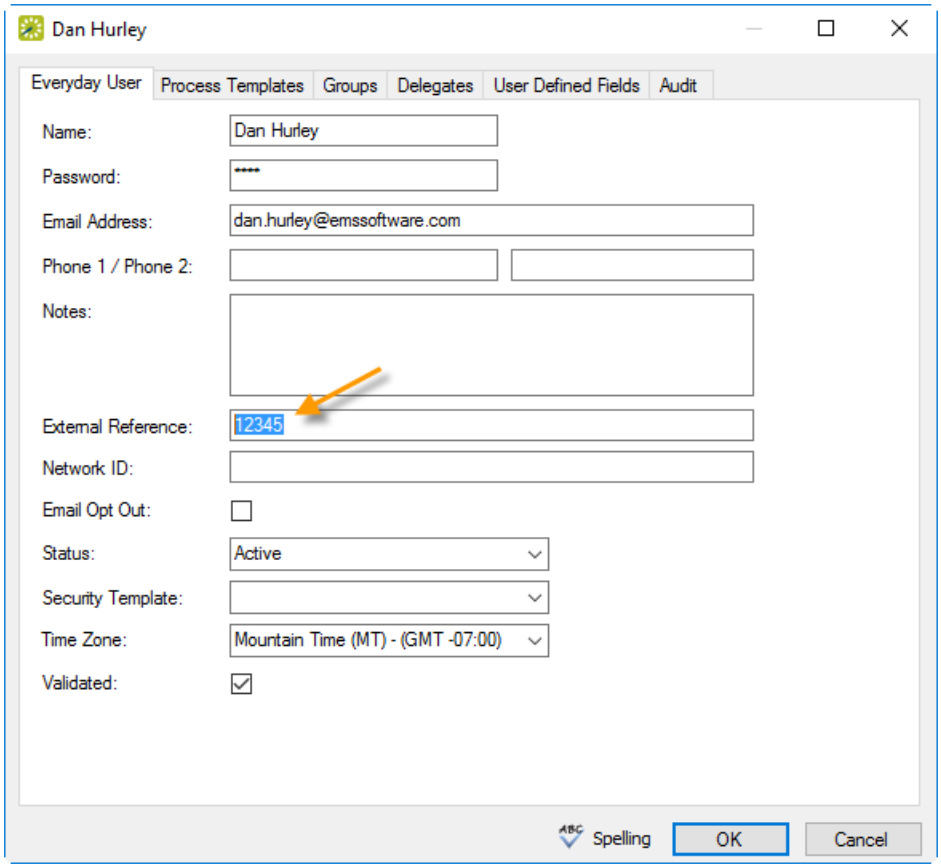
TIP: The optional EMS Integration to Exchange feature enables seamless authentication for this type of user.

To enable EMS for Outlook for your Microsoft® Outlook users, you will:

- Configure the user account (if needed) in EMS Desktop Client
- Assign the user to a process template(s) for EMS for Outlook
- Configure the process template to be available on EMS for Outlook

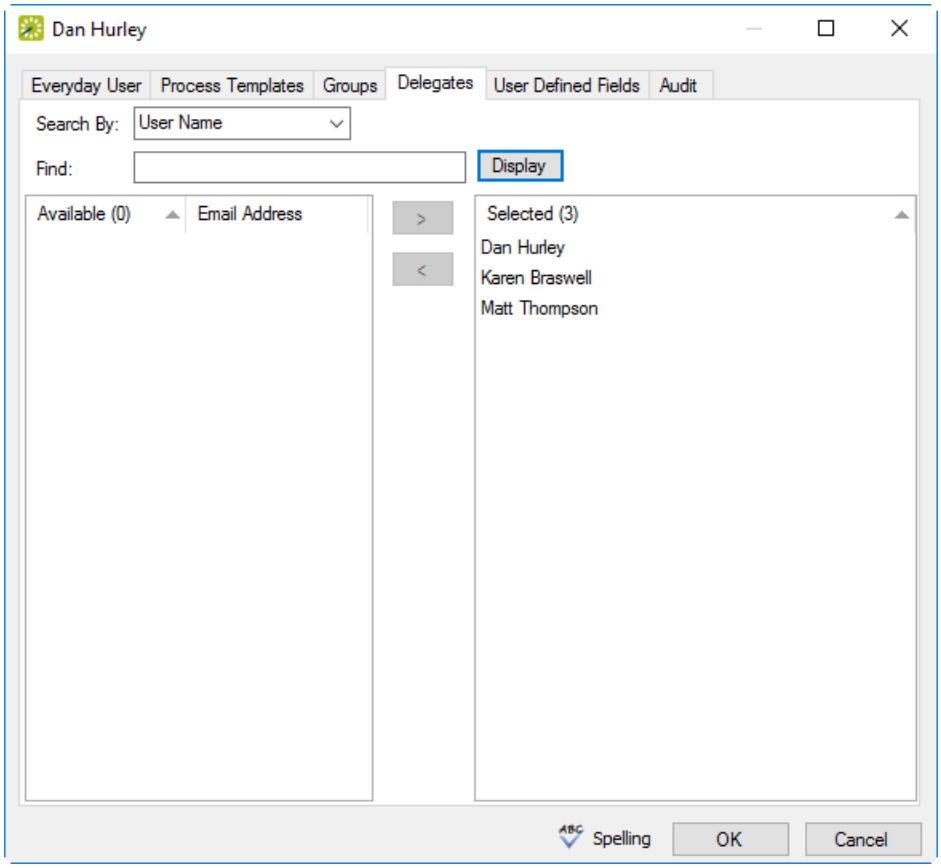
Configure EMS for Outlook Users and Process Templates

1. An active EMS Everyday User account must exist in EMS Desktop Client.
2. The EMS Everyday User account must be linked to an active EMS Group record (via the External Reference field, shown below).

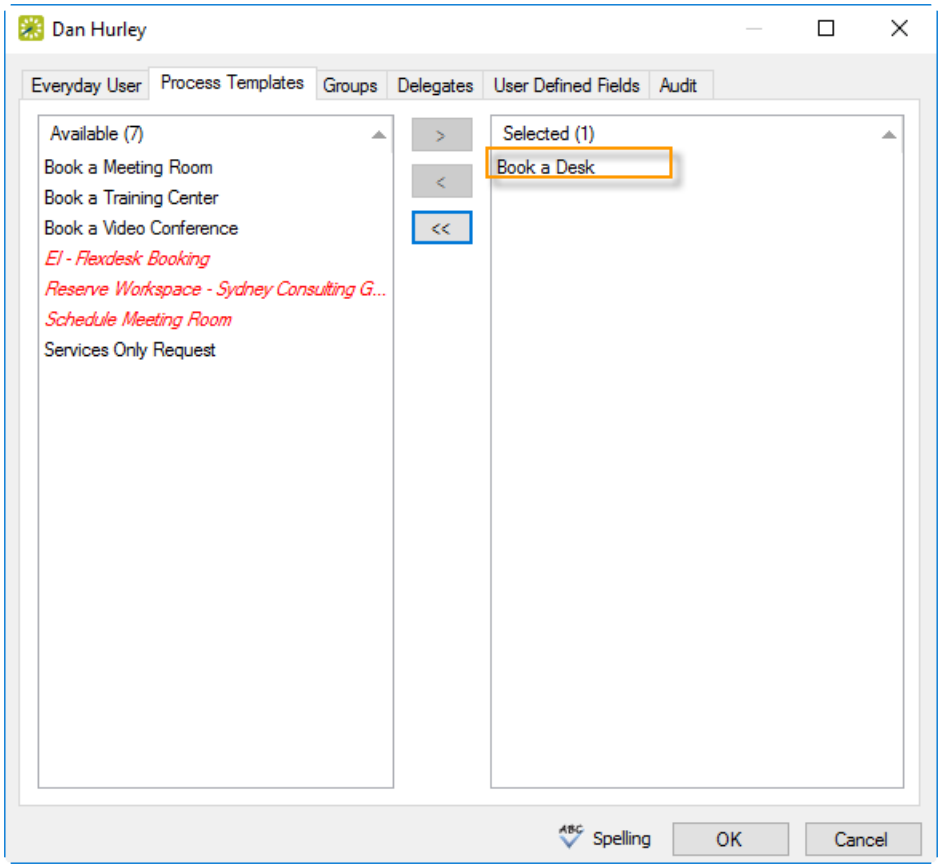


TIP: This topic assumes you have a working knowledge of configuration in EMS Desktop Client and highlights special tasks for enabling EMS for Outlook users.

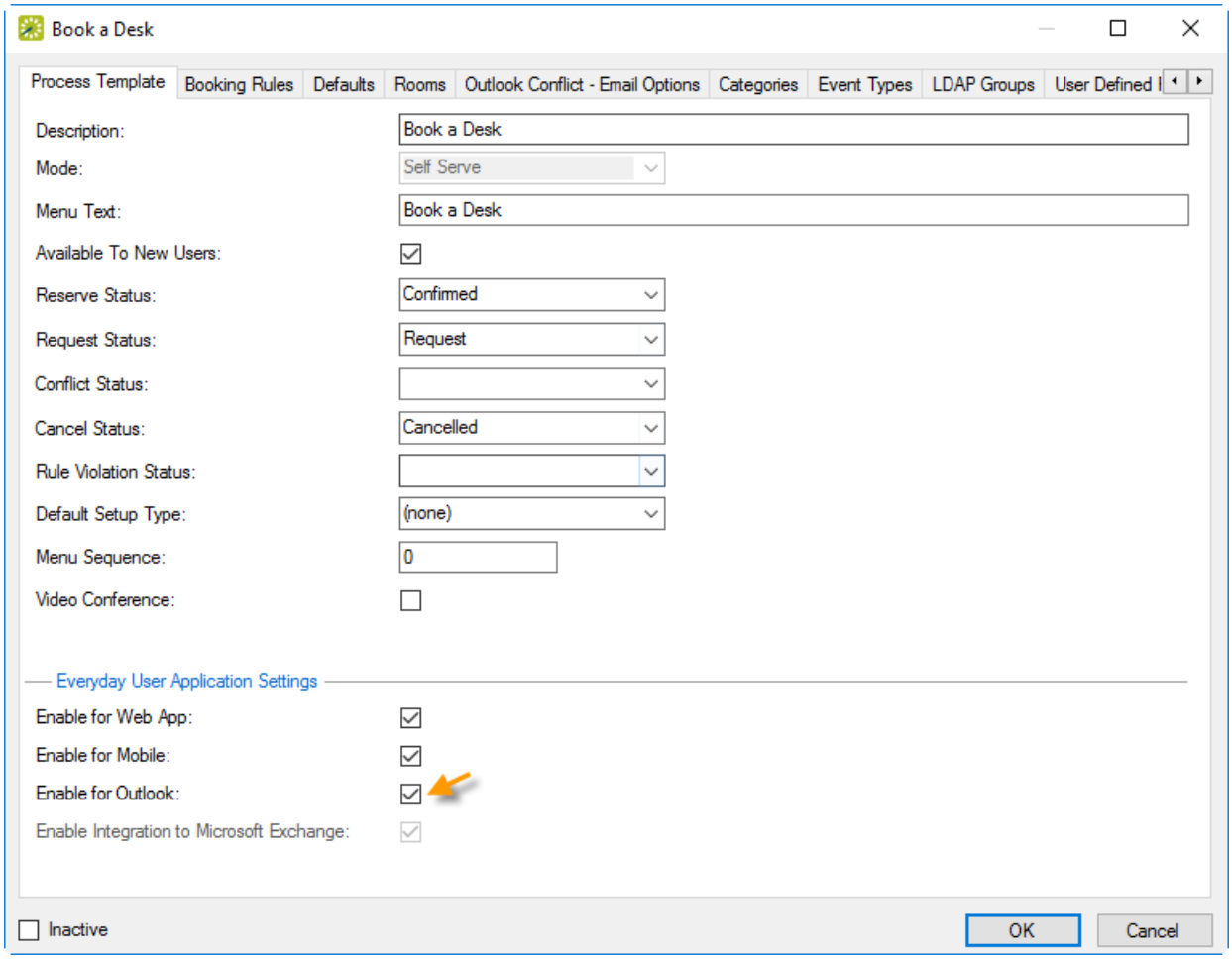
3. The EMS Everyday User must have at least one Delegate associated.



