

EMS for Outlook

Installation, Configuration, & User Guides

May 2019

Accruent Confidential and Proprietary, copyright 2019. All rights reserved.

This material contains confidential information that is proprietary to, and the property of, Accruent, LLC. Any unauthorized use, duplication, or disclosure of this material, in whole or in part, is prohibited.

No part of this publication may be reproduced, recorded, or stored in a retrieval system or transmitted in any form or by any means—whether electronic, mechanical, photographic, or otherwise—without the written permission of Accruent, LLC.

The information contained in this document is subject to change without notice. Accruent makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Accruent, or any of its subsidiaries, shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Table of Contents

CHAPTER 1: EMS for Microsoft® Outlook Add-In Installation Guide	1
Contact Customer Support	2
CHAPTER 2: Architecture of EMS for Outlook	3
CHAPTER 3: Prerequisites and Requirements for EMS for Outlook	4
Prerequisites	4
EMS for Outlook Requirements	5
Integration to Microsoft Exchange	5
EMS Platform Services Prerequisites	5
EMS Platform Services Requirements	6
CHAPTER 4: Plan Your EMS for Outlook Implementation	8
Obtain the EMS for Outlook Installation File	8
Install the EMS Integration for Microsoft Exchange	8
Install EMS Platform Services on Your Web Server	8
Install EMS for Outlook on Users' Computers	9
Configuration Path	9
CHAPTER 5: Install or Upgrade EMS for Outlook on Users' Computers	10
EMS for Microsoft Outlook Web Deployment Option	10
Benefits of Web Deployment Option	10
Web Deploy Service Installation on Server	10
Manual Installation (32-BIT or 64-bit)	11
Testing EMS for Outlook	11
CHAPTER 6: EMS for Outlook Add-In Is Offline	13
CHAPTER 7: Silent/Unattended EMS for Outlook Installation	14
CHAPTER 8: Where to See Your Exchange Server URL and EMS for Outlook Version Number	15
CHAPTER 9: Introduction to EMS Integrated Authentication	16
What is Integrated Windows Authentication?	17
What is Portal or Federated Authentication?	17
What is LDAP Authentication?	18
Contact Customer Support	19

CHAPTER 10: Integrated Authentication Considerations	20
LDAP Integration	20
Pros	20
Cons	20
Integrated Authentication	20
Pros	20
Cons	21
Portal Authentication	21
CHAPTER 11: Integrated Windows Authentication	22
Activate Integrated Windows Authentication for IIS 6.0	22
Activate Integrated Windows Authentication for IIS 7.x/8.x	24
CHAPTER 12: Manage Everyday Users For Integrated Authentication	25
Manually Create Everyday User Accounts	25
Automatically Create Everyday User Accounts	25
EMS Web App Parameters	25
Portal/Federated Authentication Parameters	26
HR Toolkit (for EMS Workplace, EMS Campus, EMS Enterprise, EMS District, and EMS Legal only)	26
Automatic Template Assignment to Users	27
Modify Existing Everyday User Accounts	27
CHAPTER 13: Configure EMS Web App to Use LDAP Authentication	28
Overview	28
Configure EMS Web App to Use LDAP Authentication	29
Configure EMS Web App Security	30
Configure Communication Options	31
Core Properties	32
Non-AD Configuration	32
LDAP Queries	33
Save Your Configuration	34
Test Your Configuration	34
Configure Authentication for EMS Mobile App	34

CHAPTER 14: Portal or Federated Authentication	35
Portal Authentication Overview	35
Installation/Configuration	36
Redirect User Log In to Your SSO Provider	36
Specify a Different Default Home Page for Guest Users	37
CHAPTER 15: Portal Authentication Methods	38
Server Variable Method (Header Variable)	38
Server Variable Method – Federated (SAML)	38
Method 1: Locally installed Service Provider	39
Method 1 Configuration Steps	39
Method 2	39
Method 2 Configuration Steps	39
EMS Desktop Client Configuration	40
Session Method	40
Form Method	40
Cookie Method	41
Query String Method	42
CHAPTER 16: EMS Integration to Microsoft® Exchange Installation and Configuration Guide	43
Exchange Integration Flow	44
Contact Customer Support	45
CHAPTER 17: System Requirements for Integration to Microsoft® Exchange	46
Web Server Requirements	46
EMS Web App Requirements	47
EMS Web App (Mobile)	47
EMS Platform Services	48
EMS for Microsoft Outlook Requirements	49
Integration to Microsoft Exchange	49
CHAPTER 18: Install or Upgrade the Exchange Integration Web Service	50
Prior to Install or Upgrade	50
Install or Upgrade Instructions	50

CHAPTER 19: Configure Integration to Microsoft Exchange	52
Configure Integration to Exchange Instructions	53
Test Your Exchange Integration	54
Optional Messaging Settings	54
Enable Larger File Attachments On The Config File	56
Enable Larger File Attachments in the Exchange Integration Web Service	57
CHAPTER 20: Configure Multiple Mail Domains	58
CHAPTER 21: Use Application Pool Identity for Integration for Exchange Service Account	60
Configure the Application Pool	60
Configure Integration for Exchange to Use the Application Pool Account	61
CHAPTER 22: Configure EWS Impersonation for Microsoft® Exchange	63
CHAPTER 23: Learn More About Exchange Web Services (EWS) Impersonation	64
FAQs	64
Additional Reading	65
CHAPTER 24: EMS for Microsoft® Outlook Add-In Configuration Guide	66
Contact Customer Support	66
CHAPTER 25: Configure EMS for Outlook	68
Customize the Add-In Label	68
Customize the Add-in icon	68
EMS for Outlook System Parameters	69
Enable User Access to EMS for Outlook	70
Assign EMS Users to Groups	72
Establish Booking Templates for EMS for Outlook Users	73
CHAPTER 26: EMS for Microsoft® Outlook Add-In User Guide (v8)	76
Contact Customer Support	77
CHAPTER 27: Microsoft Outlook, EMS for Microsoft Outlook, and EMS Web App Comparison	78
CHAPTER 28: Create a Reservation in EMS for Microsoft Outlook	79
CHAPTER 29: Create a Single Reservation	80
CHAPTER 30: Create a Series Reservation	84
CHAPTER 31: Create a Video Conference Reservation	88

CHAPTER 32: Edit or Cancel a Reservation	91
CHAPTER 33: Skype for Business in EMS for Outlook	92
Add Skype for Business to Your Reservation	92
CHAPTER 34: Resolve Booking Conflicts	94
Resolve Booking Conflicts for a Series Reservation	94
Resolve Booking Conflicts When You Receive a Warning Email	95
CHAPTER 35: View Known Errors/Alerts for EMS for Outlook	97

CHAPTER 1: EMS for Microsoft® Outlook Add-In 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.



Important!

To upgrade to Update 17 of EMS for Outlook, you will need to uninstall your legacy version and re-install.

This guide provides information about the following topics:

- [Requirements and Prerequisites for EMS for Outlook](#)
- [Architecture of EMS for Outlook](#)
- [Plan Your EMS for Outlook Implementation](#)
- [Install or Upgrade EMS for Outlook on Users' Computers](#)
 - [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](#)

See Also: EMS Integration to Microsoft® Exchange Installation and Configuration Guide topics:

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

Contact Customer Support

- **Option 1 (Recommended):** Search the Knowledge Base available at [Accruent Access](#).
- **Option 2:** Submit a case directly via [Accruent Access](#).
- **Option 3:** Email emssupport@accruent.com.
- **Option 4:** Phone (800) 288-4565.

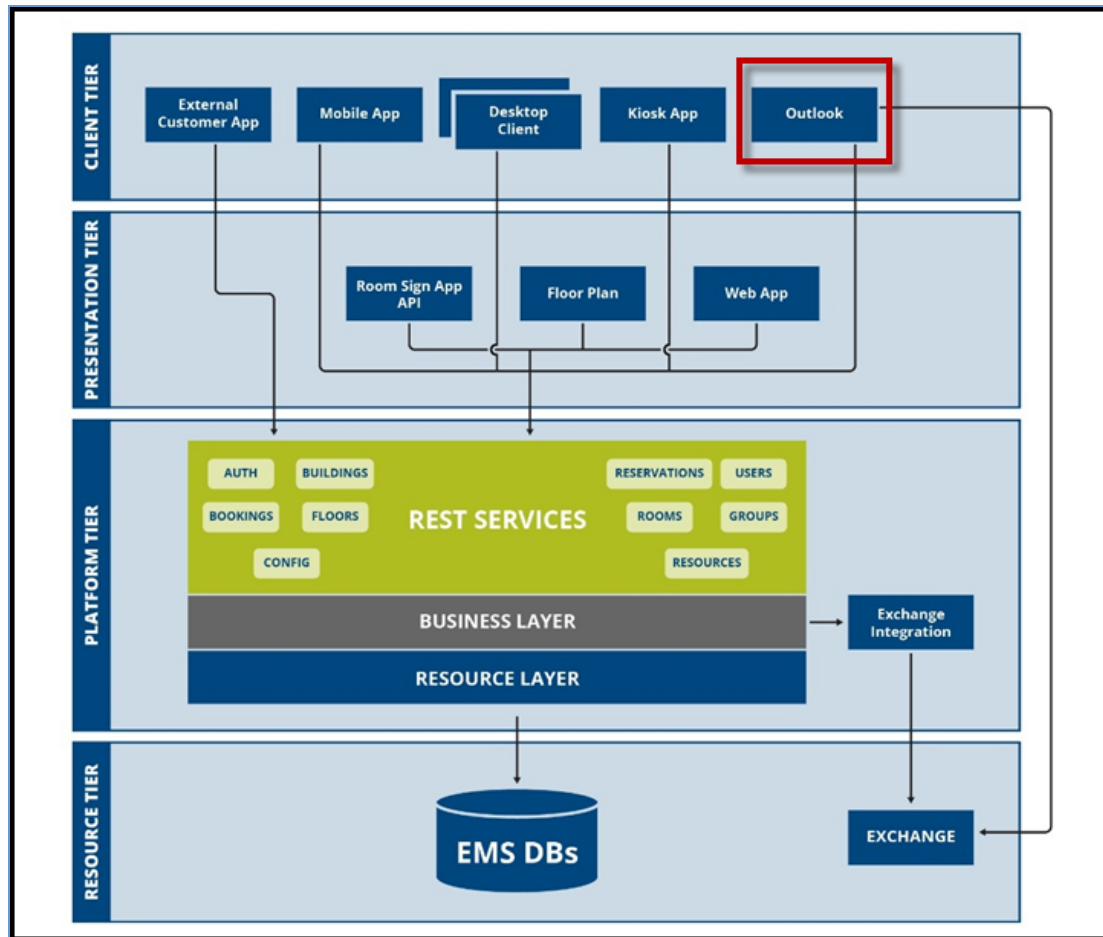


Important!

If you do not have a customer login, register [here](#).

CHAPTER 2: Architecture of EMS for Outlook

As of the September 2017 Release, EMS for Outlook is integrated with EMS Platform Services, an add-on, middle-tier component that provides a modern, scalable way for partners and customers to integrate with the EMS Platform. Platform Services enables the development of multi-platform applications that can be customized, cloud-based, scalable, and easily integrated.



EMS System Architecture

CHAPTER 3: Prerequisites and Requirements for EMS for Outlook



Important!

The September 2017 Release included a redesign of the EMS for Outlook add-in. This redesign included an enhanced user interface and streamlined functionality. Documentation for EMS for Outlook prior to the September 2017 Release is referred to as EMS for Outlook (Legacy) documentation.

This topic provides information on how to install EMS for Outlook, including:

- [Prerequisites](#)
- [EMS for Outlook Requirements](#)
- [EMS Platform Services Prerequisites](#)
- [EMS Platform Services Requirements](#)

See Also: [System Architecture](#)

Prerequisites

To successfully install EMS for Outlook:

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, see [Integration to Microsoft® Exchange](#).
3. Install Platform Services.



Note:

You can quickly verify if the service has been installed by opening a browser and entering the following:

http://[ServerName]/EMSPlatform/ (replace [ServerName] with the name of your web server)

The Platform Services Address will be required when running the **EMSForOutlook.msi** (see also: [Exchange Server URL and EMS for Outlook Version Number](#)).

4. EMS must be [configured](#) properly in order to [activate](#) the EMS for Outlook for each Outlook® user.
5. Verify that the required software is installed on your users' workstations.