4. The EMS Everyday User account must be assigned to at least one Everyday User Process Template.



5. In the Everyday User Process Template you associate with the user, the Outlook option must be enabled.



TIP: For detailed instructions and additional Everyday User Process Template configuration options, see Establish Outlook Booking Templates and Conflict Behavior.

CHAPTER 31: EMS for Outlook System Parameters

Items highlighted in blue below were added for EMS for Outlook Update 8.

IMPORTANT: Parameters listed here may also affect other EMS applications. The list below summarizes all parameters that affect EMS for Outlook, but they might also affect other Everyday User Applications.

KEYVALUE (TBLREGISTRY NAME)	TITLE	CONFIGURED WHERE?	DESCRIPTION	AREA
VEMS_ResBook_ ShowWhatInBar	Event Information to Display in Booking on Schedule View	Desktop Client > System Administration > Settings > Parameters > Everyday User Applications tab	Determines what information should show in the free/busy bar in the Book. Options include: None, Event Name or Group Name.	Schedule View
VEMS_EmailAccount	Account to Use for Sending Email	Desktop Client > System Administration > Settings > Parameters > Everyday User Applications tab	The email account against which outgoing email from VEMS is authenticated. Only required if the SMTP mail server requires authentication.	Email - Settings
VEMS_ EmailAccountPassword	Password of Email Account	Desktop Client > System Administration > Settings >	The password for the email account. Only required if the SMTP mail server	Email - Settings

KEYVALUE (TBLREGISTRY NAME)	TITLE	CONFIGURED WHERE?	DESCRIPTION	AREA
		Parameters > Everyday User Applications tab	requires authentication.	
VEMS_EmailSender	Name of Email Sender	Desktop Client > System Administration > Settings > Parameters > Everyday User Applications tab	Indicates the "From" name in the reservation summary email generated when an everyday user creates a reservation. Parameter Send Request Summary upon Submit must be enabled, and a reservation summary email must be configured (under Configuration > Everyday User Applications > Everyday User Process Templates > highlight the template and	Email

KEYVALUE (TBLREGISTRY NAME)	TITLE	CONFIGURED WHERE?	DESCRIPTION	AREA
			select Confirmation).	
VEMS_ EmailSenderAddress	Email Address of Sender	Desktop Client > System Administration > Settings > Parameters > Everyday User Applications tab	This entry indicates the "From" email address in the reservation summary email that is generated when a web user submits a reservation. Parameter Send Request Summary upon Submit must be enabled, and a reservation summary email must be configured. (Provide link or reference to where email is configured.)	Email
VEMS_EmailServer	Name or IP Address of SMTP Server	Desktop Client > System Administration > Settings >	SMTP mail server used solely for emails related to everyday user	Email - Settings

KEYVALUE (TBLREGISTRY NAME)	TITLE	CONFIGURED WHERE?	DESCRIPTION	AREA
		Parameters > Everyday User Applications tab	application functionality. This mail server does not apply to emails generated within the desktop client or by any email notification service.	
VEMS_LocationFormat	Location Format	Desktop Client > System Administration > Settings > Parameters > Everyday User Applications tab	Determines how location information is displayed in Browse Events and Create Reservation (List View). Options are Room Code, Room Description, Building Code - Room Code, Building Code - Room Description, Building Description - Room Code,	General

KEYVALUE (TBLREGISTRY NAME)	TITLE	CONFIGURED WHERE?	DESCRIPTION	AREA
			Building Description - Room Description, Building Description.	
vems_Outlook_FilterFirst	Display Filters before showing Rooms	Desktop Client > System Administration > Settings > Parameters > Everyday User Applications tab	Whether to show filter options before listing room availability.	Outlook
VEMS_ReservationBook_StartTime	Start Time on Schedule View	Desktop Client > System Administration > Settings > Parameters > Everyday User Applications tab	Determines the start time for the grid view.	Schedule View
Vems_Reservations_AutoEmailFormat	Format for Request Summary	Desktop Client > System Administration > Settings >	Specify a detailed or summarized report for the reservation	Email

KEYVALUE (TBLREGISTRY NAME)	TITLE	CONFIGURED WHERE?	DESCRIPTION	AREA
		Parameters > Everyday User Applications tab	summary email that is generated when a web user submits a reservation. Parameter Send Request Summary upon Submit must be enabled, and a reservation summary email must be configured. (Provide link or reference to where email is configured.)	
VEMS_Reservations_AutoSendSummary	Send Request Summary upon Submit	Desktop Client > System Administration > Settings > Parameters > Everyday User Applications tab	Determines whether reservation summary information is emailed to the web users when a reservation is submitted. A reservation summary email must be	Email

KEYVALUE (TBLREGISTRY NAME)	TITLE	CONFIGURED WHERE?	DESCRIPTION	AREA
			configured. (Provide link or reference to where email is configured.)	
VEMS_Reservations_AutoSendSummaryOnCancel	Send Confirmation on Cancel	Desktop Client > System Administration > Settings > Parameters > Everyday User Applications tab	Sends the reservation summary if the reservation or a booking is canceled.	Email
VEMS_Reservations_DefaultSubject	Default Subject for Email	Desktop Client > System Administration > Settings > Parameters > Everyday User Applications tab	This entry appears in the Subject line of email the reservation summary email that is generated when a web user submits a reservation. Parameter Send Request Summary upon Submit must be enabled, and a reservation	Email

KEYVALUE (TBLREGISTRY NAME)	TITLE	CONFIGURED WHERE?	DESCRIPTION	AREA
			summary email must be configured. (Provide link or reference to where email is configured.)	
VEMS_Reservations_ShowFeatureList	Show Feature Filter	Desktop Client > System Administration > Settings > Parameters > Everyday User Applications tab	Controls whether Features appear as a search criteria for a room.	Create/Manage Reservations
VEMS_Reservations_ShowFloorList	Show Floor Filter	Desktop Client > System Administration > Settings > Parameters > Everyday User Applications tab	Controls whether Floors appear as a search criteria for a room.	Create/Manage Reservations
VEMS_Reservations_ShowRoomType	Show Room Type Filter	Desktop Client > System Administration	Controls whether Room Types appear as a search	Create/Manage Reservations

KEYVALUE (TBLREGISTRY NAME)	TITLE	CONFIGURED WHERE?	DESCRIPTION	AREA
		> Settings > Parameters > Everyday User Applications tab	criteria for a room.	
PAM_ TextAboveEditLink	The text to display above the edit link	PAM Web Service > PAMConfig.aspx > Message tab	Message added to the appointment body, above a link that takes the meeting organizer to the EMS Web App Reservation Summary page for that reservation. This message is seen by all users, but only the meeting organizer can access the Reservation Summary page to make changes.	PAM
PAM_WebServiceURL	Exchange Integration Web Service	Desktop Client > System Administration	The URL to the optional Integration to	Integration to Microsoft Exchange

KEYVALUE (TBLREGISTRY NAME)	TITLE	CONFIGURED WHERE?	DESCRIPTION	AREA
	URL	> Settings > Parameters > Everyday User Applications tab	Exchange module. If Exchange Integration is enabled, this URL is inserted into the links within meeting appointments generated by the EMS Web App or EMS for Outlook.	

CHAPTER 32: Introduction to the EMS for Outlook User Guide

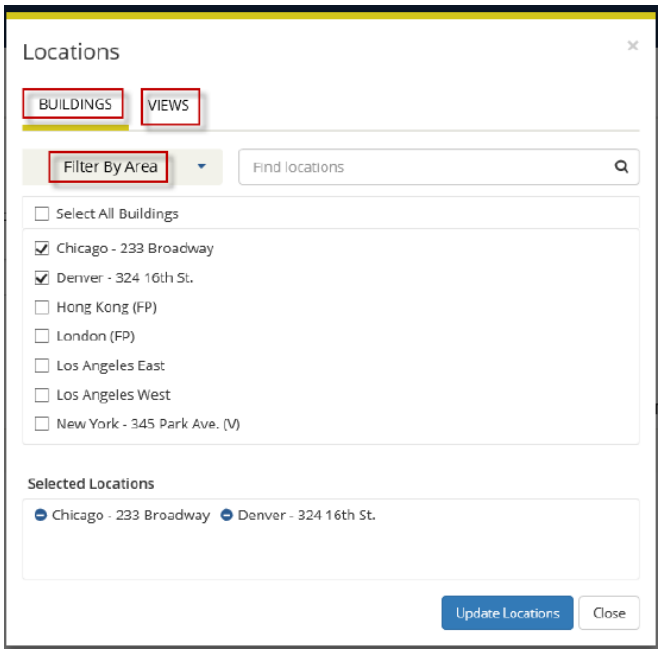
What information do you need to effectively use EMS for Outlook?

- Get Started With EMS for Outlook
- Microsoft Outlook, EMS for Microsoft Outlook, and EMS Web App Comparison
- Create Reservations in EMS for Microsoft Outlook
  - Create a Single Reservation
  - Create a Series Reservation
  - Create a Video Conference Reservation
  - Edit or Cancel a Scheduled Event
- Create a List of Favorite Rooms
- Use Skype for Business in EMS for Outlook (Legacy)
- Resolve Booking Conflicts
- View Known Errors/Alerts

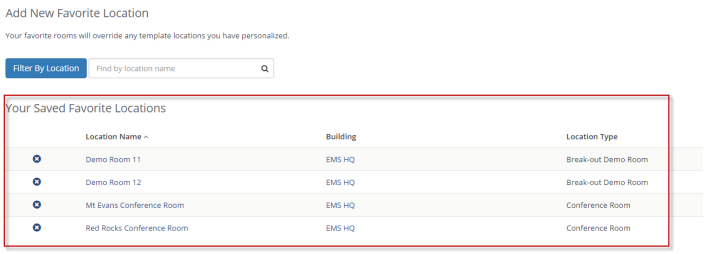
CHAPTER 33: Create a List of Favorite Rooms

Users can create a list of favorite rooms that can be searched for availability when creating a room request. This list of favorites is created in the My Account section of the EMS Web App. Once created in the Web App, the list of favorites will be displayed in the Facilities drop-down list on the Room Request page in EMS for Microsoft Outlook and the EMS Web App. If you leave the Facilities field set to this value, then all the rooms that are contained in this Favorites list are automatically searched for availability after you click Find Space.

1. Open EMS for Web App. In the upper right-hand corner, click My Account.
2. Click the My Favorite Rooms tab.
3. Under the Add New Favorite Room section, you can filter by location or find room by name.
    a. To search for a room by Area, Building, or View, click Filter by Location. The Locations dialog box appears.
        - Check the box(es) of the location you want to add to your favorites. Click Update Locations. The selected rooms will appear in the Selected Locations section at the bottom of the dialog box.



    b. You can search for a room by name by typing the name in the Find by room name field and clicking the search icon.
4. Your list of favorite rooms will appear as a list under the Your Saved Favorite Rooms section. The list can be sorted by Room Name, Building, or Room Type by clicking the sort button next to the filter.



5. Delete a Favorite Room by clicking the Delete icon to the left of the Location Name.

CHAPTER 34: Create Reservations in EMS for Microsoft Outlook

You can use the functions in the EMS for Microsoft Outlook plug-in module to check for available space for an event and to make a reservation for the event that is saved in your EMS database. You can search for rooms that are available for a particular time on one day (a simple reservation with one booking) or on multiple days (a series reservation with multiple bookings).

This section covers the following topics:

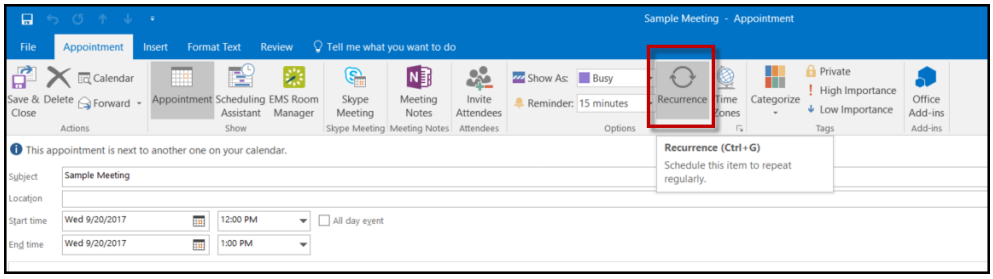
- Create a Single Reservation
- Create a Series Reservation
- Create a Video Conference Reservation
- Edit or Cancel a Scheduled Event

CHAPTER 35: Create a Series Reservation

A Series Reservation is a single reservation that includes multiple bookings. EMS for Outlook allows you to search for rooms that are available at a particular time on multiple days to create a series reservation. This section details the creation of a series reservation for a non-video conference meeting. For information about scheduling a video conference meeting, see Create a Video Conference Reservation.

1. Open Microsoft Outlook and click New Meeting to begin your reservation. Specify the subject, attendees, date, and time.
2. Click the Recurrence button.

Recurrence



Tip: The Start Time and End Time are designated when you set up the meeting in Outlook. You can edit these values in EMS for Outlook via the date and time fields or later after booking.

3. In the Appointment Recurrence dialog box, specify the Appointment Time, Recurrence pattern, Range of recurrence, and End by Date. Click OK.

IMPORTANT: Ensure you set an End Date for the recurrence. EMS for Outlook does not support infinite recurring meetings.

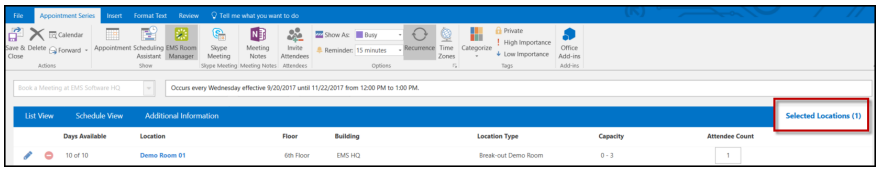
4. Click the EMS Room Manager icon in the top menu bar of Outlook.
5. Select a Template from the drop-down list (the list contains pre-defined templates set by your System Administrator).
6. Select a Room. By default, for a recurring meeting, EMS for Outlook opens in the List view. The List view shows the availability for all rooms. The list will include a Days Available column. This feature allows you to view how many days the space is available during your recurrence date range (e.g., 10/10 days). Click the Select (+) button on the left to select your room. If your room is available for all of your days, continue creating your reservation.
7. If the room you selected is not available for all days (e.g., only 8/10 days), the Resolve Conflicts dialog box will appear. (For example, for a recurrent meeting with 10 meeting dates, Demo Room 06 is available for 8 out of the 10 meeting dates.)

8. Choose a location that is available for the remaining dates during your recurrence and click the green Select (+) button.

TIP: If the user does not want to choose a room that resolves the conflict, they can skip the resolve conflicts process. Dates that are skipped will not be assigned a room and the location field in the meeting in Outlook will not be populated. The user can review the reservation at a later date and choose rooms for the skipped dates.

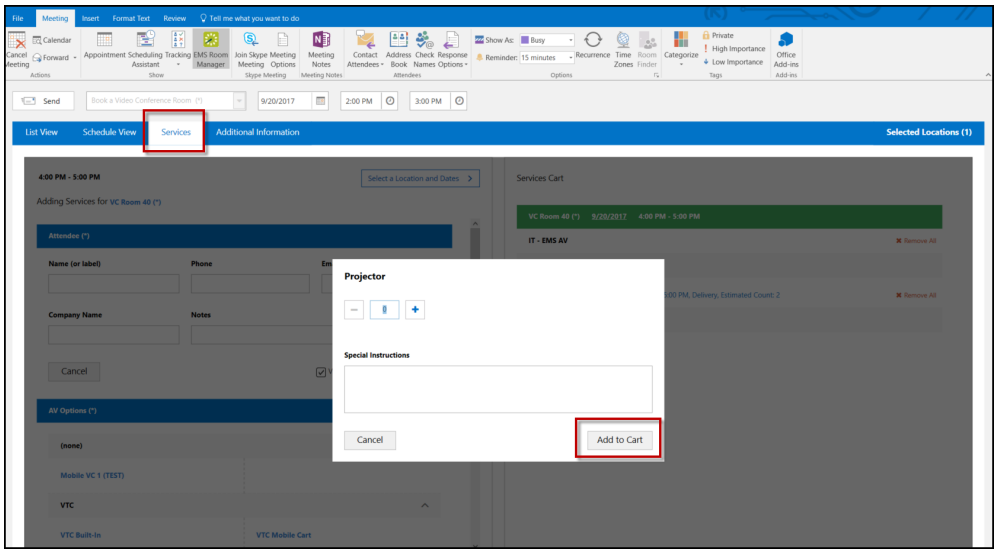
9. Optionally, click on the Selected Locations tab to view information about the selected room(s), such as Days Available, Location, Floor, Building, Location Type, Capacity, and Attendee Count. If needed, you can click the red Remove button to remove the room for the scheduled event or the Edit button to make changes.

Selected Location Tab



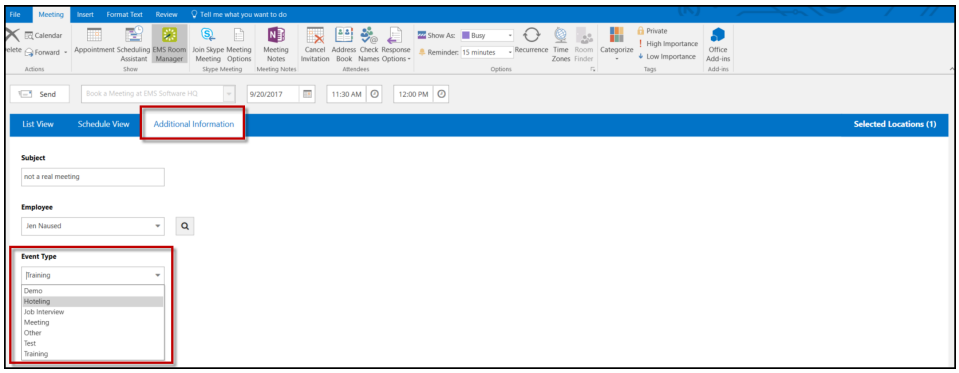
10. Optionally, you might be able to request services for the event, supply billing information for the event, and/or answer additional questions about the event. The Services tab might be available for requesting one or more services for the event, such as Catering, A/V Equipment, etc.
11. If your series has multiple rooms or start times, click on Select Service Location and Dates.
12. Click the service you want to add and provide additional information in the services dialog box if required.
13. Click Next.
14. Select quantity.
15. Click Add to Cart.

Services Tab



16. Click on the Additional Information tab. From this tab, you can edit the Subject, Employee, and Event Type.
17. Choose an Event Type from the drop-down list.

Additional Information Tab



18. From the Selected Locations tab, you can view information about the selected room, including the Floor, the Building in which it is located, its Location Type, Capacity, and the Attendee Count for your event. If needed, you can click the red remove icon to remove the room for the scheduled event so that you can select a different room. Additionally, you can edit the reservation by clicking on the edit icon.
19. To add a Skype for Business meeting to your event, click the Skype Meeting icon. The Skype icon will only appear if you have the Skype for Business Add-in enabled.
20. Click Send. The selected room is booked in the EMS database. The event is automatically added to your Outlook calendar. The invited meeting attendees receive a standard invitation for the meeting. The invitees accept or decline the meeting invitation as they normally would in Outlook. The EMS Reservation ID is included in the body of the meeting invitation.

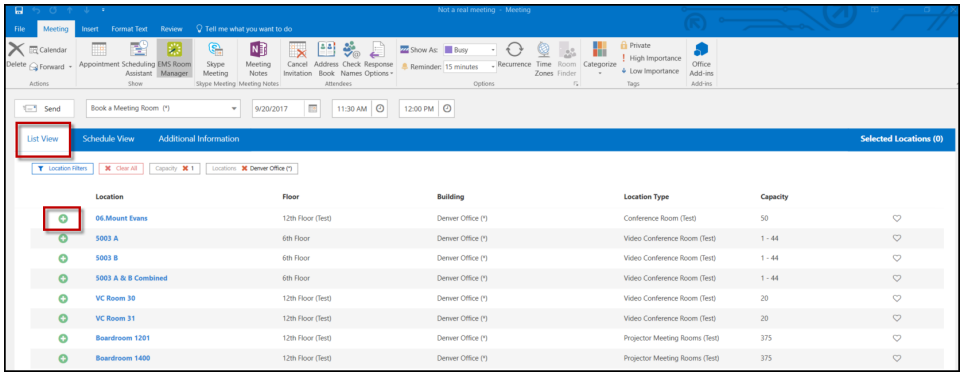
CHAPTER 36: Create a Single Reservation

In EMS for Outlook, you can search for rooms that are available for a particular time on one day and create a simple reservation with one booking.

TIP: This section details the creation of a single reservation for a non-video conference meeting. For information about scheduling a video conference meeting, see Create a Video Conference Reservation.

1. Open Microsoft Outlook and create a standard meeting that includes an event subject, attendees, and the date and time for the event.
2. Click the EMS Room Manager icon in the top menu bar of Outlook.
3. Select a template from the drop-down list (the list contains pre-defined templates set by your System Administrator).
4. The default List View will appear. This view displays the rooms available during the date and time of your event. This view shows the room's floor, building, location type and capacity.
5. Click the green Add symbol to add a room to your meeting.

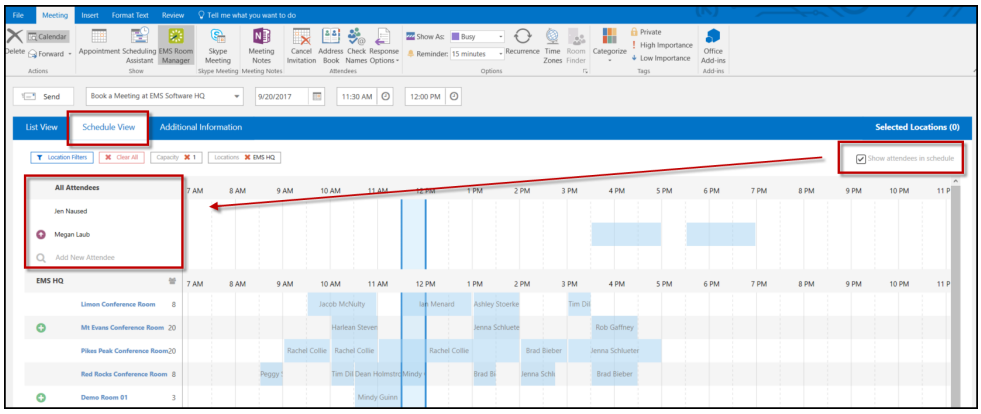
List View Tab



Tip: You can make a room your Favorite by clicking on the heart in the right-hand column. This Favorite will transfer to all EMS access points (e.g., EMS Web App, EMS Mobile App, etc.).