EMS for Outlook Requirements

Microsoft® Office	365
Outlook (32- and 64-bit)	2010, 2013, 2016
.NET Framework	4.6.1
Microsoft® Visual Studio 2010 Tools for Office Runtime	VSTO 2010
Prerequisites	
EMS Web App	Latest
On User Workstations	Desktop requirements for Microsoft® Outlook Windows 7, 8, or 10

Integration to Microsoft Exchange

Microsoft® Exchange	2010 SP3, 2013, 2016
Microsoft® Office	365

See Also: [Exchange Web Services \(EWS\) Impersonation](#) and [Configure EWS Impersonation](#)

EMS Platform Services Prerequisites

HTTPPlatformHandler IIS Module	Download Version 1.2 here OR download the installer here .
--------------------------------	--

PowerShell	5+ Version
ASP.NET Version 4.6	Under Web Server (IIS)->Web Server->Application Development: <ul style="list-style-type: none"> • ISAPI Extensions • ISAPI Filters • .NET Extensibility 4.6

EMS Platform Services Requirements

Operating System	IIS
Windows Server 2012	8
Windows Server 2012 R2	8.5
.NET Framework	4.6.1
Application Pool	4.0

Prerequisites (Prior to Update 28)

HTTPPlatformHandler IIS Module	Download Version 1.2 here OR download the installer here .
PowerShell	5+ Version
ASP.NET Version 4.6	Under Web Server (IIS) > Web Server > Application Development: <ul style="list-style-type: none"> • ISAPI Extensions • ISAPI Filters • .NET Extensibility 4.6

Prerequisites (Update 28 and Later)

ASP.NET Core	See Also: Installing ASP.NET Core .
PowerShell	5+ Version
ASP.NET Version 4.6	Under Web Server (IIS) > Web Server > Application Development:

Operating System	IIS
	<ul style="list-style-type: none"><li data-bbox="678 281 902 310">• ISAPI Extensions<li data-bbox="678 338 846 367">• ISAPI Filters<li data-bbox="678 394 951 424">• .NET Extensibility 4.6

CHAPTER 4: Plan Your EMS for Outlook Implementation

There are several steps that your Administrator must complete when installing EMS for Outlook:

1. [Obtain the installation files](#) from the EMS Customer Portal.
2. [Install the EMS Integration for Microsoft Exchange](#).
3. [Install EMS Platform Services](#) and connect to your organization's web server.
4. [Install EMS for Outlook on Users' Computers](#).
5. Ensure the [Configuration Path](#) is correct.

Obtain the EMS for Outlook Installation File

1. Log into [Accruent Access](#).
2. Click **My Products**.
3. Under **EMS**, click **Downloads**.
The downloads page opens in a new browser tab.
4. In the **Software Downloads** area, click the link for your version of software, for example, **V44.1 Releases & Patches**.
A new page opens listing the downloads available based on your license.
5. Download **EMS For Outlook (EMSForOutlook.msi)** (required for both first time installations and upgrades).

Install the EMS Integration for Microsoft Exchange

This service (typically [installed](#) where your EMS Web App resides) manages the integration between EMS Software and Exchange, including checking room availability, booking the meeting in EMS, and managing changes.

**Note:**

The Exchange Integration service needs to be properly configured. For complete instructions, see the [Integration to Microsoft® Exchange](#) guide.

Install EMS Platform Services on Your Web Server

1. Log into [Accruent Access](#).
2. Click **My Products**.
3. Under **EMS**, click **Downloads**.

The downloads page opens in a new browser tab.

4. In the **Software Downloads** area, click the link for your version of software, for example, **V44.1 Releases & Patches**.

A new page opens listing the downloads available based on your license.

5. Download the **EMSPPlatformServices.msi** file.
6. Run this file on your web server.

**Note:**

You will need to enter the SQL server and EMS database. Make a note of the database name. The typical install path is C:\Program Files\EMS Software\Ems.Platform.Api.

7. When all prompts have been completed, click **Install**. The API is installed on your web server.
8. You will also need a Virtual Directory Name (typical default is EMSPlatformServices). Make a note of the new site you have created. This URL will need to be entered during the installation process (e.g., [http://\[ServerName\]/EMSPPlatform/](http://[ServerName]/EMSPPlatform/) [replace with the name of your web server]).

Install EMS for Outlook on Users' Computers

This add-in should be installed on your users' desktops. You will be prompted to supply the Platform Services URL during the installation process. 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

**Note:**

A 64-bit machine installation will require an elevated permission level.

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

Configuration Path

EMS must be [configured](#) properly to activate EMS for Outlook for each Outlook user:

1. The Outlook user must have an active EMS Everyday User account.
2. The EMS Everyday User account must be assigned to [at least one Everyday User Process Template](#) with the Outlook option enabled.
3. The EMS Everyday User account must be [associated to an active EMS Group record](#).

CHAPTER 5: Install or Upgrade EMS for Outlook on Users' Computers



Important!

The installation/upgrading process must begin by uninstalling previous versions of the EMS for Outlook add-in.

EMS for Microsoft Outlook Web Deployment Option

As of the Update 19.1 software release (December 2017), a web deployment option is now available for EMS for Microsoft Outlook. This is the recommended method for installing EMS for Outlook locally on individual user machines. Administrators can use the web deployment to host EMS for Outlook on a web server, with the ability to push the URL to any EMS Administrators so they can download EMS for Outlook without needing Administrative Privileges on their local machine.

For either 32- or 64-bit installation, you will also need an EMS Platform Services Virtual Directory Name (typical default is EMSPlatform). Make a note of the new site you have created. This URL will need to be entered during the installation process (e.g., [http://\[ServerName\]/EMSPlatform/](http://[ServerName]/EMSPlatform/) [replace ServerName with the name of your web server]).

Benefits of Web Deployment Option

The web deploy application is installed on your web server. The EMS for Outlook Add-in is included within this installation. Once installed, end users point their web browsers to the EMS Web Deployment Application, which points them with a link to download the EMS for Outlook Add-in. Once a user downloads and runs that link, the EMS for Outlook is installed in the user's profile on that workstation. Once installed, the EMS for Outlook Add-in will check the server for an updated version of the client each time the client is launched. If a new version is available, then it will automatically download and install the update.

Web Deploy Service Installation on Server

1. Verify that the Requirements and Prerequisites have been met.
2. Download the **EMS.Outlook.WebDeploy.msi** file onto the user's desktop.
3. Close Outlook.
4. Run **EMS.Outlook.WebDeploy.msi**.
5. The first screen welcomes you to the EMS Outlook Web Deploy Setup Wizard.
6. Click the **Next** button to begin the installation process. The Destination Folder screen will appear.

7. Specify the Installation Folder.
8. Click the **Next** button. The EMS Platform Services screen will appear.
9. Enter the address your organization uses (e.g., [http://\[ServerName\]/EMSPlatform](http://[ServerName]/EMSPlatform)).
10. Click the **Next** button. The Ready to install EMS for Outlook Web Deploy screen will appear.
11. Click the **Install** button to complete the installation. Click the **Close** button to exit.

Manual Installation (32-BIT or 64-bit)



Note:

A 64-bit installation requires an elevated permission level.

1. Verify that the Requirements and Prerequisites 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.
6. Click the **Next** button to begin the installation process. The Destination Folder screen will appear.
7. Specify the Installation Folder.
8. Click the **Next** button. The EMS Platform Services screen will appear.
9. Enter the address your organization uses (e.g., [http://\[ServerName\]/EMSPlatform](http://[ServerName]/EMSPlatform)).
10. Click the **Next** button. The Ready to install EMS for Outlook screen will appear.
11. Click the **Install** button to complete the installation. Click the **Close** button to exit.
12. Launch Outlook. The **EMS** button should display on the user's Outlook toolbar on the Calendar as online.



Note:

If the EMS for Outlook displays as Offline, see [EMS for Outlook Add-In Is Offline](#).

Testing EMS for Outlook

EMS Software recommends that customers test new versions of EMS for Outlook before deploying to production. Ideally, customers would have PROD and TEST Exchange environments to pair with the PROD and TEST EMS environments, and separate machines for each environment (e.g., have a machine dedicated to being connected to the test environment).

When creating a reservation in EMS for Outlook, the application stores a unique “PAM ID” on the reservation in EMS and stores the EMS Reservation ID on the Exchange object (meeting/appointment) in order to establish the link between the two systems.

If the customer has both PROD and TEST linked to the same Exchange environment, here is the risk:

1. User creates reservation 1234 while connected to TEST EMS.
2. User switches connection (by changing Platform URL) to PROD EMS.
3. User cancels reservation 1234 from Outlook, that was originally created in TEST EMS.
4. Since the connection was changed to PROD, instead of canceling 1234 in TEST, 1234 is canceled in PROD. 1234 in TEST and PROD are almost guaranteed to be two completely different reservations for different users. So the user has now canceled an unrelated reservation in PROD by accident.

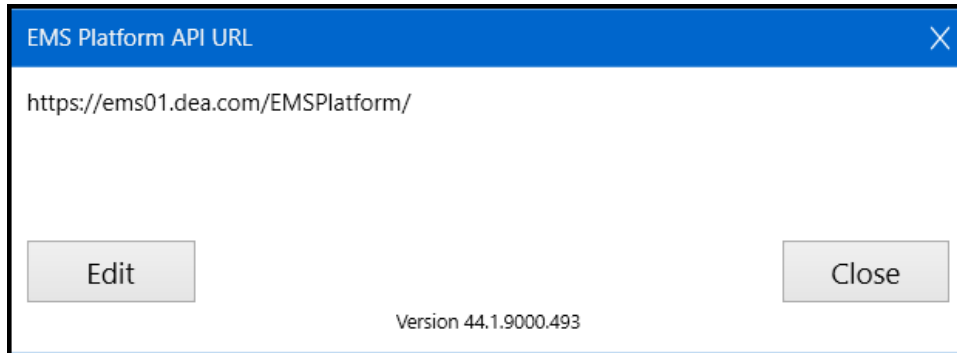
Having separate TEST and PROD Exchange environments is the best way to avoid the problem; however, this is often impractical and costly, if not impossible. The alternative option is to be careful and deliberate when following the guidelines below:

1. Users can use a single machine.
2. Install TEST EMS for Outlook version, connect with TEST Platform URL.
3. Make reservations according to test cases and include TEST in the subject line of all meetings created here to help distinguish them.
4. If they are tracking with UAT test cases they can document the date/time/reservation ID used for each test case in order to help track these.
5. Before going back to PROD EMS for Outlook, all TEST reservations must be canceled while still connected to TEST EMS.
6. Once all TEST reservations are canceled, the normal process of uninstalling the TEST EMS for Outlook and reinstalling with PROD can go forward (ensure the Platform URLs are correct).

CHAPTER 6: 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 should perform this step. See Also: [Integration to Microsoft® Exchange](#).

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

CHAPTER 7: Silent/Unattended EMS for Outlook Installation

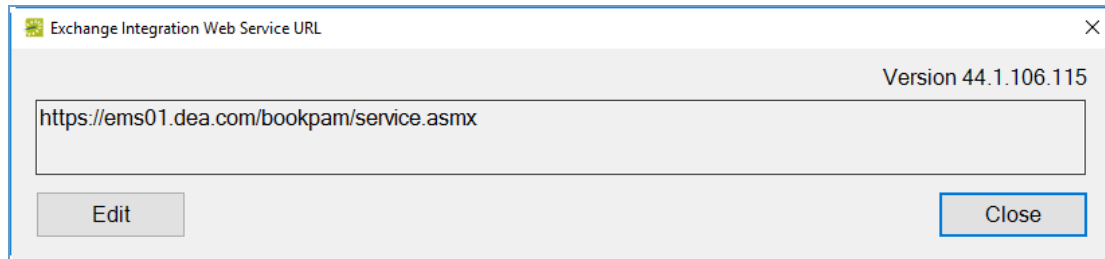
You can push your EMS for Outlook Installation to user machines if your system enables this type of administration.

Use the following command to establish an Unattended/Silent installation of the **EMSForOutlook.msi** (replace <url> with your URL):

```
msiexec /i " EMSForOutlook.msi" RSURL="https://<url>"  
  
msiexec /i " EMSForOutlook.msi" /quiet /qn /norestart RSURL=  
L="https://<url>"
```

CHAPTER 8: Where to See Your Exchange Server URL and EMS for Outlook Version Number

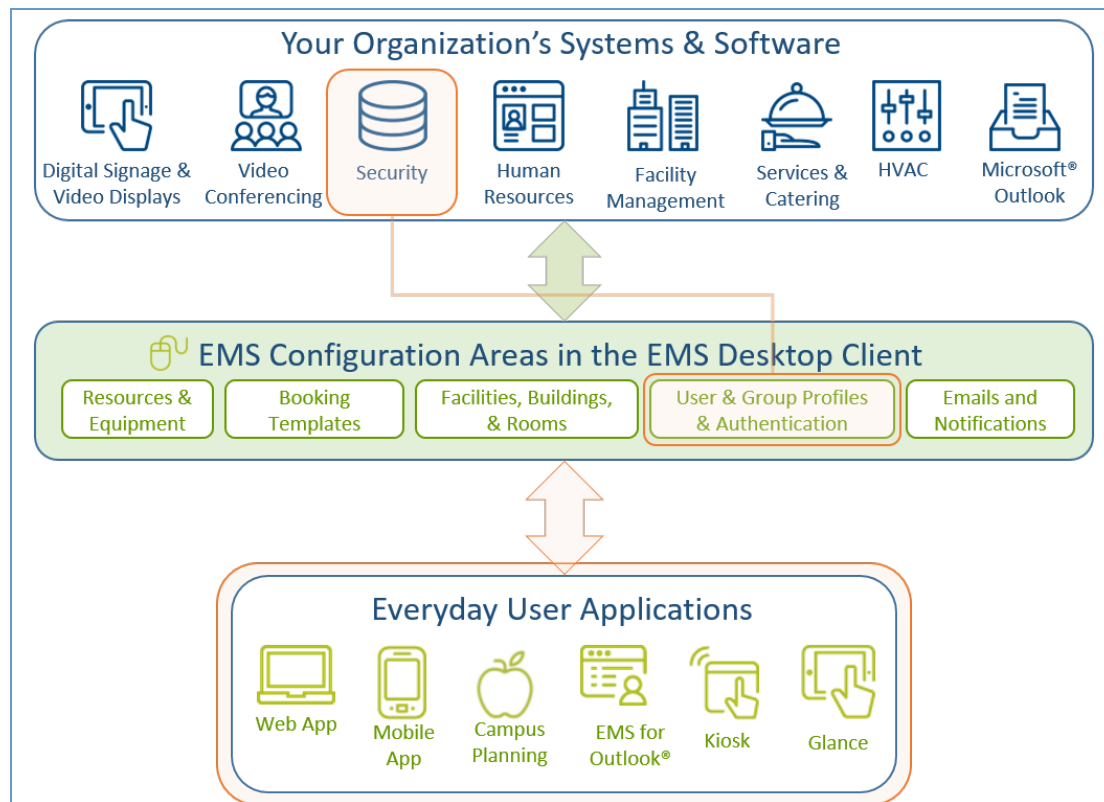
Click the EMS for Outlook icon from the Outlook toolbar. A pop-up shows the Version number of the add-in and the Exchange Integration Server URL.