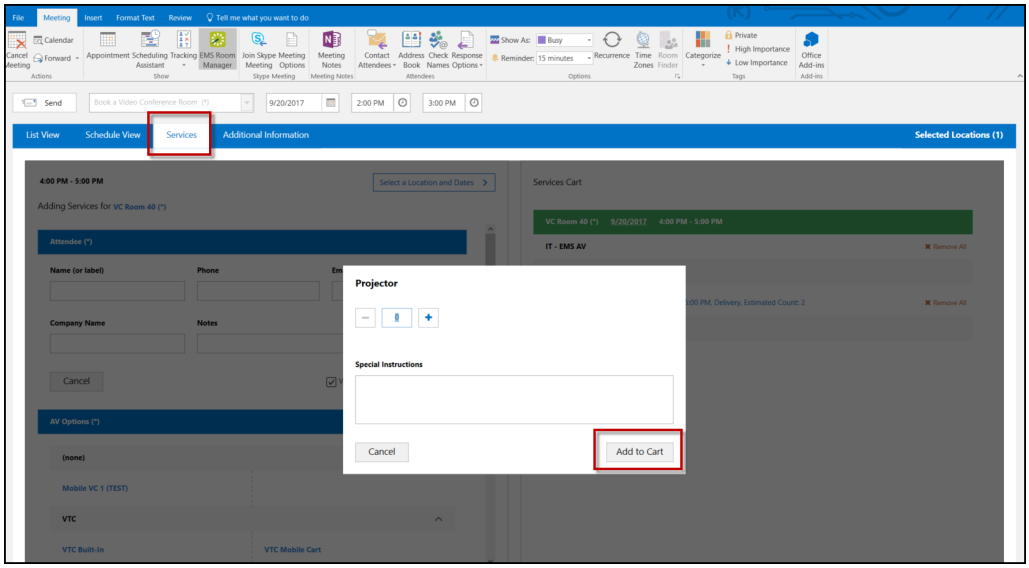
6. The Schedule View displays all the rooms in the building during the event time and who has booked them. If you have chosen a room for your event, a “Booking Edit in Progress” status (green color) is displayed for the room.
7. To view your meeting's attendees in the Schedule View, click the Show attendees in schedule checkbox in the right-hand corner. Click Add New Attendee to add an attendee to your meeting. You can make a required attendee optional by clicking on the icon next to their name.

Schedule View Tab



8. Optionally, you might be able to request services for the event and/or provide setup notes for the event. The Services tab might be available for requesting one or more services for the event, such as Catering, A/V Equipment, etc. Click on the service you want to add and provide additional information in the services dialog box.

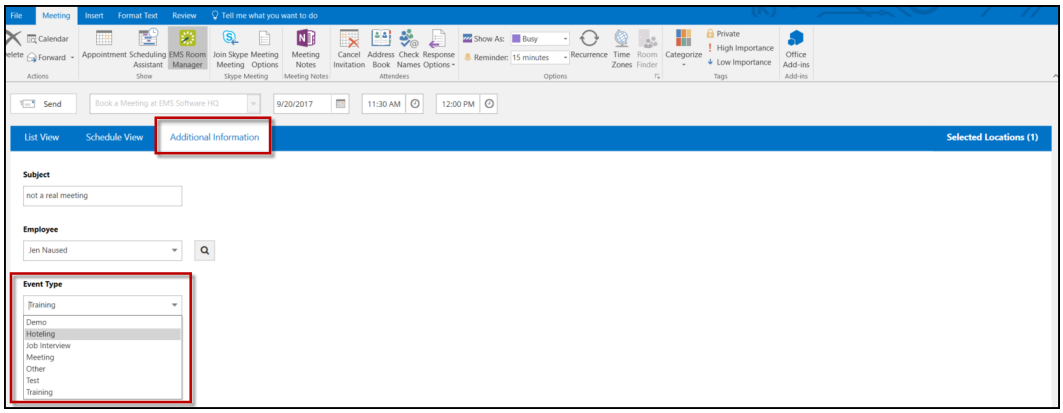
Adding Services from the Services Tab



NOTE: From theServices tab, you can select services for specific locations and dates by clicking on the Select a Location and Dates at the top of the tab.

9. Click Add to Cart to add the service to your event.
10. Click on the Additional Information tab. From this tab, you can edit the Subject, Employee, and Event Type.
11. Choose an Event Type from the drop-down.

Additional Information Tab



12. From the Selected Locations tab, you can view information about the selected room, including the Floor, the Building in which it is located, its Location Type, Capacity, and the Attendee Count for your event. If needed, you can click the red remove icon to remove the room for the scheduled event so that you can select a different room. Additionally, you can edit the reservation by clicking on the edit icon.
13. To add a Skype for Business meeting to your event, click the Skype Meeting icon. The Skype icon will only appear if you have the Skype for Business Add-in enabled.
14. Click Send. The selected room is booked in the EMS database. The event is automatically added to your Outlook calendar. The invited meeting attendees receive a standard invitation for the meeting. The invitees accept or decline the meeting invitation as they normally would in Outlook. The EMS Reservation ID is included in the body of the meeting invitation.

CHAPTER 37: Create a Video Conference Reservation

You can create a video conference reservation for both a single reservation and a series reservation. When you create a video conference reservation, two room options are available:

1. The room is a dedicated video conferencing room. (The room has built-in video conferencing features.)
2. The room has no built-in video conferencing features. Instead, you must use a mobile video conferencing cart in the room.

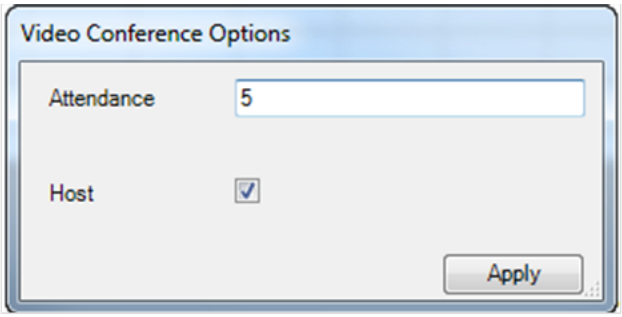
Please note the following differences for a video conference reservation:

- A video conference reservation requires two rooms
- You must always designate the capacity for each room
- You must indicate which room is the *host* room

To create a video conference reservation:

1. Follow the appropriate steps for creating either a Create a Single Reservation or Create a Series Reservation reservation.
2. Add the video conference option to your reservation. The Video Conference Room dialog box will appear.

Video Conference Room dialog box

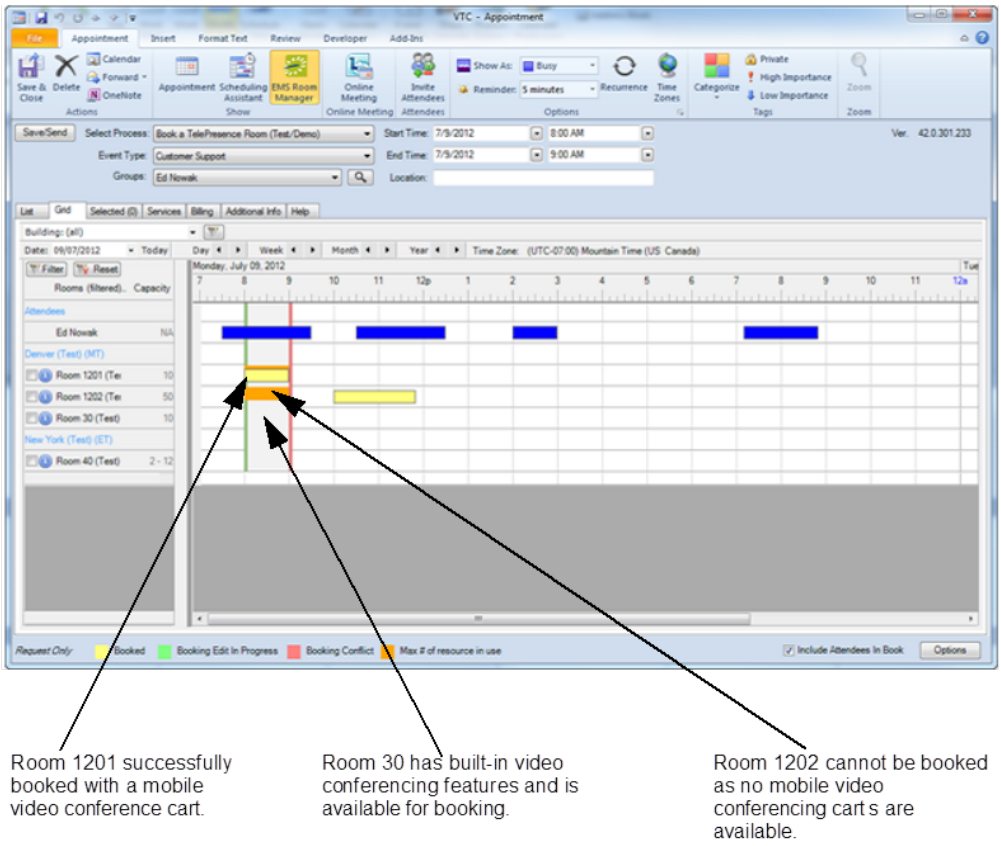


- If a room that you request for a video conference reservation requires a mobile video conferencing cart, and at least one mobile video conferencing cart is available, then an orange line is displayed for the room. After you book the room, the standard booking color of yellow with an orange line above it is displayed to indicate that you have successfully booked the room and a cart for the room.
- If a room that you request for a video conference reservation requires a mobile video conferencing cart, but no carts (resources) are available to book, then a solid orange rectangle is displayed for the room to indicate that the maximum number of resources are in use and you cannot book the room.

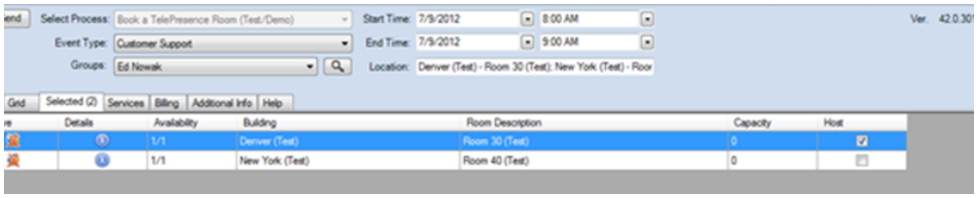
- If a room that you request for a video conference reservation has built-in video conferencing features and the room is available to book, then no color is initially displayed for the room. After you book the room, the standard booking color of yellow is displayed to indicate that you have successfully booked the room.

3. After you successfully book a video conference reservation, the host room is indicated on the Selected tab.

Video Conference Room Availability Indicators



Host room indicated on the Selected tab for a video conference reservation



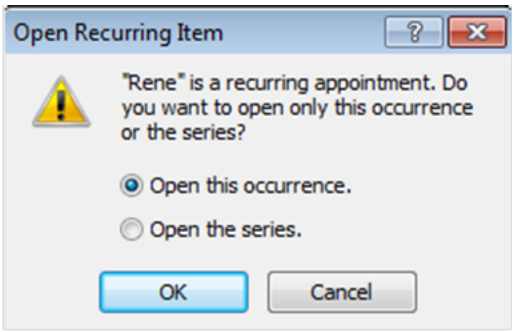
CHAPTER 38: Edit or Cancel a Scheduled Event

You can edit or cancel both a single reservation and a series reservation in the EMS for Outlook add-in.

To edit or cancel a scheduled event:

1. Open your Outlook calendar.
2. In the calendar, double-click on an event date.
   - If the reservation is a single reservation, then the meeting information opens in the standard Outlook meeting format.
3. If needed, edit the Start Time and/or End Time, and then click EMS Room Manager.
4. Edit any and all of the information for the scheduled event as needed (see Create a Single Reservation) or click Cancel Meeting to cancel the event.

   Tip: To cancel a scheduled service for an event, open the Services tab and clear the selection for the service.
   - If the reservation is a series reservation, then an *Open Recurring Item* message opens. The message indicates that the event is recurring and asks you if want to open only this occurrence of the event, or the series.