CHAPTER 9: 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.

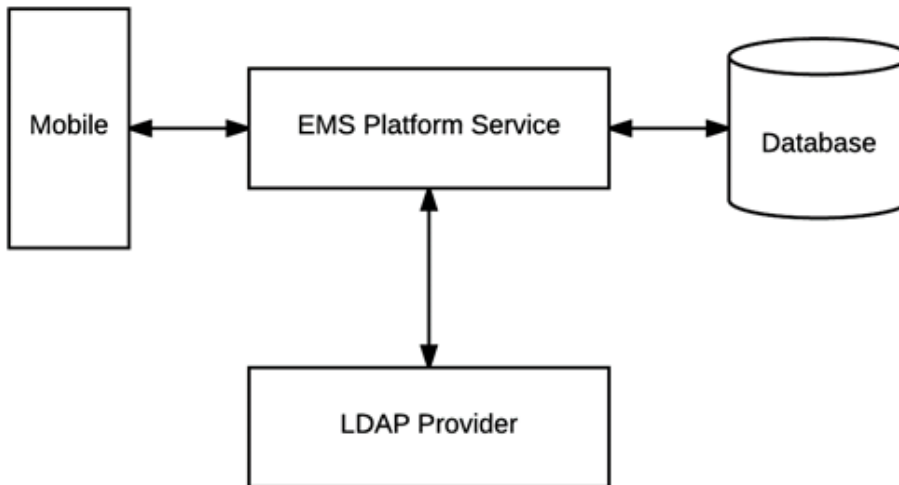
Several built-in authentication methods to pass-in credentials are available including:

- 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.

**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.
- 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 at [Accruent Access](#).
- **Option 2:** Submit a case directly via [Accruent Access](#).
- **Option 3:** Email emssupport@accruent.com.
- **Option 4:** Phone (800) 288-4565.

**Important!**

If you do not have a customer login, register [here](#).

CHAPTER 10: Integrated Authentication Considerations

When you purchase the Integrated Authentication Service, you are able to use LDAP Integration, Integrated Authentication (IA), or Portal Authentication. Integrated and Portal Authentications are true Single Sign-On (SSO) solutions; LDAP is not. These methods are not typically used together. This section explains how each one works, along with pros and cons for each method.

LDAP Integration

LDAP integration allows you to bypass creating individual web users for your organization. By configuring EMS to query your LDAP groups, you can use LDAP groups to assign web template permissions. Your users would just use their windows credentials to login to the site. After creating a web user account (most data is pre-populated from their LDAP account), they receive the template permissions granted to their LDAP group.

Pros

- No need to create/maintain individual accounts for web users. Mass assign process templates.

Cons

- Requires LDAP groups to be precisely defined and maintained to ensure proper access. EMS does not create or update LDAP groups, so product may require assistance from LDAP/Exchange administrators.
- NOT Single Sign-on: users must enter windows credentials on each visit.

Integrated Authentication

IA is SSO. For this to work, every user must have a web user account created (manually through client/virtual piece or using our HRToolkit module). In each web account, a network ID is added. When a user visits VEMS or EMS Web App, a call is made to the machine to retrieve the windows account signed in. It compares that value to the network ID field in existing accounts, logging in users automatically. Permissions are assigned to the individual web user accounts.

Pros

- Can be true SSO – the account creation and maintenance can be completely invisible to the end user. Not reliant on Exchange/LDAP administrators.

Cons

- Requires active web user creation and maintenance: manually on the client side, manually through end-user input, or automatically through an HR feed.

Portal Authentication

With Portal Authentication, user information is passed from your existing portal to records in EMS by cookie, session string or similar. Portal Authentication is true SSO when used with our supported methods.

**Note:**

When you implement Integrated Authentication, your consultant will assist you with creating templates and web users during onsite training. If you are adding this module separately and need assistance with virtual configuration contact your account manager about purchasing training. This document is intended to explain the different authentication options available, so you can anticipate any configuration needs. If you choose LDAP Integration, you will need to create an administrator account and admin web template to access the configuration page. See the EMS Configuration Guide for questions with creating that template. Using LDAP with IA or Portal Authentication requires each user be responsible for creating/verifying their account on the first visit; SSO isn't immediate. Portal authentication can be used with LDAP, but this is atypical in most portal environments since other credentialing is available.

CHAPTER 11: 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.

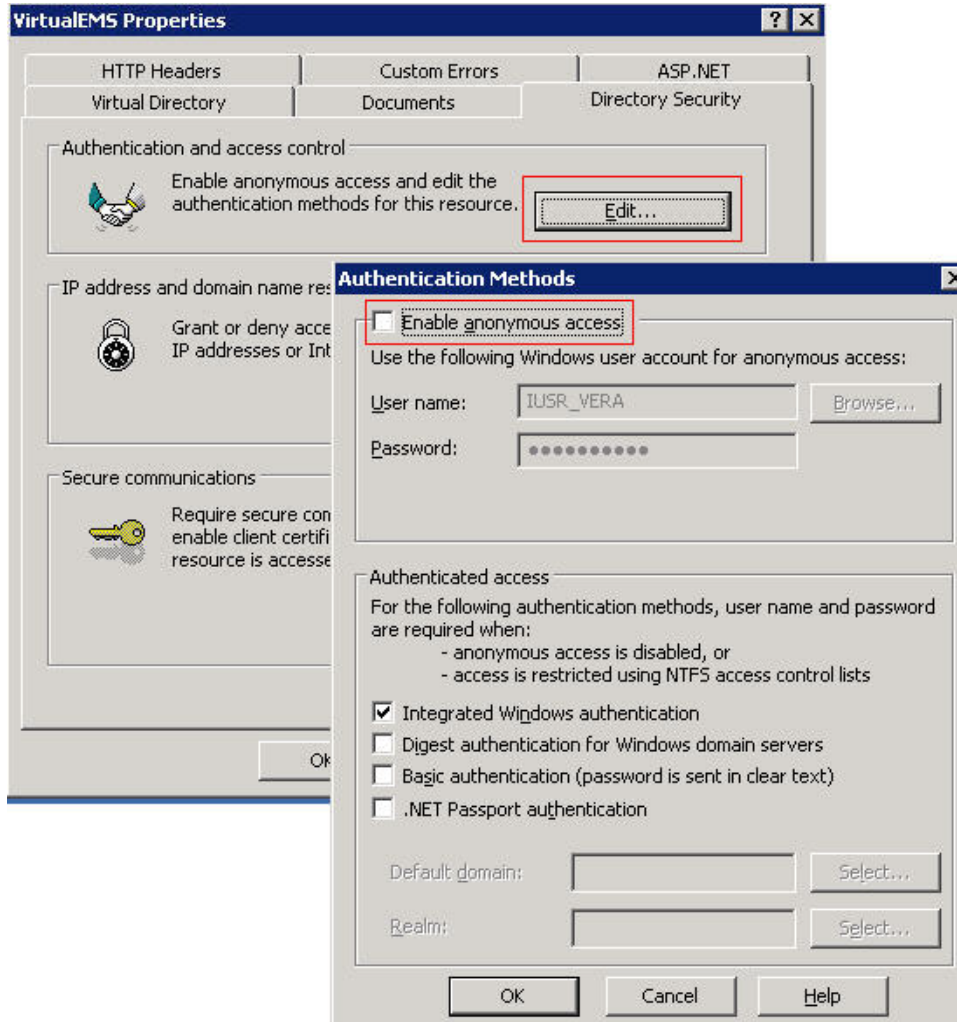
**Note:**

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.

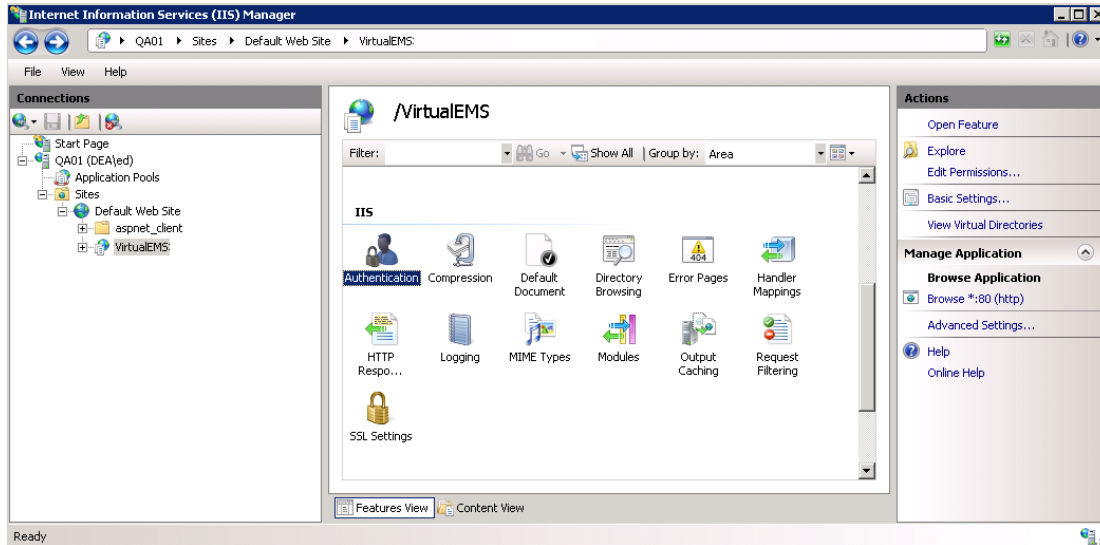
4. Go to the **Directory Security** tab and click the **Edit** button under the Authentication and access control section. The Authentication Methods screen will open.
5. Uncheck the **Enable anonymous access** option. The **Integrated Windows authentication** option should be the only option checked.



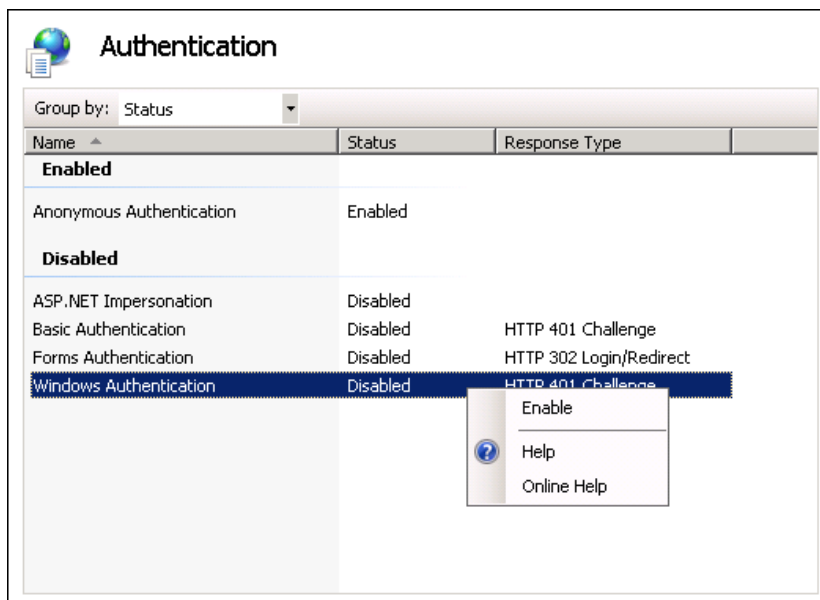
6. Click **OK** to exit the Authentication Methods screen. Click **OK** again to exit the Properties screen. You have completed the necessary IIS configuration steps for IIS 6.0.

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 12: Manage Everyday Users For Integrated Authentication

In order to make a reservation in EMS Everyday User Applications, such as EMS Web App, EMS Mobile App, and EMS for Outlook, a user must have an active Everyday User account with appropriate security and process templates.

In EMS, you can create Everyday User accounts as follows:

- [Manually Create Everyday User Accounts](#)
- [Automatically Create Everyday User Accounts](#)
- [Modify Existing Everyday User Accounts](#)

Manually Create Everyday User Accounts

Everyday User accounts can be created manually by EMS Administrators within EMS Desktop Client or by anonymous Everyday Users on their respective EMS Everyday Applications.

To create Everyday User accounts in the EMS Desktop Client, see [Configure Everyday Users](#).

To configure EMS Web App to allow anonymous Everyday Users to request an account, you adjust parameters. See also: [EMS Web App System Parameters](#).



Important!

When manually creating an Everyday User account in an Integrated Authentication environment, you must specify a value in the Everyday User Network ID field or the External Reference field. The Field Used to Authenticate Everyday User parameter (within **System Administration > Settings > Parameters > Everyday User Applications** tab) is used to determine which value should be used for authentication.