5. Do one of the following:
   a. To edit the Start Time and/or End Time for a single occurrence of a series reservation, leave Open this occurrence selected, and then click OK.
   b. To edit any value other than the Start Time and/or End Time for all bookings for a series reservation in a single step, select Open the series, and then click OK.
6. Click EMS Room Manager. The EMS for Outlook add-in opens in the Selected Locations tab. From this tab, users can edit the date, time and location. Click on Additional Information or Services tab to make further edits if necessary.

CHAPTER 39: Get Started With EMS for Outlook

EMS for Outlook is an optional add-on for Microsoft® Outlook; if you have it installed, you will see the EMS for Outlook icon in the top toolbar of your Outlook application window. This tool enables you to easily use Outlook to search for available rooms throughout your EMS database and make a reservation without exiting the application. Once you begin a meeting in Microsoft® Outlook, you can access the add-in by clicking the EMS icon. You can search for room availability for a particular time on one day (a simple reservation with one booking) or on multiple days (a series reservation with multiple bookings).

EMS for Outlook online Video Tutorials:

- Booking a Meeting
- Booking a Meeting With Services
- Booking a Video Conference

CHAPTER 40: Microsoft Outlook, EMS for Microsoft Outlook, and EMS Web App Comparison

The EMS for Outlook add-in provides one-click access to self-service room reservation and resource booking using the familiar Outlook personal scheduling interface. Users can find available rooms, reserve them and book resources—such as A/V equipment or catering—all from within Microsoft Outlook.

The EMS Web App provides robust, real-time access to scheduling information via an internet browser. A broad range of scheduling options and scheduling scenarios are supported easily. Authorized users can, depending on the level of access granted, submit room requests or create self-service reservations directly. Users can create basic or advanced reservations, schedule resources, view building schedules, or search for specific events.

Some important points to note about the EMS for Outlook add-in as compared to Microsoft Outlook and the EMS Web App are the following:

- For complex room reservations and resource management (such as copying a reservation), the EMS Desktop Client application might be preferred.
- Simple routine reservations made using the EMS for Outlook add-in generally follow the same rules as simple Outlook reservations.
- The add-in supports existing Outlook delegation assignments; however, the everyday user accounts must have the same corresponding delegation settings.
- The add-in can be used just like Microsoft Outlook to schedule regular recurring appointments (day and time). EMS for Outlook does not support recurring appointments without an end date.
- Just like reservations created in the EMS Web App, EMS for Outlook reservations abide by the rules of the Web Process template and the EMS Web App settings of the applicable categories and resources. The ability to modify and cancel EMS for Outlook reservations (dates, time, rooms, services and/or resources) are determined by these rules and the restrictions of Microsoft Outlook and Exchange.

CHAPTER 41: Resolve Booking Conflicts

This topic provides information on the following:

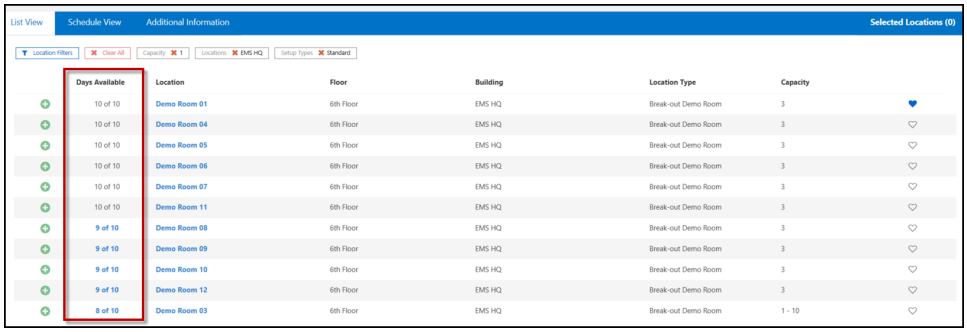
- To resolve booking conflicts for a series reservation:
- To resolve booking conflicts when you receive a warning email:

To resolve booking conflicts for a series reservation:

When booking a recurring meeting, you might encounter a booking conflict. To resolve this conflict:

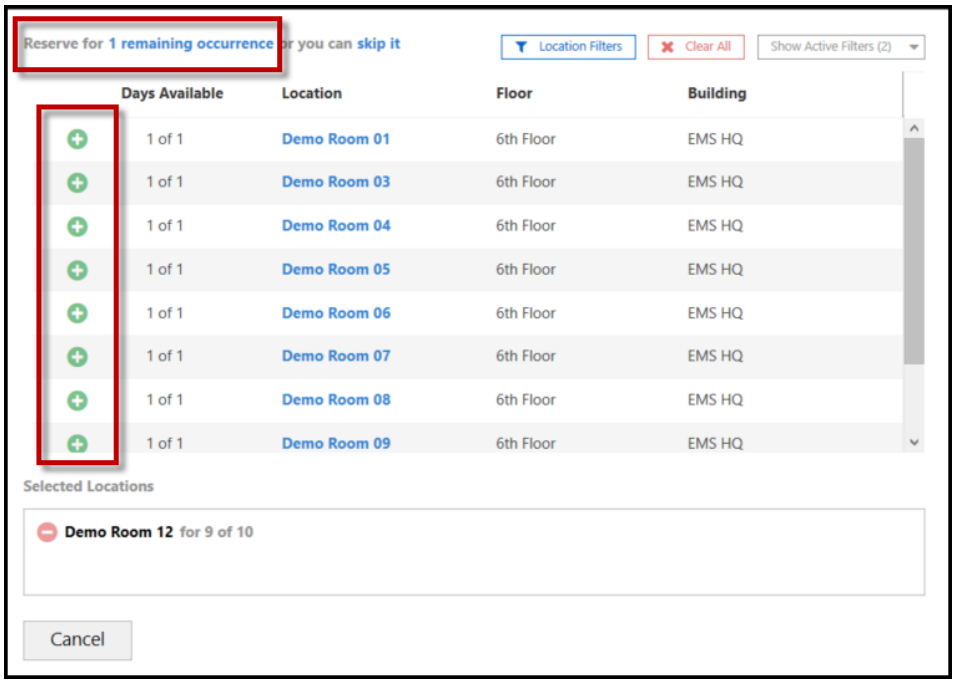
1. Create your Create a Series Reservation.
2. Click the EMS Room Manager icon to choose your room. The List View will display with a list of all available rooms that match your meeting criteria.
3. Choose a room by clicking the Add (+) button next to the Location.
4. To avoid booking conflicts, choose a room that is available for the entire span of your recurring meeting (as displayed in the Days Available column).

Days Available Column Indicates Potential Conflicts



5. If you choose a room that is not available for the entire time span of your recurrence, a booking conflict has been created. The Conflict Resolution dialog box will open.
6. From the Conflict Resolution dialog box, choose a room for the remaining occurrences that do not yet have locations by clicking the Add (+) button.

Conflict Resolution Dialog Box



TIP: You can click the skip it link at the top of the Conflict Resolution dialog box to bypass this resolution. However, you will not have space reserved for the booking, and it will not appear on your calendar. EMS Software recommends that you find and select an alternate room for each booking conflict.

7. Choose an alternate room. The conflict has been resolved and will be reflected on your calendar.

To resolve booking conflicts when you receive a warning email:

As the meeting scheduler, you might receive a booking error message (e.g., "One or more of your rooms were not available and are in conflict. Refer to your email for next steps.") and an email that indicates the bookings that are in conflict for the reservation. This email will alert you that "The following rooms could not be reserved because they are unavailable. You must reserve a new room for each time slot shown below."

1. Open your Outlook calendar and click on the EMS Room Manager.
2. Navigate to the date of the scheduled event and double-click the event for which a booking is in conflict.
3. If the event is recurring, an *Open Recurring Item* message opens. The message indicates that the event is recurring and asks you if want to open only this occurrence of the event, or the series.
4. Leave Open this occurrence selected, and then click OK.
5. Click the EMS Outlook Manager icon in the Outlook toolbar. The EMS for Outlook add-in opens the Selected Rooms tab to show you the booking conflicts.

CHAPTER 42: EMS for Microsoft® Outlook (Legacy) User Guide

The EMS for Microsoft Outlook plug-in module provides one-click access to self-service room reservation and resource booking from within the familiar Outlook personal scheduling interface. Users can find available rooms, reserve them and book resources—such as A/V equipment, catering, etc.—all from within Microsoft Outlook.

What information do you need?

Get Started With EMS for Outlook

- Microsoft Outlook, EMS for Microsoft Outlook, and EMS Web App Comparison

Create Reservations in EMS for Microsoft Outlook

- Create a Single Reservation
- Create a Series Reservation
- Create a Video Conference Reservation
- Edit or Cancel a Scheduled Event

Create a List of Favorite Rooms

Use Skype for Business in EMS for Outlook (Legacy)

Resolve Booking Conflicts

View Known Errors/Alerts

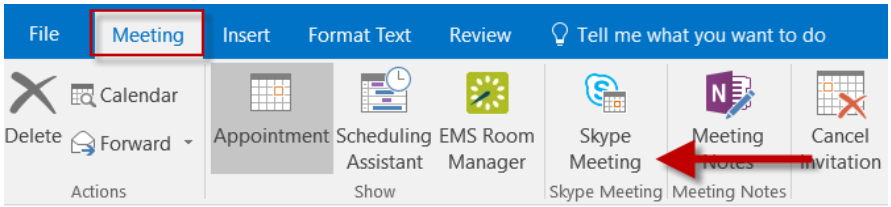
CHAPTER 43: Use Skype for Business in EMS for Outlook (Legacy)

Everyday Users can now integrate audio/video conferencing tools with EMS applications, starting with Skype for Business. It will no longer be necessary for users to simultaneously create a separate meeting to enable an audio/video conferencing component to their meetings. The EMS integration of Skype for Business allows users to easily integrate instant messaging and audio/video conferencing to their meetings without the need for A/V support. Skype for Business is only available for Exchange-enabled templates.

IMPORTANT: Skype for Business meetings cannot be removed from Outlook appointments, including those tied to reservations using EMS for Outlook.

To Use Skype for Business:

1. Ensure you have the Skype for Outlook add-in.
2. Open Microsoft Outlook and create a standard event request that includes the event subject, the date, and time for the event, and invite the necessary attendees.
3. Click the EMS Room Manager icon. Create Reservations in EMS for Microsoft Outlook .
4. Under the Meeting tab, click the Skype Meeting button on the top menu. Skype meeting information will appear in your meeting invitation and will be stored on the EMS database.



5. If this is your first time using Skype for Business, an authentication form will appear. Sign in using your Skype credentials.
    - If the user's Skype account is authenticated, they can continue creating their reservation.
    - If the user's Skype account is not authenticated, an authentication modal will appear.
    - If the user fails to authenticate their Skype account, the Skype toggle will be disabled.

IMPORTANT: Authentication to Skype is dependent upon the deployment type.

There are three deployment types for Skype for Business:

- On Premise: This deployment for Skype for Business does not retain a token and requires authentication every 8 hours. As a result, you will be asked to sign in every 8 hours.
- Online: This deployment retains the token so only an initial authentication is required.
- Hybrid: This deployment has the same authentication method as the Online deployment.

6. Complete your reservation. Once Skype has been added to your meeting, the Skype meeting information will appear in all EMS applications that have been integrated with Skype for Business (i.e., EMS

Mobile App and EMS Web App).

For more information regarding the features of Skype for Business, please see Microsoft Skype for Business User Guide.

CHAPTER 44: View Known Errors/Alerts

During the course of using the EMS for Microsoft Outlook plug-in module to schedule reservations and make appointments, you might encounter alerts and error messages.