Automatically Create Everyday User Accounts

Various configuration settings are available to automatically create Everyday User records (and assign the appropriate Security and Process Template(s) if applicable) when a user accesses an EMS Everyday User Application (such as EMS Web App for the first time).

EMS Web App Parameters

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

Area	Description	Value
Account Management	Auto Create Everyday User Account (for Integrated Authentication)	Yes
Account Management	Default Security Template for User	<i>Must be specified</i>
Account Management	Default Account Status for Newly-Created User	Active

Portal/Federated Authentication Parameters

For organizations using Portal or Federated authentication, EMS supports a simple account provisioning strategy. When using Auto Create, EMS requires that a Everyday User account is provisioned with a name, an email address and a NetworkId (some authentication key). Otherwise, the user will be redirected to the Account Management page and be asked to manually enter the required information. In addition to the required fields, EMS also supports collecting phone, fax, and an external reference value. The parameters below are meant to help create a more complete Everyday User. The values for each of the parameters are to be determined by the information populated by your portal.

Area	Description	Value
Authentication	Portal Authentication Email Variable	<i>Must be specified</i>
Authentication	Portal Authentication External Reference Variable	<i>Must be specified</i>
Authentication	Portal Authentication Fax Variable	<i>Must be specified</i>
Authentication	Portal Authentication Name Variable	<i>Must be specified</i>
Authentication	Portal Authentication Phone Variable	<i>Must be specified</i>

HR Toolkit (for EMS Workplace, EMS Campus, EMS Enterprise, EMS District, and EMS Legal only)

The HR Toolkit is an optional component that allows you to automate the creation and maintenance of Everyday User records in EMS using an outside employee data source like your HR system or another data store within your organization. Please refer to the [HR Toolkit Installation Instructions](#) for information. If you are not licensed for the HR Toolkit, but would like to learn more about it, please contact your Account Executive.

Automatic Template Assignment to Users

The Default Security Template for User parameter shown above is used to automatically assign the correct Everyday User Security Template to new Everyday User records.

You can automatically assign default Everyday User Process Templates when a new Everyday User account is created. To automatically assign a Everyday User Process Template to new Everyday Users, select the Available to New Everyday Users option within your Everyday User Process Template(s) (**Configuration > Everyday User Applications > Everyday User Process Templates (Edit the template > Process Templates tab)**)).

EMS customers using the LDAP Authentication method can use an alternate method to assign a Everyday User Process Template to a Everyday User based on the LDAP Group(s) to which the user belongs. This approach can be used in addition to or in lieu of the Everyday User Process Template assignment approach discussed above. Please see the [LDAP Authentication](#) section for configuration instructions.

Modify Existing Everyday User Accounts



Important!

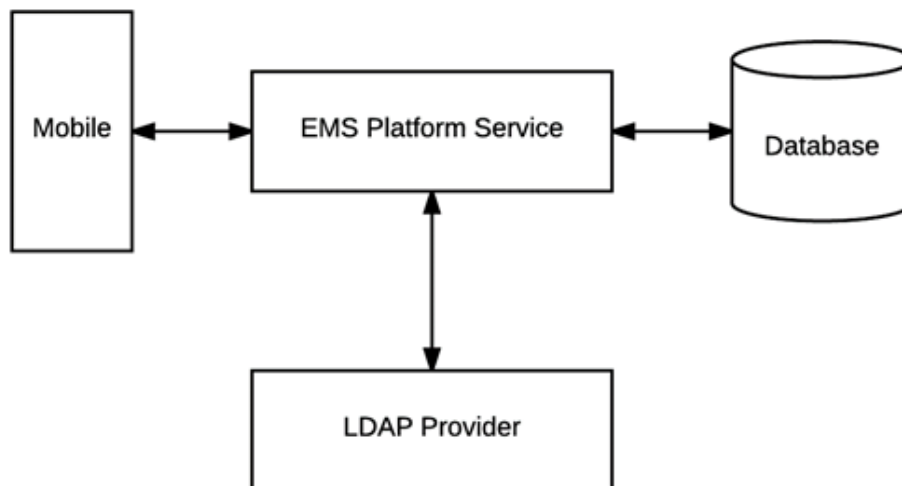
EXISTING EMS CUSTOMERS

Before activating any Integrated Authentication option, the **Network ID** field or **External Reference** field must be populated on all existing Everyday User records. Ignoring this step may result in duplicate Everyday User records.

CHAPTER 13: Configure EMS Web App to Use LDAP Authentication

Overview

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.



This topic provides information on the following:

- [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](#)

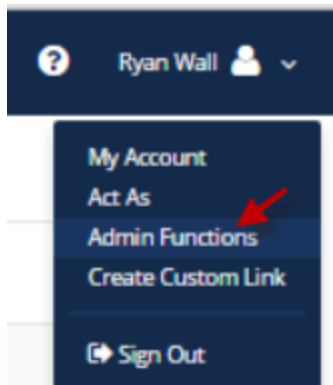
When a user logs into EMS Web App or EMS Mobile App with their User ID and Password, their credentials are authenticated against LDAP and compared against corresponding user information recorded in the **Network ID** and/or **External Reference** fields of your EMS Everyday User records. If a match exists,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

**Note:**

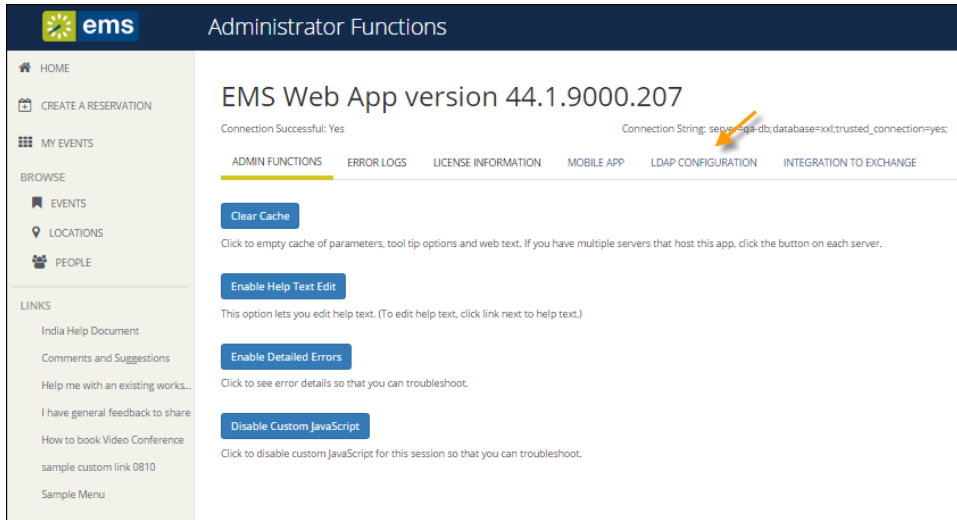
- The EMS Web App LDAP-Process Template assignment process requires that your implementation of LDAP stores group information (e.g., staff, student, department, etc.) as a Directory Service object containing a property (i.e., member) that contains the users that belong to your various groups.
- The Field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

Configure EMS Web App to Use LDAP Authentication

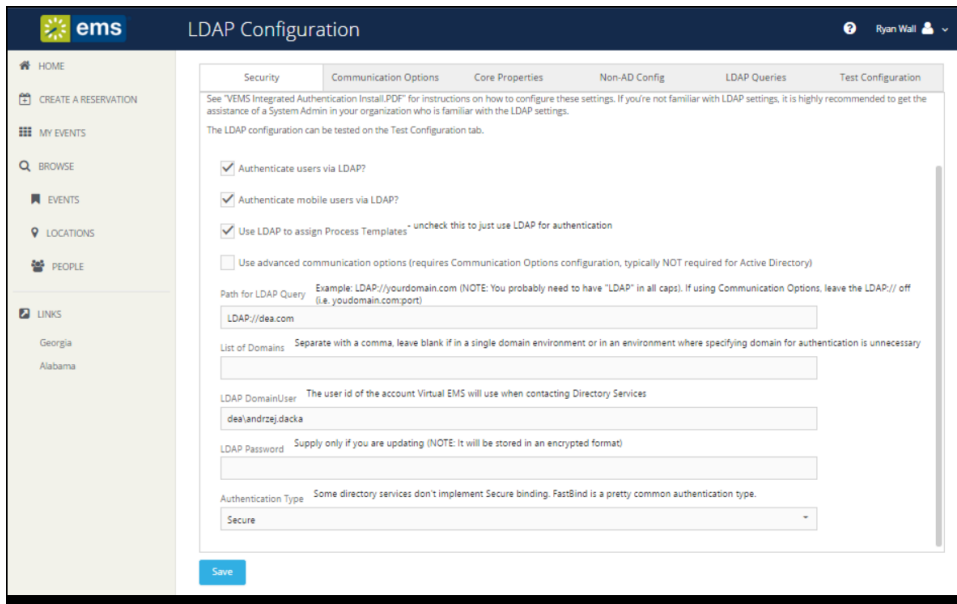
1. Log into EMS Web App with a User that belongs to an Everyday User Security Template containing the **Web Administrator** role (controlled in the EMS Desktop Client under **Configuration** > **Everyday User Applications** > **Everyday User Security Templates**).
See Also: [Configure Security Templates](#).
2. From the User Options, select **Admin Functions**.



3. Then click the **LDAP Configuration** tab.



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



Configure EMS Web App Security

On the **Security** tab:

1. Select the **Authenticate users via LDAP** checkbox to enable LDAP authentication.
2. If LDAP will be used to assign Everyday User Process Templates to your Web Users, select the **Use LDAP to assign Process Templates** checkbox.

3. **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.
4. In the **Path for LDAP Query** field, specify a valid LDAP path (example – LDAP://YourCompany.com)
5. **List of Domains:** Skip this step if your organization uses a single domain. Otherwise, provide a comma separated list of your domains.
6. In the **LDAP Domain\User** field, enter a Domain User account that has rights to query LDAP (example – YourDomain\User)
7. In the **Password** field, enter a valid Password for the User Account entered in the previous step.
8. 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.

Configure Communication Options

**Important!**

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



Important!

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



Important!

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



Important!

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 be 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).

Auth attempted with: jen.nausec Authentication successful LDAP UserName = Jen Nausec LDAP Phone = LDAP Fax = LDAP EmailAddress = Jen.Nausec@emssoftware.com LDAP NetworkId = Jen.Nausec User belongs to the following groups: Users,Certificate Service DCOM Access,Domain Users,Staff,VPN Users,Testers,SupportSecurity,WirelessAccess,Hourly Billing,TFS Full Web Access,SophosUser,SupportTFS, success

- 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.

Configure Authentication for EMS Mobile App

1. If your organization uses EMS Mobile App, click the **Mobile App** tab.
2. [Choose the LDAP option](#).

CHAPTER 14: Portal or Federated Authentication

This topic provides information on the following:

- [Portal Authentication Overview](#)
- [Installation/Configuration](#)
 - [Redirect User Log In to Your SSO Provider](#)
 - [Specify a Different Default Home Page for Guest Users](#)

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](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 15: Portal Authentication Methods

This topic provides information about the following:

- [Server Variable Method \(Header Variable\)](#)
- [Server Variable Method – Federated \(SAML\)](#)
 - [Method 1: Locally installed service provider](#)
 - [Method 2](#)
- [EMS Desktop Client Configuration](#)
 - [Session Method](#)
 - [Form Method](#)
 - [Cookie Method](#)
 - [Query String Method](#)

**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]/ EMSWe-  
bApp/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.

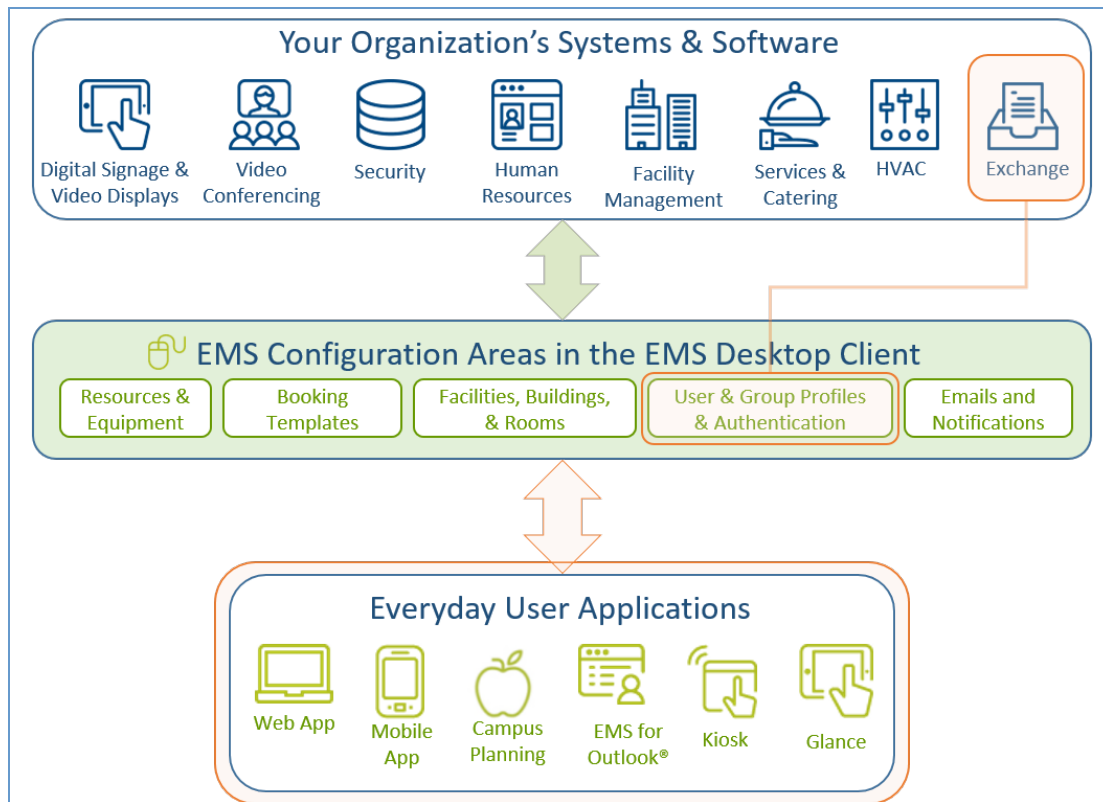
CHAPTER 16: EMS Integration to Microsoft® Exchange Installation and Configuration Guide

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

Contact Customer Support

- **Option 1 (Recommended):** Search the Knowledge Base available at [Accruent Access](#).
- **Option 2:** Submit a case directly via [Accruent Access](#).
- **Option 3:** Email emssupport@accruent.com.
- **Option 4:** Phone (800) 288-4565.



Important!

If you do not have a customer login, register [here](#).

CHAPTER 17: 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

Operating System	IIS VERSION
Windows Server 2016	10.0
Windows Server 2012	8.0
Windows Server 2012 R2	8.5
Windows Server 2016	
Prerequisites	
Application Pool Running	(2.0 or 4.0 depending on the EMS Software Application)
.NET Framework 4.6.1**	
Minimum System Requirements	
Processor: 2.0 GHz and 4 cores or faster	

Operating System	IIS VERSION
Memory: 8 GB or more** Hard-Disk Space: 1 GB or more *For up to 100 concurrent users. Increased specs required for 100+ concurrent users.	


*Requires an update to Windows Management Framework to version 3.

**= varies per EMS Software Application

EMS Web App Requirements

Desktop Browser
Introduction to EMS for Outlook (please see Note below)
Microsoft Edge (latest)
Microsoft Internet Explorer (IE11)
Firefox (latest)
Chrome (latest)
Safari (Mac) (latest)

*= varies per application.

 **Note:** EMS Web App V44.1 has been optimized for Internet Explorer 11 and does not require compatibility with previous versions of Internet Explorer. EMS recommends *disabling compatibility mode* when using EMS Web App V44.1.

EMS Web App V44.1 no longer supports Internet Explorer 10 or older.

EMS Web App (Mobile)

Mobile Browser	Platform
Internet Explorer for Mobile 8.1	Windows

Mobile Browser	Platform
Internet Explorer for Mobile 10	Windows
Chrome	Android 4.4, 6.0, 7.0, 7.1 iOS 9.x, iOS 10.x
Safari	iOS 9.x, iOS 10.x



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

Operating System	IIS
Windows Server 2012	8
Windows Server 2012 R2	8.5
.NET Framework	4.6.1
Application Pool	4.0

Prerequisites (Prior to Update 28)

HTTPPlatformHandler IIS Module	Download Version 1.2 here OR download the installer here .
PowerShell	5+ Version
ASP.NET Version 4.6	Under Web Server (IIS) > Web Server > Application Development: <ul style="list-style-type: none"> • ISAPI Extensions • ISAPI Filters • .NET Extensibility 4.6

Prerequisites (Update 28 and Later)

ASP.NET Core	See Also: Installing ASP.NET Core .
------------------------------	---

Operating System	IIS
PowerShell	5+ Version
ASP.NET Version 4.6	Under Web Server (IIS) > Web Server > Application Development: <ul style="list-style-type: none"> • ISAPI Extensions • ISAPI Filters • .NET Extensibility 4.6

EMS for Microsoft Outlook Requirements

Microsoft® Office	365
Outlook (32- and 64-bit)	2010, 2013, 2016
.NET Framework	4.6.1
Microsoft® Visual Studio 2010 Tools for Office Runtime	VSTO 2010
Prerequisites	
EMS Web App	Latest
On User Workstations	Desktop requirements for Microsoft® Outlook Windows 7, 8, or 10

Integration to Microsoft Exchange

Microsoft® Exchange	2010 SP3, 2013, 2016
Microsoft® Office	365
See Also: Exchange Web Services (EWS) Impersonation and Configure EWS Impersonation	

CHAPTER 18: 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 19: 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](#)
 - [Configure Multiple Mail Domains](#)
- [Test Your Exchange Integration](#)
- [Optional Messaging Settings](#)
 - [Enable Larger File Attachments on the Config File](#)
 - [Enable Larger File Attachments in the Exchange Integration Web Service](#)

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.
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).



Note:

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.

Account Info **Message** Exchange 2000/2003

Message To Append:
 *****GENERATED BY EMS WEB APPLICATION*****

To view the details of this reservation click the below link:
 To view the details of this reservation, click the below link:

If you are the meeting organizer click the below link to edit the reservation:
 If you are the meeting organizer, click the link below to edit your reservation:

Allow Attachments
 Maximum AttachmentSize (KB):
 8192 *Domino versions prior to 7.0.1 have a maximum post limit of 64kb*

Save

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 edit the reservation	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.
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="2147483644"
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**.

**Important!****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 20: 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.




```

File Edit Format View Help
web - Notepad
<?xml version="1.0"?>
<configuration>
  <configSections>
    <section name="dataConfiguration" type="Dea.Data.Configuration.DatabaseSettings, Dea.Data"/>
    <sectionGroup name="system.web">
      <section name="planMeetingService" type="Dea.Providers.PlanMeeting.PlanMeetingSection, Dea.Prc
    </sectionGroup>
  </configSections>
  <appSettings>
    <add key="QueryStringKey" value="KLKJHF3565DF90G3210ILHINER630"/>
    <add key="ignoreCertValidation" value="false" />
    <add key="enableTrace" value="false" />
    <add key="useAutodiscoverFallbackUrl" value="false"/>
    <add key="LogTimings" value="false" />
    <add key="EnableScplookups" value="true" />
    <add key="DurationToCacheAutodiscoverUrlInMinutes" value="1440"/>
    <!--<add key="mailDomains" value="Default" />-->
    <!-- Milliseconds
    <add key="autodiscoverTimeout" value="100000" />
    -->
    <!--
    These keys provide a way to further secure the PAM Web Service. If running the PAM Web Service under windows auther
    these keys allows us to compare the callers group membership to ensure that they have access to perform the call.
    Either supply ALL keys or none of the keys, only supplying a couple will disable the products that you do not supp
    If all left blank, then all callers are allowed.
    emsApiSecurityGroup: Windows Group For the EMS API (configured identity of EMS API AppPool)
    Calls:
  
```

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.

The screenshot shows a configuration window for Exchange 2007/2010. It includes sections for 'Test Configuration', 'Provider', and 'Authentication Information'. The 'Provider' section has dropdown menus for 'Exchange Web Services' and 'Mail Domain', and a text field for 'URI to Exchange Web Services'. The 'Authentication Information' section has checkboxes for 'Use application pool identity' and 'For Exchange Web Services, should impersonation be used', along with 'Username' and 'Password' fields.

5. [Test your Exchange Integration.](#)

 **Note:**
These settings are stored in the tblPamSettings table.

CHAPTER 21: Use Application Pool Identity for Integration for Exchange Service Account

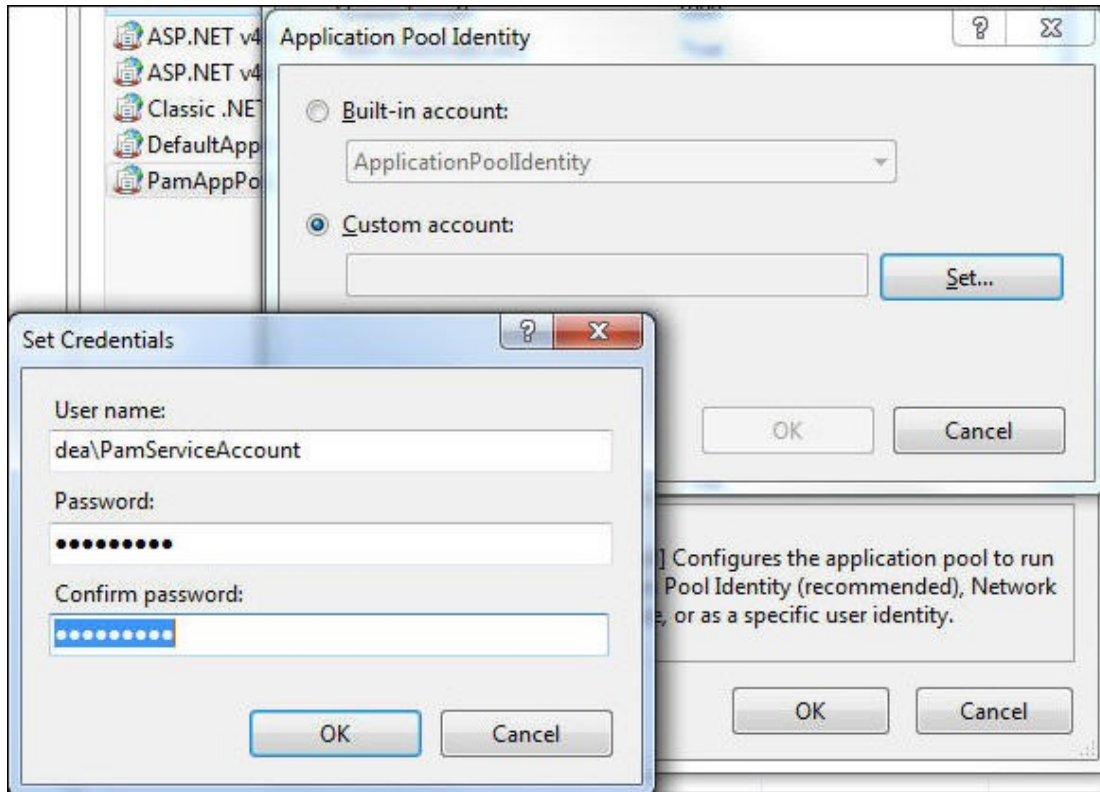
Rather than entering the Integration for Exchange account credentials on the PAMConfig.aspx page (as in V44 and previous releases), credentials can be maintained at the Application Pool level. This allows your organization to maintain absolute control—**only** IIS applications running in the newly created 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 mailbox 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 configure.
7. Choose **Custom Account** and then click **Set**. Enter the username and password for your EMS Integration to Exchange account. Confirm the password and click **OK** on any remaining dialogs (see following 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](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.

The screenshot shows a configuration page for Exchange 2000/2003. At the top, there are tabs for 'Account Info', 'Message', and 'Exchange 2000/2003'. Below the tabs is a 'Test Email' field and a 'Test Configuration' button. The main section is titled 'Provider' and contains the following elements:

- Provider:** Choose Exchange Web Services for Exchange 2007 (SP1 or later), Exchange 2010 and for all coexistence (Exchange 2003 w/Exchange 2007 or Exchange 2003 /w Exchange 2010 or Exchange 2007 /w Exchange 2010) scenarios.
- Provider:** Exchange Web Services (dropdown menu)
- Check this box if your Exchange environment has mailboxes on 2000/2003 servers and 2007/2010 servers. If you are in Mixed Mode, AutoDiscover MUST be utilized
- Check this box to utilize AutoDiscover to locate the best Client Access Server for the uses. If you are in Mixed Mode, AutoDiscover MUST be utilized
- Url to Exchange Web Services:** https:// [text input] Supply this value only if you cannot use AutoDiscover for some reason. NOTE: It is considered a best practice to use AutoDiscover when accessing the Exchange Web Services.
- Follow AutoDiscover redirects to these Urls (pipe (|) delimited):** [text input]
- Authentication Information**
- Use application pool identity when authenticating to calendaring service (only applicable for Exchange 2007/2010 environments, all other situations REQUIRE username and password below)
- Username:** exchangeaccount [text input] This is the account which will make the requests
- Password:** [text input] Provide only if updating
- For Exchange Web Services, should impersonation be used when accessing the mailboxes. If not, then FULL ACCESS or DELEGATE (at least Editor) access must be granted to the account for ALL mailboxes.

CHAPTER 22: 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.

**Note:**

For more information on EWS Impersonation, see [What is EWS Impersonation?](#)

CHAPTER 23: 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, "EMSEExchangeAccount", 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 EMSEExchangeAccount 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 24: EMS for Microsoft® Outlook Add-In 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.



Important!

To upgrade to Update 17 of EMS for Outlook, you will need to uninstall your legacy version and re-install.

The following topics are covered in the Microsoft® Outlook Add-In configuration guide:

- [Integrated Authentication Options for EMS for Outlook Add-In](#)
 - [Integrated Authentication Considerations](#)
 - [Manage Everyday Users For Integrated Authentication](#)
 - [LDAP Authentication](#)
 - [Portal or Federated Authentication](#)
 - [Portal Authentication Methods](#)
- [Configure EMS for Outlook](#)
 - [Customize the Add-In Label](#)
 - [Customize the Add-in Logo](#)
 - [EMS for Outlook System Parameters](#)
 - [Enable User Access to EMS for Outlook](#)
 - [Assign EMS Users to Groups](#)
 - [Establish Booking Templates for EMS for Outlook Users](#)

See Also: [Configure Outlook TBD Rooms](#)

Contact Customer Support

- **Option 1 (Recommended):** Search the Knowledge Base available at [Accruent Access](#).
- **Option 2:** Submit a case directly via [Accruent Access](#).