This following table details the known alerts and error messages for the module and provides an explanation for each:

ALERT/ERROR MESSAGE	DESCRIPTION
Alerts	
Resource Alert	Customer-specified resource alerts are displayed when a user selects a resource.
Room Alert	Customer-specified room alerts are displayed when a user selects a room.
Errors	
You have an unapplied service order. Are you certain you want to continue?	Displayed if a user has entered a service order, but clicks Save before clicking Apply.
Appointment "SUBJECT" is tied to an EMS Booking.	Displayed when a user attempts to copy or cut a meeting on a calendar that is linked to EMS.
The meeting you are viewing is no longer being monitored by EMS. Changing this meeting will disconnect the meeting from EMS.	• Displayed if a user opens a meeting that has occurred in the past. • Prior to build 43.0.28—in inconsistent scenarios—this message was displayed when a user created a creating on a delegate's calendar and then tried to modify the meeting.
Your web user id does not match the web user id on the reservation. Any changes to this meeting will disconnect the meeting from the EMS Reservation.	Displayed when a user attempts to open a meeting for which they are not the web user.

ALERT/ERROR MESSAGE	DESCRIPTION
This reservation has been invoiced. Any changes to this meeting will disconnect the meeting from the EMS Reservation.	Displayed when a user attempts to open a meeting that has been invoiced.
This reservation is assigned to a process template that is unavailable to you in Outlook. Any changes to this meeting will disconnect the meeting from the EMS Reservation.	Displayed when a user attempts to open a reservation that is tied to a process template to which they do not have access to or is not available in Outlook.
EMS requires all meetings be 24 hours or less.	Displayed if a user sets a start/end date/time combination to anything greater than 24 hours.
You changed the time after changing the location which invalidated your locations.	Displayed if a user: • Changes the meeting time after selecting a meeting location. • Changes the meeting recurrence any in way after selecting a location. Note: A user must verify a room after changing times or recurrences.
One or more of your locations was not available.	Displayed when a user attempts to save a meeting and one or more of the EMS rooms requested was not available.
One or more of your services violated the available quantity and was not applied to your meeting.	Displayed when a user attempts to save a meeting that has a service order and one or more of the resources had insufficient quantities available.
There was a problem saving your reservation in EMS.	Displayed when EMS encounters an unexpected error trying to save the reservation in EMS.

ALERT/ERROR MESSAGE	DESCRIPTION
Your request would violate the maximum allowed duration for a reservation ({0} minutes).	Displayed when a user attempts to add a booking that violates the Max Minutes Allowed value as specified by the Web Process template.
This template only allows for {0} booking(s) at a time.	Displayed when a user attempts to add a booking that violates the Max Number of Bookings value as specified by the Web Process template.
Terms must be accepted.	Displayed if a user does not select the option to accept Terms and Conditions.
Event type is required.	Displayed if a user attempts to submit an entry without an event type being selected.
Group is Required.	Displayed if a user has not selected a group. (Group label used in message.)
Use the Send Cancellation button on the appointment tab.	Displayed in the meeting cancel notification if a user attempts to press the EMS Save/Send button.

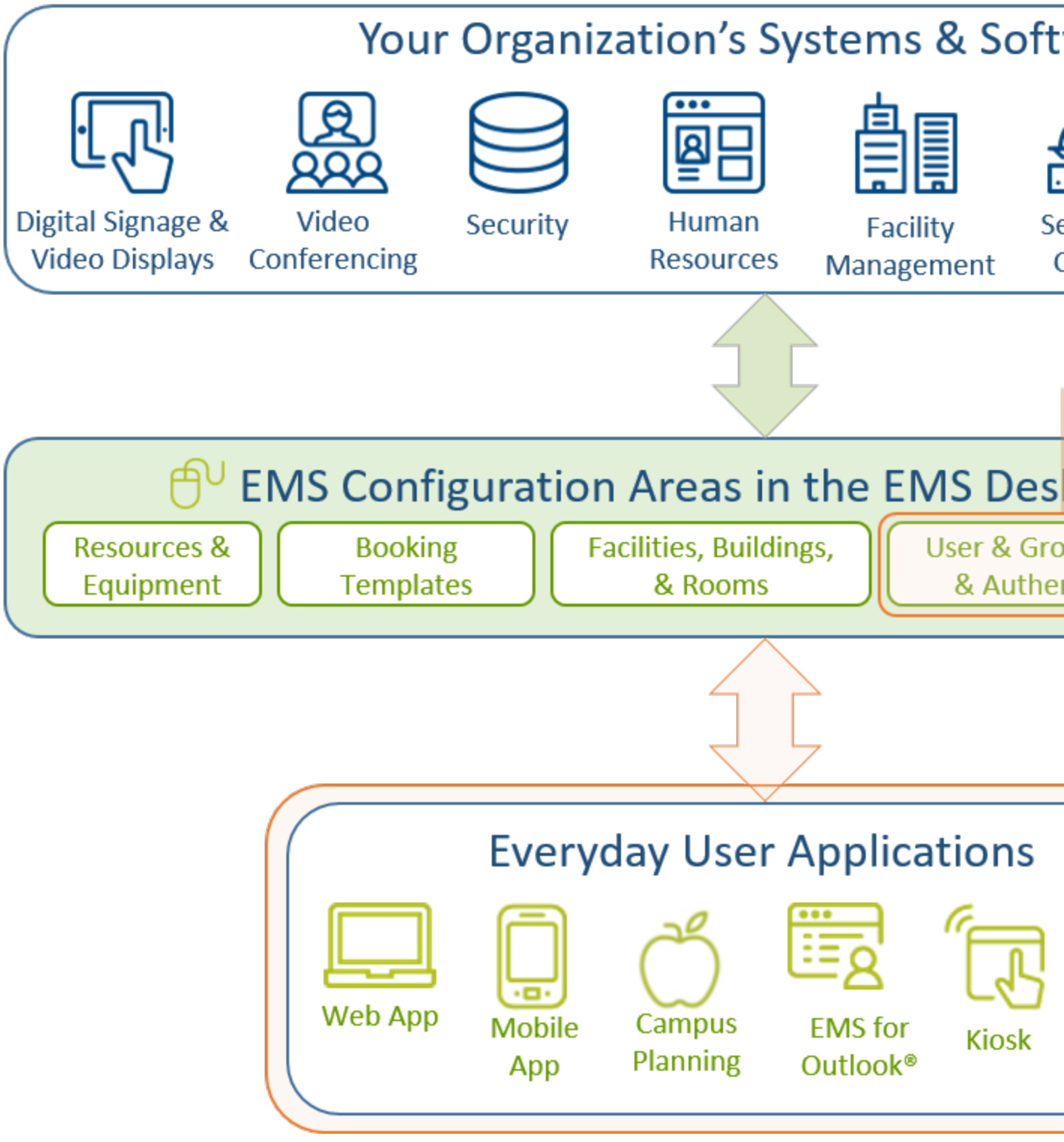
CHAPTER 45: Introduction to EMS Integration to Microsoft® Exchange

EMS Integration to Microsoft® Exchange is a component that integrates EMS Everyday User applications, such as EMS Mobile App, EMS for Outlook and EMS Web App, with Microsoft® Exchange. This module enables everyday users to view the availability of both meeting rooms *and* attendees, and send Outlook® meeting invitations, all from within EMS Everyday User applications.

This guide provides instruction for installing Integration to Microsoft® Exchange for System Administration and IT users. The following information is included in this guide:

- System Requirements for Integration to Microsoft® Exchange
- Install or Upgrade the Exchange Integration Web Service
- Configure Integration to Microsoft® Exchange
- Use Application Pool Identity for Integration for Exchange Service Account
- Configure EWS Impersonation for Microsoft® Exchange
    - Learn More About Exchange Web Services (EWS) Impersonation

Exchange Integration Flow



You must be licensed for EMS, EMS Web App, and Integration to Microsoft® Exchange in order to configure and use this feature. If you are unsure if your organization is licensed for Integration to Exchange, or if you would like to learn more about it, please contact your Account Executive.

To install and configure Integration to Exchange, you will:

- Install the Exchange Integration Web Service
- Configure EMS Integration to Exchange
- Configure EWS Impersonation for Exchange Online (Office 365)

The following requirements must be met to install and configure Integration to Microsoft® Exchange. See Also: System Requirements for Integration to Microsoft Exchange.

- EMS and/or EMS Web App Installed
- EMS must be installed and operational
- Valid Outlook Integration License

CHAPTER 45: Integration to Microsoft® Exchange

This guide provides instruction for installing Integration to Microsoft® Exchange for System Administration and IT users. The following information is included in this guide:

CHAPTER 45: System Requirements for Integration to Microsoft® Exchange

You must be licensed for EMS Desktop Client, EMS Web App, and Integration to Microsoft® Exchange to configure and use this module. If you are unsure if your organization is licensed for Integration with Exchange, or if you would like to learn more about it, please contact your Account Executive.

The following requirements must be met to install and configure Integration to Exchange:

- System requirements must be met for the following:
  - EMS Web Server
  - EMS Web App
  - EMS Platform Services
  - EMS for Outlook and Integration to Exchange
- EMS Desktop Client and/or EMS Web App Installed
- EMS Desktop Client must be installed and operational
- Valid EMS for Microsoft Outlook License

Web Server Requirements

EMS Web App Requirements

IMPORTANT: Integration with Exchange configuration issues often relate to access rights with this account. Please ensure that the account has the necessary permissions.

EMS Platform Services

EMS for Microsoft Outlook Requirements

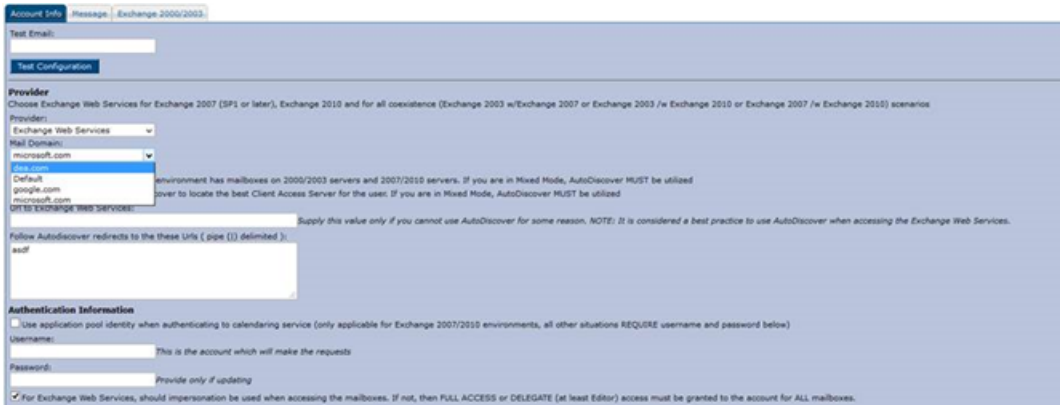
CHAPTER 45: Configure Multiple Mail Domains

To configure multiple mail domains, you must edit the web.config file. This will enable the Mail Domain drop-down that allows Administrators to specify different EWS URLs, AutoDiscover settings, and authentication options based on the domain.

When an EIWS booking is made through EMS for Outlook or the EMS Web App, it will automatically pull the domain from that user's email address. It will then use the corresponding Mail Domain option.

1. Open the web.config file.
2. Navigate to the mail domains line at the top under the Configuration section.

3. Remove the comment marks (<!-- -->) and add your domains to the value (e.g., `<add key="mailDomains" value="dea.com|google.com|microsoft.com"/>`
4. Save your web.config file. You will now see the Mail Domain drop-down menu on the pamconfig.aspx screen. Each menu item will have its own Provider area.



5. Test your Exchange Integration.

NOTE: These settings are stored in the tblPamSettings table.