- **Option 3:** Email emssupport@accruent.com.
- **Option 4:** Phone (800) 288-4565.



Important!

If you do not have a customer login, register [here](#).

CHAPTER 25: Configure EMS for Outlook

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.

Additional configuration tasks are required in order to enable your Microsoft Outlook users to access EMS for Outlook functionality. See Also: [Configure Outlook TBD Rooms](#).

The topic provides information about the following:

- [Customize the Add-In Label](#)
- [Customize the Add-In Icon](#)
- [EMS for Outlook System Parameters](#)
- [Enable User Access to EMS for Outlook](#)
- [Assign EMS Users to Groups](#)
- [Establish Booking Templates for EMS for Outlook Users](#)

Customize the Add-In Label

1. Log into EMS Desktop Client.
2. Navigate to **System Administration > Settings > Parameters** and select the **Desktop Client** tab.
3. In the Area drop-down, select **EMS for Outlook - Specific**.
4. Select **EMS Room Scheduling** in EMS for Outlook and click **Edit**.
5. Make your changes and click **OK**.
6. Click **Close**.

**Note:**

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.

Customize the Add-in icon


You can replace the default EMS for Outlook icon that displays in Outlook with a custom icon of your choosing.

1. Log into EMS Desktop Client.
2. Navigate to **System Administration > Settings > Parameters** and select the **Desktop Client** tab.



Note:
Make sure to select the **Desktop Client** tab instead of the **Everyday User Applications** tab.

3. In the Area drop-down field of the Parameters dialog, select **System**.
4. Select **Custom Calendar Icon** and click **Edit**.
5. Make your changes and click **OK**.
6. Click **Close**. Microsoft Outlook will need to be restarted to see the custom icon change.



Important!
Supported file types are .ico, .jpeg, .jpg, or .png. The recommended size is 32 x 32 pixels.

EMS for Outlook System Parameters

In addition to changing the Add-in label and custom icon, you can use the following parameters to make additional changes. See Also: [EMS for Outlook Parameters](#).

Parameter	Value	Description
Display filters before showing rooms	Yes/No	For large organizations using templates in Outlook that have a large amount of locations, setting this to Yes can provide better performance and user experience.
Number of available rooms upon search in Outlook	Numeric (<500)	Controls the maximum number of results when searching for a room. For optimal performance, set to 50 or less.
Show attendees in book	Yes/No	Allows users to see attendee and room availability on the Schedule View. Best practice includes setting this to Yes.
Text to display under icon in EMS for Outlook	Text	Customize the add-in label.

Parameter	Value	Description
Text to append to EMS for Outlook meetings	Text	Adds text to Outlook meetings when the meetings are created using the EMS for Outlook add-in. Can be plain text with a 50 character limit; HTML is not supported. The text you enter will be added to the meeting body.

Enable User Access to EMS for Outlook

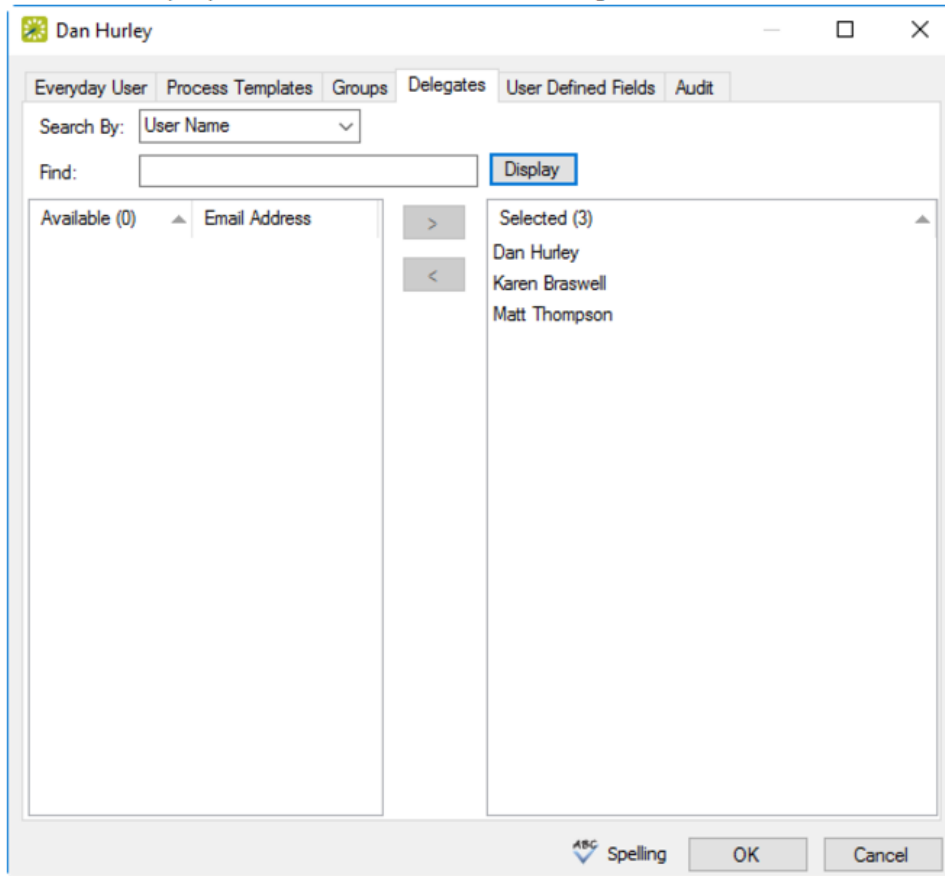


Important!

This topic assumes you have a working knowledge of configuration in EMS Desktop Client and highlights special tasks for enabling EMS for Outlook users. For more detailed instructions in creating new users, See Also: [Configure Everyday Users](#).

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

1. Configure an active EMS Everyday User Account in the EMS Desktop Client.
2. Link the EMS Everyday User Account to an active EMS Group record.
3. (Optional) The **Delegates** tab allows you to associate a delegate to an EMS Everyday User. To assign a delegate in EMS for Outlook, that delegate must also be assigned in Exchange.



Delegates Tab

4. Assign at least one Everyday User Process Template to the EMS Everyday User Account.
5. Enable the **Outlook** option for the Everyday User Process Template you associated with the user.



Note:

When Outlook is enabled, Integration to Microsoft Exchange is automatically enabled.

Process Template Tab

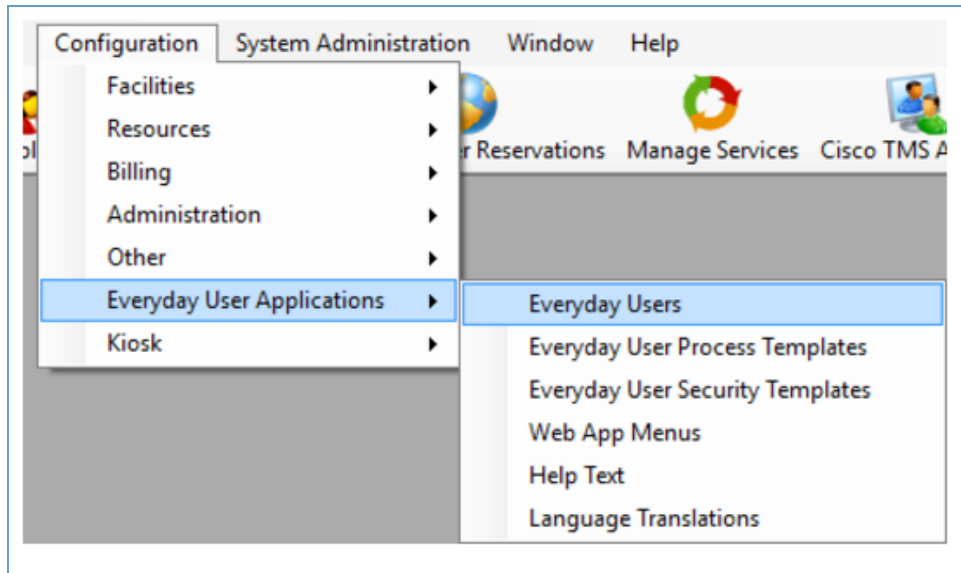
Assign EMS Users to Groups

You assign users to see groups in EMS by modifying the group or the Everyday User accounts.

1. Navigate to **Reservations > Reservations > Groups**. (The **Groups** label can be modified by your system administrator.)
2. Select a **Group**.
3. Click the **Everyday User** tab.
4. Click **Edit**. In the dialog box, search for everyday user accounts to add/remove from a Group record.

The following alternate path is available to assign users to groups:

1. Navigate to the Everyday User's account on the **Everyday User** tab within **Configuration > Everyday User Applications > Everyday Users**.



Navigating to the Everyday User Tab

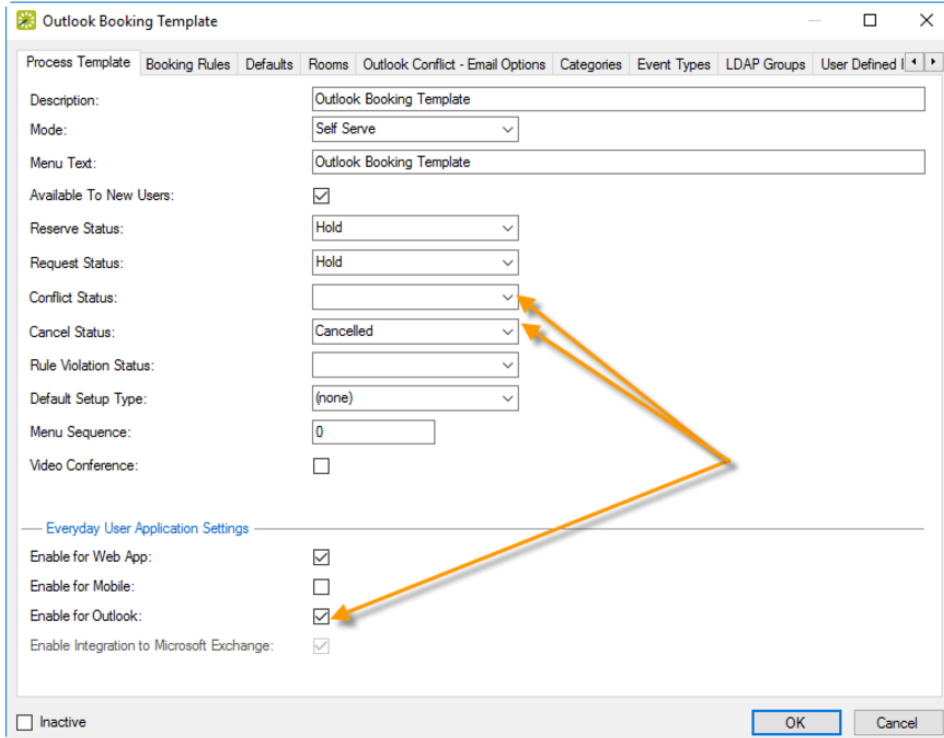
2. Open the Everyday User's account by clicking the **Edit** button.
3. On the **Groups** tab, search for a Group to add/remove from an everyday user account.

Establish Booking Templates for EMS for Outlook Users

When [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, do the following to establish booking templates for EMS for Outlook users:

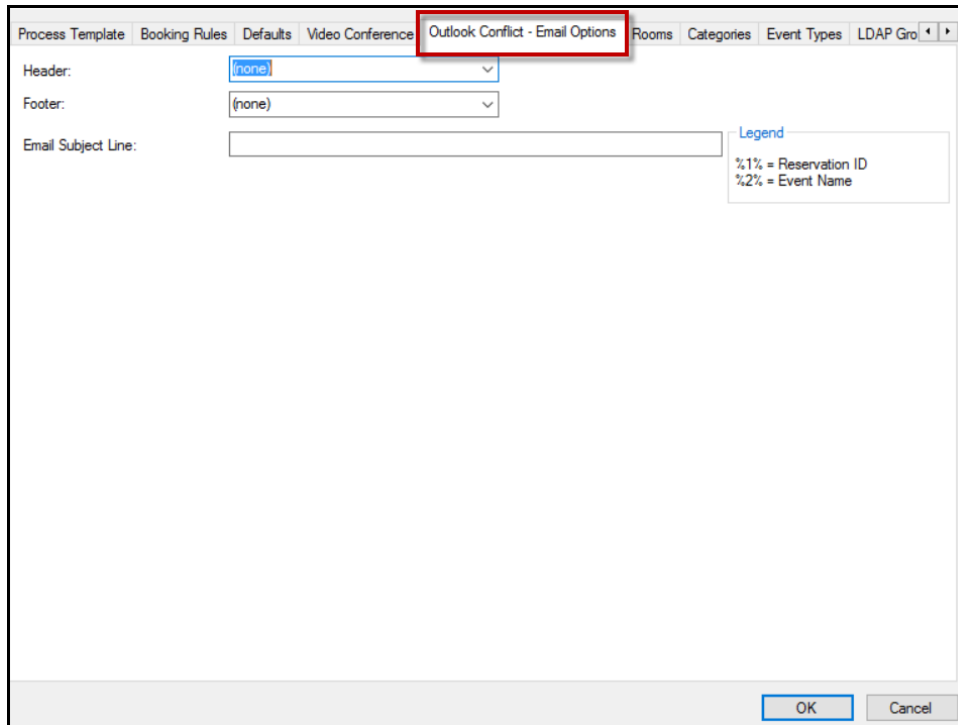
1. Click **Edit** on the Everyday User Process Template to fully enable and customize the EMS for Outlook Add-in.
2. Select the **Enable for Outlook** checkbox to enable the template to display to associated everyday users in the EMS for Outlook Add-in.
3. Select a status from the Conflict Status drop-down list to determine the *type of conflict* status assigned to bookings made using this template that are in conflict.
4. Select a status from the Rule Violation Status drop-down list to determine the *status of bookings* that have violated the template booking rules or category rules. This option is only available when **Enable for Outlook** is selected. When a user in EMS for Outlook requests 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 two years in advance when the process template only allows a booking a year in advance, then the booking is set to the status you specify in this field (such as Rule Violation).

Note:
The values in this drop-down list come from settings in the booking [Statuses](#) area of EMS Desktop Client.



New Booking Template Created for EMS for Outlook

5. Navigate to the **Outlook Conflict – Email Options** tab to control behavior for the see notification email sent to the Outlook user if a booking conflict arises during the process of booking through Outlook.



Outlook Conflict Email Options Tab

CHAPTER 26: EMS for Microsoft® Outlook Add-In User Guide (V8)

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).



Important!

EMS for Outlook is currently only available for Windows Outlook. It is not compatible with Outlook Online or for Mac.



Note:

EMS for Outlook checks for connection to EMS upon initialization. If you are offline or off-network (VPN) when opening Outlook, you might see the icon indicate 'offline' within Outlook. If this happens, establish connectivity to the appropriate network and restart Outlook to establish the connection to EMS.

This guide includes information about the following topics:

- [Microsoft Outlook, EMS for Outlook, and VEMS Comparison](#)
- [Create Reservations](#)
 - [Single Reservation](#)
 - [Series Reservation](#)
 - [Add Services to a Booking](#)
 - [Video Conference Reservation](#)
 - [Edit or Cancel a Reservation](#)
- [Using Skype for Business in EMS for Outlook](#)
- [Resolve a Booking Conflict](#)
- [View Known Errors/Alerts](#)

See Also: [EMS for Outlook Video Tutorials](#)

Contact Customer Support

- **Option 1 (Recommended):** Search the Knowledge Base available at [Accruent Access](#).
- **Option 2:** Submit a case directly via [Accruent Access](#).
- **Option 3:** Email emssupport@accruent.com.
- **Option 4:** Phone (800) 288-4565.



Important!

If you do not have a customer login, register [here](#).

CHAPTER 27: 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, managed spaces, 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 28: Create a Reservation in EMS for Microsoft Outlook

You can use the functions in the EMS for Microsoft Outlook add-in 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:

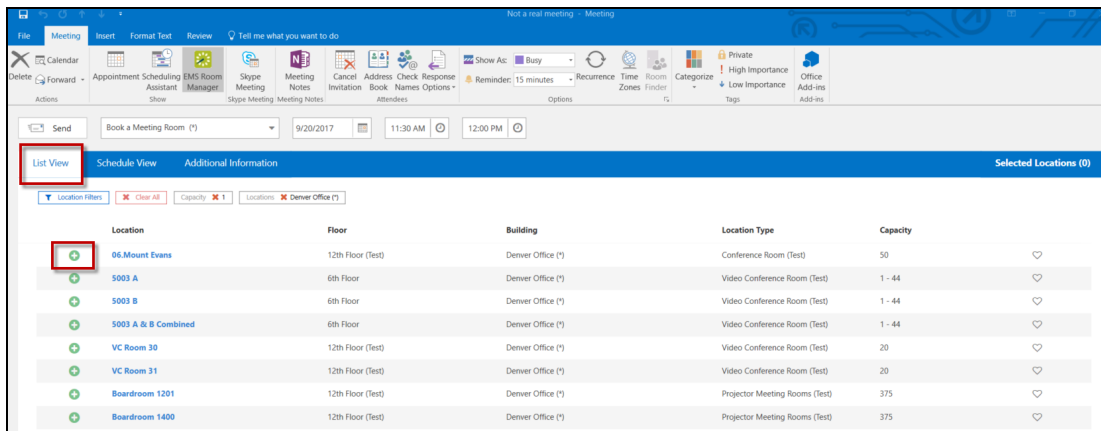
- [Create a Single Reservation](#)
- [Create a Series Reservation](#)
- [Create a Video Conference Reservation](#)
- [Edit or Cancel a Reservation](#)

CHAPTER 29: 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.

Note: 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](#).

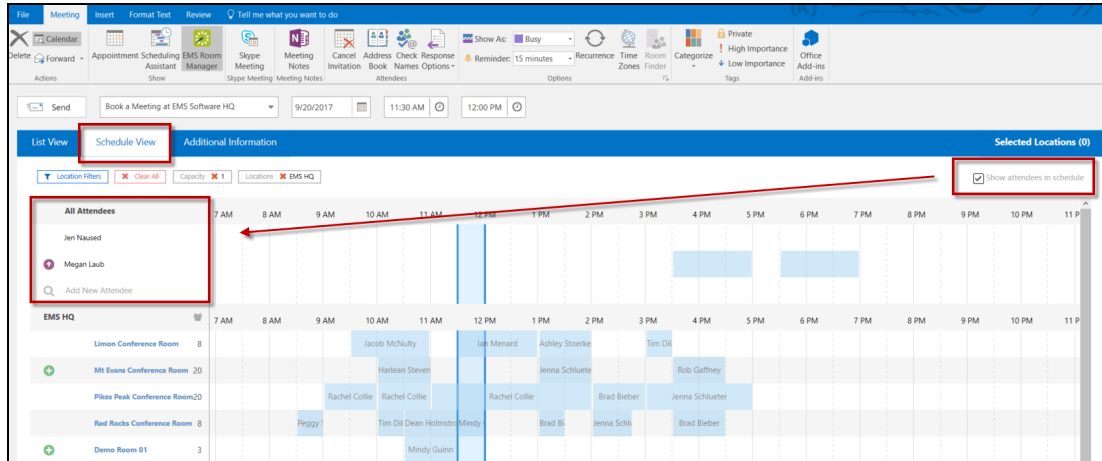
1. Open Microsoft Outlook and create a standard meeting that includes an event subject, attendees, and the date and time for the event.
2. Click the **EMS Room Manager** icon in the top menu bar of Outlook.
3. Select a template from the drop-down list (the list contains pre-defined templates set by your 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

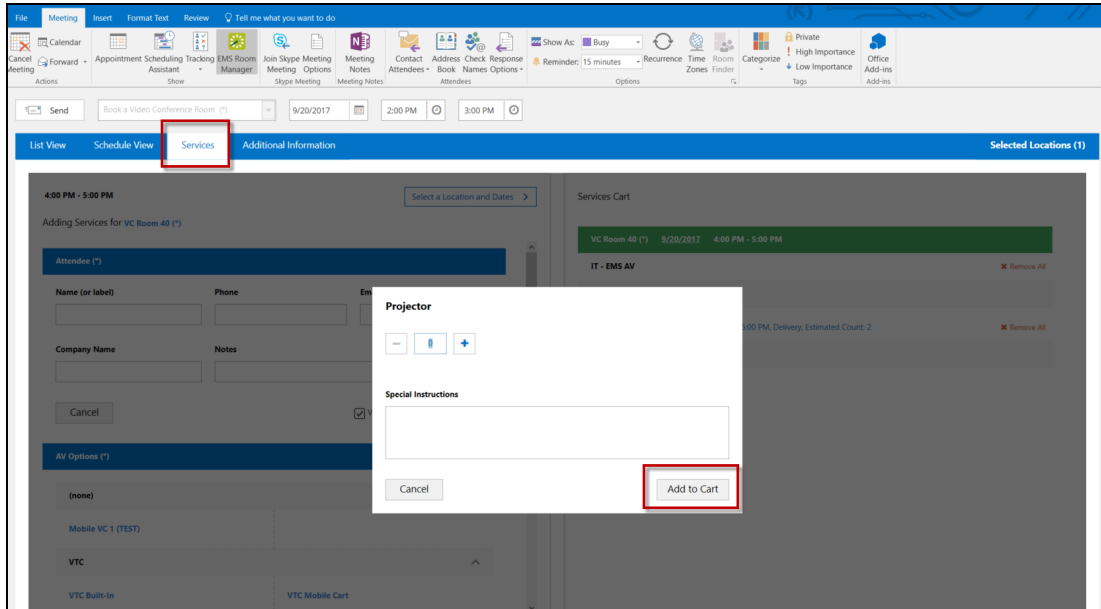
Note: You can make a room your Favorite by clicking on the heart in the right-hand column. This Favorite will transfer to all EMS access points (e.g., EMS Web App, EMS Mobile App, etc.).

- 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.
- 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

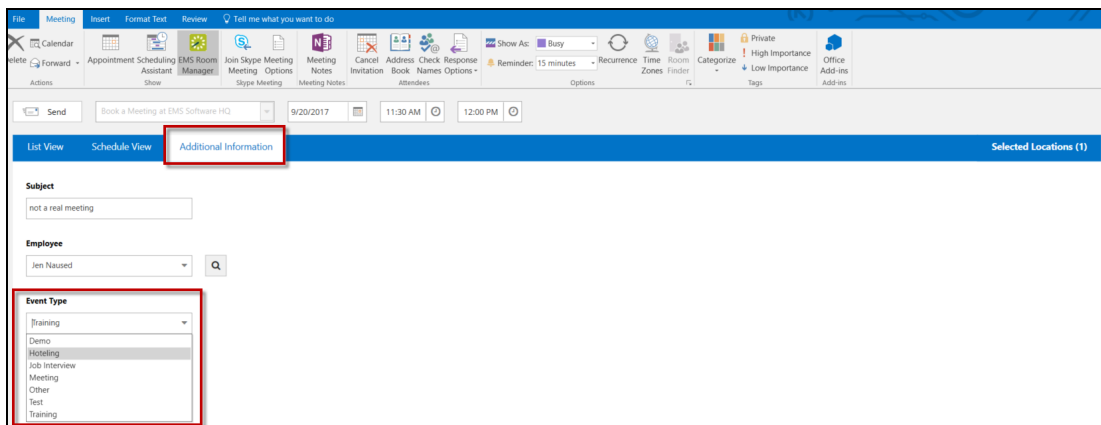
- Optionally, you might be able to request services for the event and/or provide setup notes for the event. The **Services** tab might be available for requesting one or more services for the event, such as Catering, A/V Equipment, etc. Click on the service you want to add and provide additional information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



Adding Services from the Services Tab

Note: From the **Services** 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 list.



Additional Information Tab

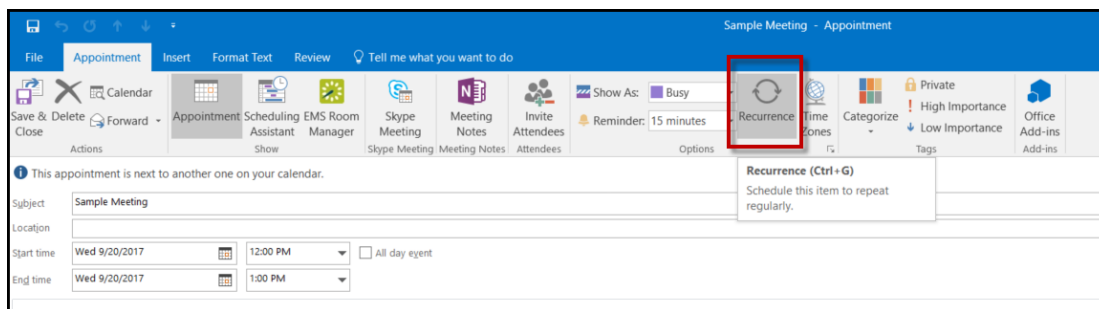
12. From the **Selected Locations** tab, you can view information about the selected room, including the Floor, the Building in which it is located, its Location Type, Capacity, and the Attendee Count for your event. If needed, you can click the red remove icon to remove the room for the scheduled event 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 30: 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](#).

To create a series 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.



Note:

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.

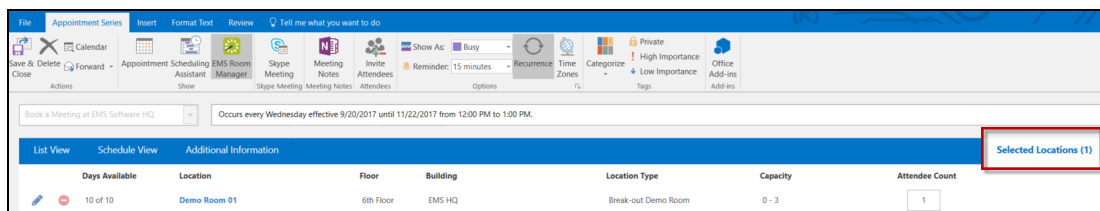
7. If the room you selected is not available for all days (e.g., only 8/10 days), the Resolve Conflicts dialog box will appear. (For example, for a recurrent meeting with 10 meeting dates, Demo Room 06 is available for 8 out of the 10 meeting dates.)
8. Choose a location that is available for the remaining dates during your recurrence and click the green **Select (+)** button.

Important!

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.