CHAPTER 45: Configure Integration to Microsoft Exchange

NOTE: As of 44.1, Update 24, the testing function on pamconfig.aspx will test the FindItems, GetUserAvailability, Create, Edit, and Cancel EWS calls used by the EMS integration. Previously, only FindItems was tested. There is not necessarily a 1:1 guide as to what would cause a failure for each specific call, however this does not mean that scenarios exist where 'create' would succeed but 'cancel' would fail for example. The 'GetUserAvailability' call does not leverage ApplicationImpersonation, so if this is succeeding and the create/edit/cancel calls are failing then the issue is likely around permissions for the service account. Testing will be logged in the logfile, which has a default location of ExchangeIntegrationWebService\LogFiles and can be modified in the web.config file.

Configuring EMS to work with Exchange Online (Office 365) or Exchange 2013 is the same as configuring EMS to work with a 2007/2010 Exchange environment that is hosted on your network. See Configure EWS Impersonation for Microsoft® Exchange for information on configuring impersonation on Exchange Online (Office 365). If you need additional assistance configuring this, please contact support@emssoftware.com.

NOTE: Integration to Exchange requires the use of a mail-enabled service account that has the Application/Impersonation role in Exchange for all users who will be accessing EMS. See Also: Configure Exchange Web Service Impersonation.

This topic provides information on the following:

Configure Integration to Exchange Instructions

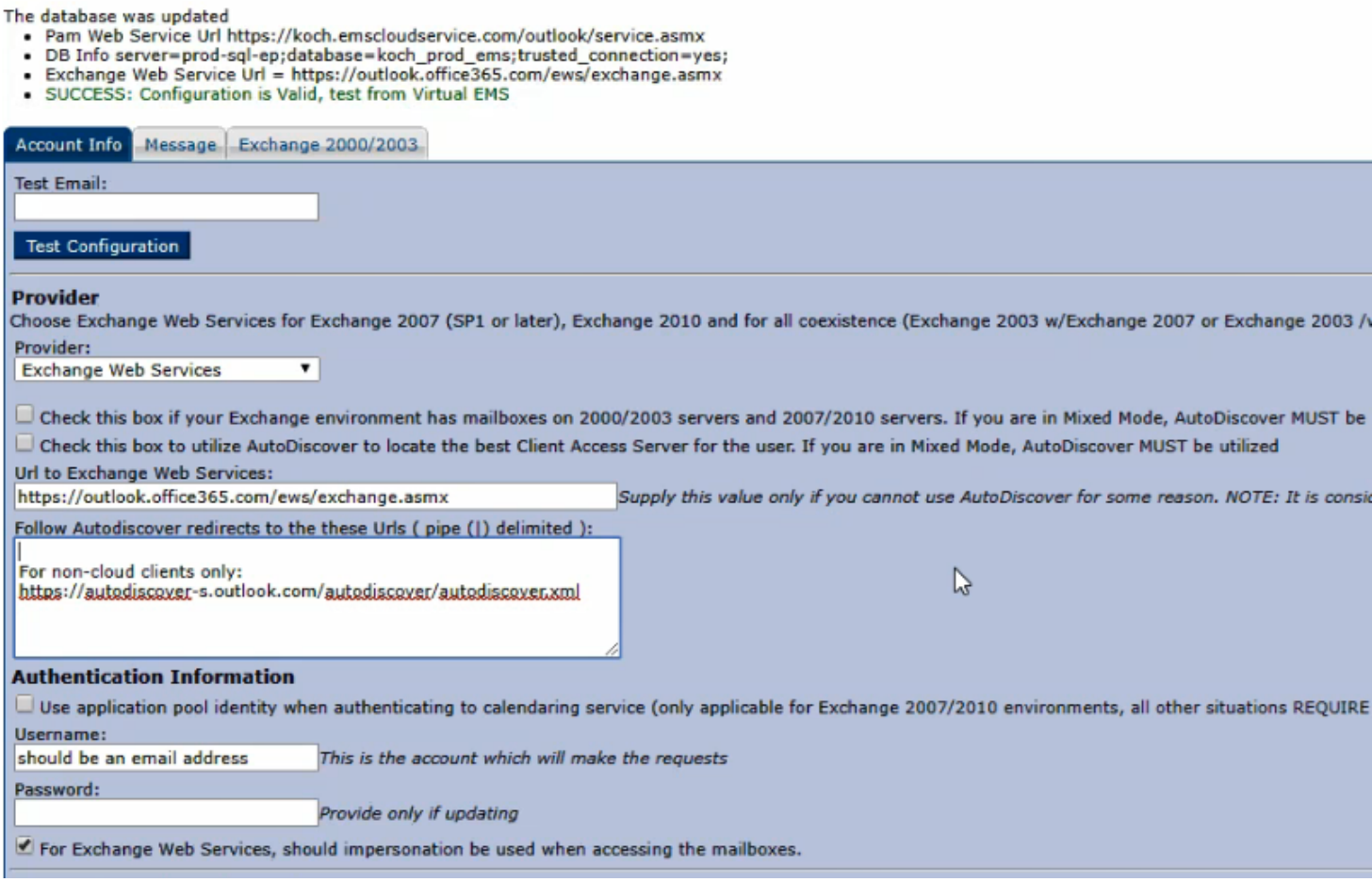
Important: As of Update 28, access to the PAMconfig.aspx page is restricted by default. Customers who do not enable Windows Authentication in IIS for the Exchange Integration Web Service should comment out the following section in order for EIWS to work properly:

```
<remove users="*" roles="" verbs=""/>

<add accessType="Allow" roles="Users"/>”
```

1. After following the installation instructions, access the Integration to Exchange configuration area by opening a browser and entering the following: http://[ServerName]/ExchangeIntegrationWebService/PamConfig.aspx (replace [ServerName] with the name of your web server)
2. Go the Account Info tab.

Office 365 Configuration Example



3. Select your email system in the Provider drop-down list using the instructions provided on the page.
4. Check the box "... utilize AutoDiscover to locate the best Client Access Server for the user..." NOTE: If you do not check this box, you must fill in the Url to Exchange Web Services field.
5. Within the Authentication Information section, enter your Integration to Exchange Account User Name and Password. The User Name should be prefixed with your domain (example – YourDomain\Integration to Exchange Account, or Integration to Exchange Account@YourDomain) . TIP: Make a note of this URL for use later in this topic.

6. (*Optional*) The "Use application pool identity…" option allows you to set the Integration to Exchange Account credentials at the Application Pool level instead of storing the credentials in the EMS database. See the Use Application Pool Identity for Integration for Exchange Service Account topic for more information about this option. If this option is selected, you must check the box to use Impersonation.
7. If you selected "Exchange Web Services" as your Provider, select the checkbox if the account specified has Exchange Impersonation access to all mailboxes in your Exchange mailbox store.
8. Select the Authentication Type:
   - Anonymous – No authentication
   - Specify Account – Relies on a custom account (not the Integration to Exchange Account) that you create and manage. Please contact Customer Support (or a member of the Professional Services group if you are working with one) to discuss the configuration process for this option.
   - Default Credentials – Relies on security context of EMS application calling the Integration with Exchange Web Service. If using this option, Integrated Windows Authentication should be enabled for the Integration with Exchange Web Service.
   - For MS Exchange 2007/2010 environments, click Save.

   NOTE: When testing Integration to Exchange, the email account that is being used (either on the Test Settings tab or in the Testing Integration to Exchange section below) MUST exist in the Exchange environment being tested. If you are testing Integration with Exchange in a development environment, please verify that a mailbox for the email being used exists in that domain/environment.
9. Click Test Configuration. If any errors are encountered, please verify your configuration. Otherwise, your Integration to Exchange configuration is complete.

Test Your Exchange Integration

To test your configuration, you will need to log into EMS Web App with a user account (configured with the user's primary email address) belonging to a Everyday Application Process Template (within the EMS client application) that has the Enable Integration to Microsoft Exchange option checked.

1. Log into EMS Web App. Begin making a reservation and selecting a room.
2. Select the Add to my calendar checkbox. If this option is not available, please verify (within the EMS client application) that your user account belongs to a Everyday User Process Template that has the Allow Invitations option checked.
3. Find and add an attendee using the Find Attendee field.
4. Complete necessary information on the Details tab and click Submit Reservation.
5. Verify that an appointment was added to your Outlook Calendar and that your attendee received an invitation.

Optional Messaging Settings

The options on the Message tab (as reached above in Step 2) shown below guide you in further configuring your integration.

Message Tab Fields

FIELD	DESCRIPTION
Message To Append	Message appended to the bottom of the appointment body. This message is seen by all users.
To view the details of this reservation click the below link	Message added to the appointment body, above a link that takes a user to a view-only EMS Web App page for the appointment. This message is seen by all users.
If you are the meeting organizer click the below link to	Message added to the appointment body, above a link that takes the meeting organizer to the EMS Web App Reservation Summary page for that reservation. This message is seen by all users, but only the meeting organizer can access the Reservation Summary page to make changes.

FIELD	DESCRIPTION
edit the reservation	
Allow Attachments	Allows users to add attachments within EMS Web App when making an appointment.
Maximum Attachment Size	If attachments are allowed, set the maximum file size allowed for an attachment.

Concept: The default installation allows file attachments up to 4MB.
If your implementation needs file attachments that are larger, follow the two procedures below:

1. Update the config file.
2. Update the database.

NOTE: File sizes larger than 2 GB are not allowed at this time.

Enable Larger File Attachments On The Config File

By default, Exchange Integration attachments will only accept files 4MB or less. If your implementation needs to allow files of larger sizes to be attached to reservations, the following config updates will be required, both in EMS Web App and in the Exchange Integration Web Service.

IMPORTANT: The maximum file size is 2 GB.

1. In the <system.webServer> section, include this xml node:

```
<security>
      <requestFiltering>
        <requestLimits maxAllowedContentLength="51200000"/> <!--
maxAllowedContentLength in bytes, 50MB=51200000-->
      </requestFiltering>
    </security>
```

2. In the <httpRuntime element, add these highlighted attributes with the end result looking like this:

```
<httpRuntime targetFramework="4.5" requestLengthDiskThreshold="214-
7483644"
maxRequestLength="51200"  />  <!--requestLengthDiskThreshold in
bytes, & maxRequestLength in KB, 50MB-->
```

3. Under the <appSettings> look for the "MaximumUploadSizeInBytes" key. Update this value to the number of bytes allowed. For instance, 50MB would look like this:

```
<add key="MaximumUploadSizeInBytes" value="52428800000"/>  <!--
in bytes50MB-->
```

Enable Larger File Attachments in the Exchange Integration Web Service

By default Exchange Integration attachments will only accept files 4MB or less. If your implementation needs to allow for Exchange message attachments larger than 4MB, the config updates above will need to be applied in the Exchange Integration Web Service.

NOTE: Due to the size of the xml sent, we recommend adding 5MB to the desired file upload size. (i.e., if you want to allow a max of 20MB files, calculate a total of 25MB worth of Kilobytes and bytes.

In addition to these web.config settings above, a web administrator will need to update the file size in the Exchange Integration Web Service as follows:

1. Navigate to the Exchange Integration Web Service/PAMConfig.aspx
2. Click the Message tab
3. Update the Maximum Attachment Size text box and Save.

WARNING: For Externally Exposed Web App sites

If your EMS Web App site is externally exposed, some of the web.config settings above could make the site vulnerable to DoS site attacks. We highly recommend setting network-level protection to prevent DoS attacks.

CHAPTER 45: Configure EWS Impersonation for Microsoft® Exchange

NOTE: The service account requires a mailbox and must be mail enabled. EMS Software recommends disabling the password expiration for these accounts.

1. Log in to the Office 365® Exchange Administration Center. For Microsoft Exchange 2010, please see here.
2. Create a Service Account User within your Office 365 Environment.
   OR
   Configure a already migrated account.
3. Select Exchange > Admin Roles from the navigation tree.
4. Click the + icon to add a new role
5. In the role group dialog box, provide a name for your Role Group (e.g. "EMS_Exchange_Impersonation"). It is also helpful to enter a Description.
6. Under Role, click the + icon to add the "Application Impersonation" Role.
7. Under Members, click the + icon and find your Exchange Service Account.