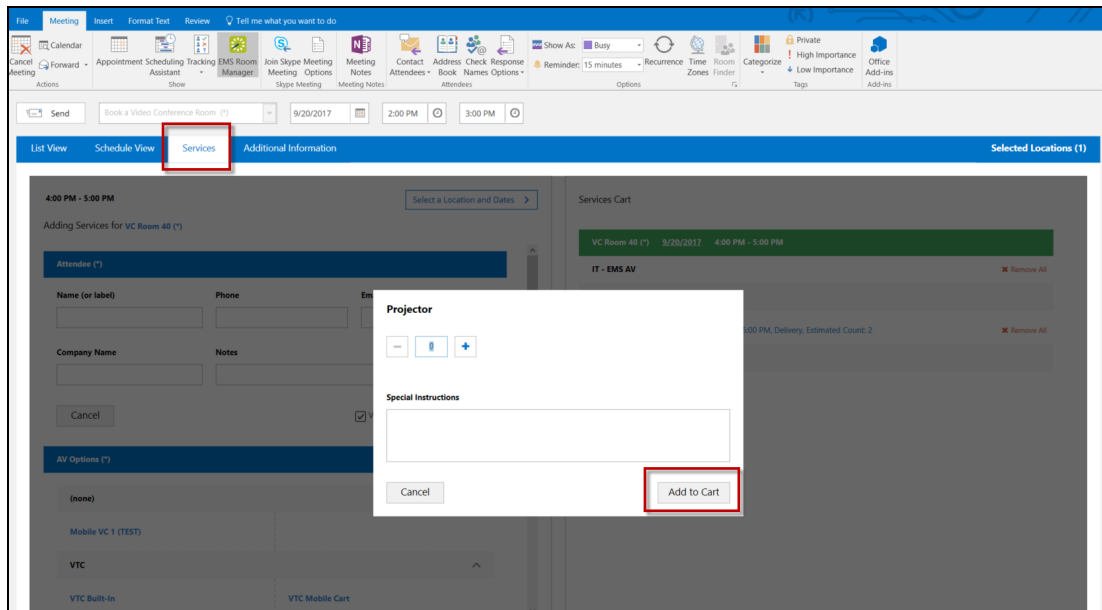
9. Optionally, click on the **Selected Locations** tab to view information about the selected room(s), such as Days Available, Location, Floor, Building, Location Type, Capacity, and Attendee Count. If needed, you can click the red Remove button to remove the room for the scheduled event or the Edit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

Selected Location Tab



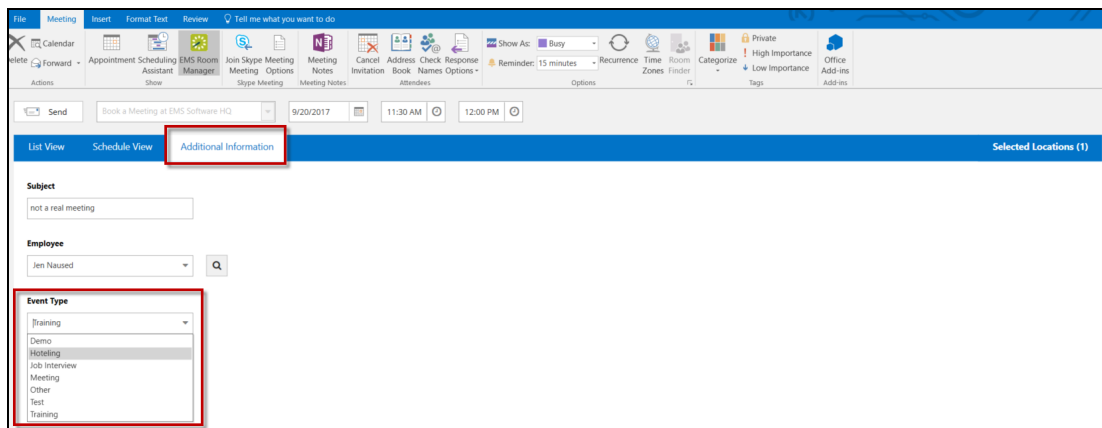
10. Optionally, you might be able to request services for the event, supply billing information for the event, and/or answer additional questions about the event. The **Services** tab might be available for requesting one or more services for the event, such as Catering, A/V Equipment, etc.
11. If your 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**.



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.



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 31: 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.

To create a video conference reservation, follow these steps:

1. Follow the appropriate steps for creating either a [single](#) or [series](#) reservation.



Note:

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

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.

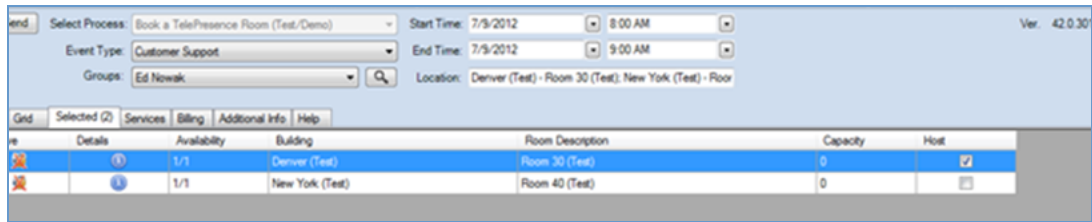
3. After you successfully book a video conference reservation, the host room is indicated on the **Selected** tab.

Room 1201 successfully booked with a mobile video conference cart.

Room 30 has built-in video conferencing features and is available for booking.

Room 1202 cannot be booked as no mobile video conferencing carts are available.

Video Conference Room Availability Indicators



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

CHAPTER 32: Edit or Cancel a Reservation

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, follow these steps:

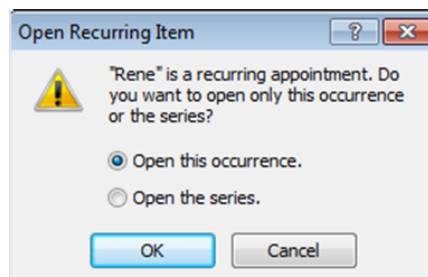
1. Open your Outlook calendar.
2. In the calendar, double-click on an event date.
 - If the reservation is a single reservation, then the meeting information opens in the standard Outlook meeting format.
3. If needed, edit the **Start Time** and/or **End Time**, and then click **EMS Room Manager**.
4. 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.



Note:

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 you 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 33: Skype for Business in EMS for Outlook

Everyday Users can now integrate audio/video conferencing tools with EMS applications, starting with Skype for Business. 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**. For more information, see [Configure Skype for Business](#).



Important!

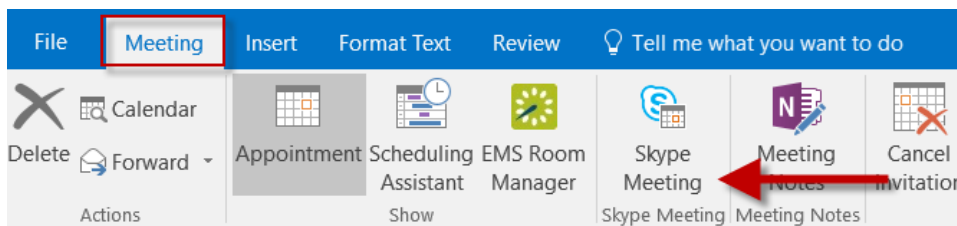
When considering using the Skype for Business Integration, keep in mind the following:

- Skype for Business is **ONLY** available on **Exchange-enabled templates**.
- Skype for Business meetings cannot be removed from Outlook appointments, including those tied to reservations using EMS for Outlook.

For more information about Configuring Skype for Business, see [Configure Skype for Business](#).

Add Skype for Business to Your Reservation

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 your reservation](#).
4. Under the **Meeting** tab, click the **Skype Meeting** button. 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 your Skype account is authenticated, you can continue creating your reservation.
- If your Skype account is not authenticated, an authentication modal will appear.
- If you fail to authenticate your Skype account, the Skype toggle will be disabled.

**Note:**

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.

For more information regarding authentications in Skype for Business, see [Skype for Business Deployment Types](#).

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 using Skype for Business in other EMS access points, refer to:

- [Skype for Business in EMS Mobile App](#)
- [Skype for Business in EMS Web App](#)

For more information regarding features of Skype for Business, refer to the [Microsoft Skype for Business User Guide](#).

CHAPTER 34: Resolve Booking Conflicts

This topic provides information on the following:

- [Resolve Booking Conflicts for a Series Reservation](#)
- [Resolve Booking Conflicts When You Receive a Warning Email](#)

Resolve Booking Conflicts for a Series Reservation

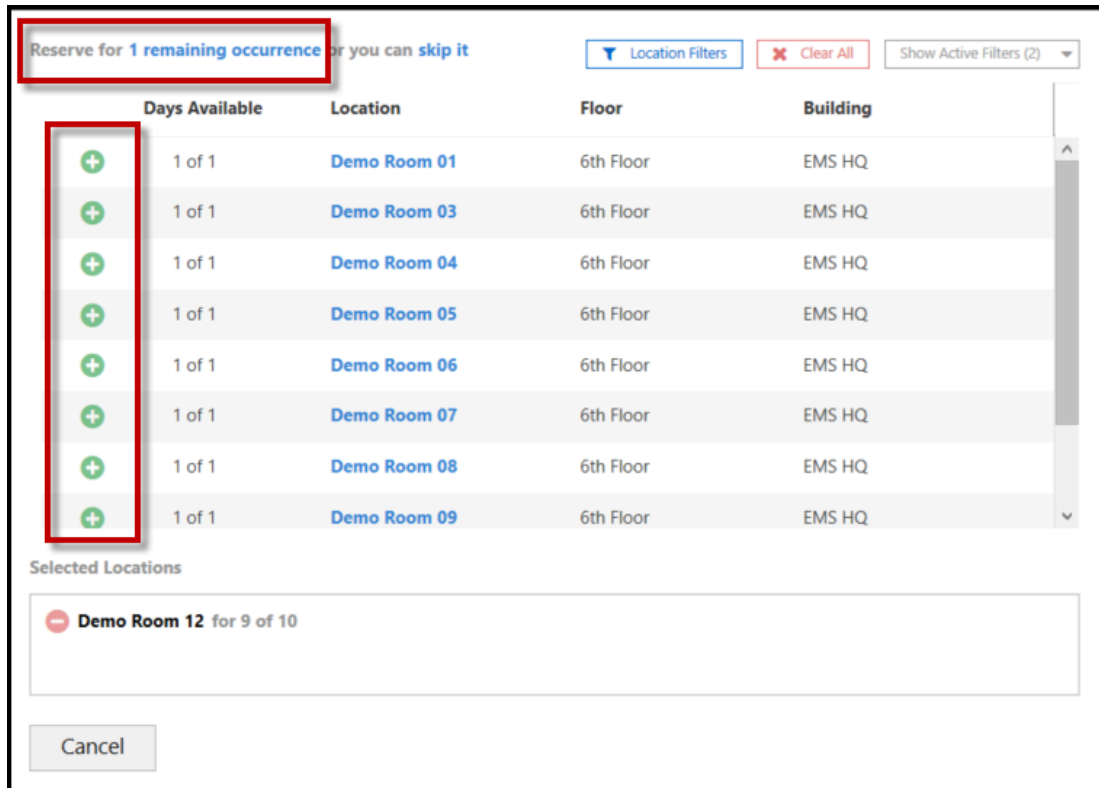
When booking a recurring meeting, you might encounter a booking conflict. To resolve this conflict:

1. Create your [recurring 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	Location	Floor	Building	Location Type	Capacity
10 of 10	Demo Room 01	6th Floor	EMS HQ	Break-out Demo Room	3
10 of 10	Demo Room 04	6th Floor	EMS HQ	Break-out Demo Room	3
10 of 10	Demo Room 05	6th Floor	EMS HQ	Break-out Demo Room	3
10 of 10	Demo Room 06	6th Floor	EMS HQ	Break-out Demo Room	3
10 of 10	Demo Room 07	6th Floor	EMS HQ	Break-out Demo Room	3
10 of 10	Demo Room 11	6th Floor	EMS HQ	Break-out Demo Room	3
9 of 10	Demo Room 08	6th Floor	EMS HQ	Break-out Demo Room	3
9 of 10	Demo Room 09	6th Floor	EMS HQ	Break-out Demo Room	3
9 of 10	Demo Room 10	6th Floor	EMS HQ	Break-out Demo Room	3
9 of 10	Demo Room 12	6th Floor	EMS HQ	Break-out Demo Room	3
8 of 10	Demo Room 03	6th Floor	EMS HQ	Break-out Demo Room	1 - 10

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

Note: 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 define an "Outlook TBD" room for each building in your database. This will ensure skipped bookings remain in the correct timezone and will allow for localized notifications and reports to be created around meetings without locations.

See Also: [Configure Outlook TBD Rooms.](#)

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

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 35: View Known Errors/Alerts for EMS for Outlook

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	
Rooms cannot be booked in the past.	Displayed if a user opens a meeting that has occurred in the past.
You must be the organizer of the meeting to make changes.	Displayed when a user attempts to open a meeting for which they are not the web user.
Bookings cannot be longer than 24 hours.	Displayed if a user sets a start/end date/time combination to anything greater than 24 hours.
Resource quantities have been reset.	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.
Updating the reservation system was unsuccessful.	Displayed when EMS encounters an unexpected error trying to save the reservation in EMS.
Bookings cannot be longer than {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.
The terms and conditions must be accepted prior to saving the reservation.	Displayed when a user attempts to add a booking that violates the Max Number of Bookings value as specified by the Web Process template.

Alert/Error Message	Description
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.)

EMS for Outlook - May 2019

Accruent, LLC

11500 Alterra Parkway

Suite 110

Austin, TX 78758

www.accruent.com