TIP: For more information on EWS Impersonation, see What is EWS Impersonation?

CHAPTER 45: Install or Upgrade the Exchange Integration Web Service

Prior to Install or Upgrade

IMPORTANT: Before beginning the installation process, complete the following steps.

1. Install or upgrade your EMS databases as outlined in the EMS Desktop Client Installation Guide.
2. Manually uninstall any previous versions of the Exchange Integration Service on your web server.
3. If you are upgrading from previous versions, update your parameter settings for "PAM Web Service URL" to "Exchange Integration Web Service URL"
   (i.e., http://server/ExchangeIntegrationWebService). See Also: EMS Web App Parameters.

Install or Upgrade Instructions

1. Verify that the requirements outlined in the System Requirements section have been met.
2. Download ExchangeIntegrationWebService.msi onto the web server that will be running the service.
3. Run ExchangeIntegrationWebService.msi.
4. The first screen welcomes you to the Exchange Integration Service Setup Wizard. Click Next to begin the installation process. The Destination Folder screen will appear.
5. Select the destination folder. The installation process will create a new physical directory on your web server based on the destination folder path entered ("ExchangeIntegrationService" in the example above.) Click Next.
   NOTE: The Exchange Integration Service should not be installed in the same physical directory as other EMS web-based products.
6. The SQL Server and database information screen will appear.
7. Enter your EMS SQL Instance Name.
8. Enter your EMS Database Name, typically named "EMS".
9. Click Next. The Virtual Directory information screen will appear.
10. The Virtual Directory Name will default to the destination folder specified in Step 5. It is recommended that you keep the default setting. The installation process will create a virtual directory on your web server based on the virtual directory entered ("ExchangeIntegrationWebService" in the example above.) Click Next.
    NOTE: The Exchange Integration should not be installed in the same virtual directory as other EMS web-based products.
11. The Ready to Install Exchange Integration Web Service screen will appear. Click Install to install the Exchange Integration.

12. The Completed the Exchange Integration Web Service Setup Wizard screen will appear. Click Finish.
13. After following the steps above, verify your installation by opening a browser and entering the following:
    http://[ServerName]/ExchangeIntegrationWebService/Service.asmx
    (replace [ServerName] with the name of your web server)
    IMPORTANT: A standard installation requires that the Exchange Integration be published without any authentication methods in place (e.g., Integrated Windows Authentication or Portal Authentication). If you require the Exchange Integration to be secured with authentication, additional configuration is necessary. Contact your implementation consultant for further details.

CHAPTER 45: Learn More About Exchange Web Services (EWS) Impersonation

EMS offers two Exchange integration options to enable seamless room, resource, and attendance scheduling:

1. EMS Integration to Exchange offers users the convenience of scheduling rooms, resources, and services, confirming attendee availability, and managing Outlook invitations via EMS Web App (our web-based reservation tool). See Also: Installation Overview.
2. EMS for Outlook lets users find available rooms, review their details, reserve them and book any necessary resources (equipment, etc.) without ever leaving Microsoft® Outlook.

To achieve this seamless interaction between everyday users, Outlook hosts, and EMS administrators, an account with Exchange impersonation access to all mailboxes in your Exchange mailbox store is required.

See Also: Configure EWS Impersonation for Microsoft® Exchange

FAQs

Why is this account necessary?

Meetings created via EMS Integration for Exchange either on EMS Web App or EMS for Outlook are owned by the host and associated with a specific Exchange account. That Exchange user can move, update, or cancel the event. However, these meetings can also be moved, changed, or canceled by IT admins and expert users in EMS Desktop Client. When a reservation is moved, changed or canceled in the client, EMS must be able to update the record on the host's Exchange account. Co-ownership of events between the meeting host and the EMS administrators necessitates an account that can read and write to all Exchange accounts being used for booking.

Can we exclude people from impersonation? (For example, remove CEO, Board of Directors, etc. from being impersonated.)

Microsoft Exchange Server supports a CustomRecipientScope parameter when defining the impersonation role. You can define a scope of included users by implementing this parameter.

Is there any way that we could use a delegation feature (like allowing office admins delegate rights) instead of impersonation to notify hosts of updates/changes?

Delegation is possible, here are some things you should know:

- The account needs Editor w/Folder owner (so a custom rights set).

- Custom rights, at least through exchange 2010, are not scriptable. This means the delegation account will get set to owner, which is the only built in (read scriptable) option that has all the necessary permissions.
- EMS for Outlook creates a custom property on the Calendar folder, which allows you to programmatically search the folder for items that have the custom property. Once that custom property is created, then Editor will be enough. It is the creation of the custom property at the folder level that requires owner permission.
- While you can use PowerShell to script the permissions and loop through the users and set the permissions (owner), you would need to make sure that the script got applied to any new users and reapplied to any users that have changed the permissions of the delegation account
- Rights are granted to ANY mail client (Outlook, OWA, etc): when using the impersonation account, rights are only granted to Exchange Web Services, so nobody could type in the service account into Outlook and gain the same permissions.
- These rights are visible to the end user. For example, if an account, "EMSExchangeAccount", has been granted, delegation rights (any level) to User1's calendar, and User1 goes to the Permissions tab of his calendar, he will see the EMSExchangeAccount and the rights it is assigned. Additionally, User1 would be able to change the rights, which would essentially disable the Exchange integration.
- This restricts access only to the calendar

By contrast, EWS impersonation provides the following alternatives to delegation:

- Allows access ONLY through Exchange Web Services
- Does grant permission to do anything the impersonated user could do (assuming it is available as part of EWS)
- End users do not see (and cannot change) the permissions

Additional Reading

The links below provide additional information from Microsoft® about Exchange Web Services (EWS).

- The Importance of EWS Impersonation
- Authentication and EWS in Exchange
- Impersonation and EWS in Exchange

  With Impersonation, a service account has full access to a defined set of mailboxes. What it can access in those mailboxes (such as specific folders) cannot be filtered or defined. Only an Exchange Admin can configure an EWS Impersonation account for impersonation and configure its mailboxes to allow the impersonation.
- Delegate Access and EWS in Exchange

  Delegate access allows a user to access certain folders in another user's mailbox Delegate permissions can be set by a mailbox owner or administrator using an app or other app code.

CHAPTER 45: Use Application Pool Identity for Integration for Exchange Service Account

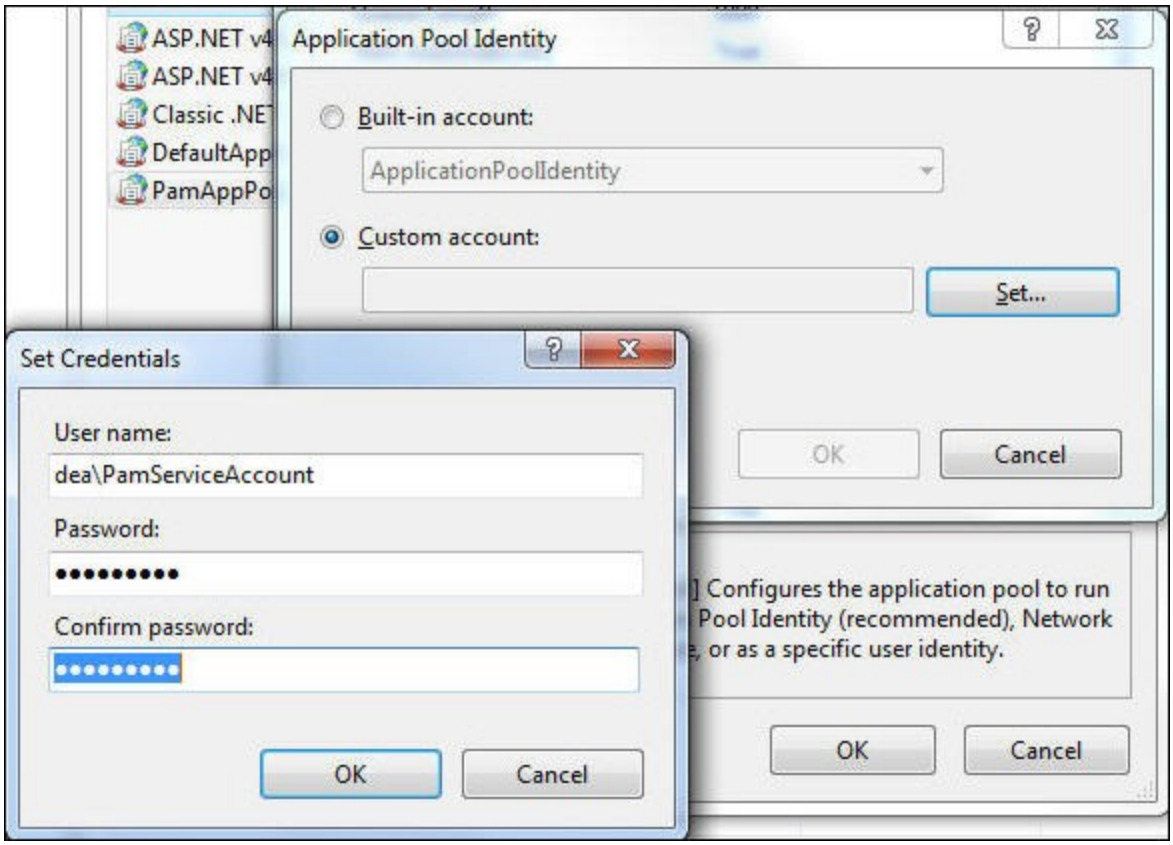
Rather than entering the Integration for Exchange account credentials on the PAMConfig.aspx page (as in V44 and previous releases), credentials can be maintained at the Application Pool level. This allows your organization to maintain absolute control—only IIS applications running in the newly created application pool can run as the Integration to Exchange Account.

This functionality requires the following:

- Microsoft Exchange 2007 (SP1) or Exchange 2010.
- Microsoft Exchange Impersonation Account (your EMS Integration to Exchange account). This account must be using Exchange Web Services (EWS) Impersonation, not full access to the mail-box store.

Configure the Application Pool

1. Open IIS Manager
2. Open the Application Pools panel
3. Click Add Application Pool…
4. The Add Application Pool window opens. Enter a unique name and ensure the correct .NET Framework is selected. Managed pipeline mode should be Integrated. Click OK
5. Find the Application Pool you just created. Right-click it and select Advanced Settings.
6. The third section in the list is Process Model. Highlight Identity and then click the (…) button to con-figure.
7. Choose Custom Account and then click Set. Enter the username and password for your EMS Integ-ration to Exchange account. Confirm the password and click OK on any remaining dialogs (see fol-lowing image).



8. Within IIS Manager, navigate to the Virtual Directory containing the Integration for Exchange Web Service. This is under the Default website by default, but can be installed to a different website.
9. With the IntegrationExchangeWebService Virtual Directory highlighted in the left pane, select Basic Settings… under Actions in the right pane.
10. Click the Select button and then choose your newly created application pool from the list.
11. Click OK on all remaining dialogs.

Configure Integration for Exchange to Use the Application Pool Account

1. Navigate to the Integration for Exchange configuration area by opening a browser and entering the following:
   http://[ServerName]/PAMWebService/PAMConfig.aspx (replace [ServerName] with the name of your web server)
2. From the Account Info tab, find the Authentication Information section, check the box for Use application pool identity when authenticating to calendaring service (see following image).
3. With this option enabled, you can leave the Username and Password fields blank in the Authentication Information section.

4. Click Save button at the bottom of the page.

EMS for Outlook -- April 2019

Accruent, LLC

11500 Alterra Parkway

Suite 110

Austin, TX 78758

www.accruent.com