EMS FOR MICROSOFT OUTLOOK

Installation Guide

V44.1

Last Updated: March 5, 2018

EMS Software | emssoftware.com/help | 800.440.3994 | © 2018 EMS Software, LLC. All Rights Reserved.

Table of Contents

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.

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

CHAPTER 2: Introduction to EMS for Microsoft Outlook Add-in

EMS for Microsoft 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 Installation Guide provides information on installing EMS for Microsoft Outlook Add-in.

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

CHAPTER 3: Requirements and Prerequisites 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
- 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.

> **TIP:** 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

AREA	VERSION
Microsoft® Outlook (32- and 64-bit)	2010, 2013, 2016
.NET Framework	4.6.1
Microsoft® Visual Studio 2010 Tools for Office Runtime	VSTOR 2010
Microsoft® Exchange	2010 SP3, 2013, 2016
Microsoft® Office	365
Operating System	Windows 7, 8, or 10

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: » ISAPI Extensions » ISAPI Filters » .NET Extensibility 4.6

EMS PLATFORM SERVICES REQUIREMENTS

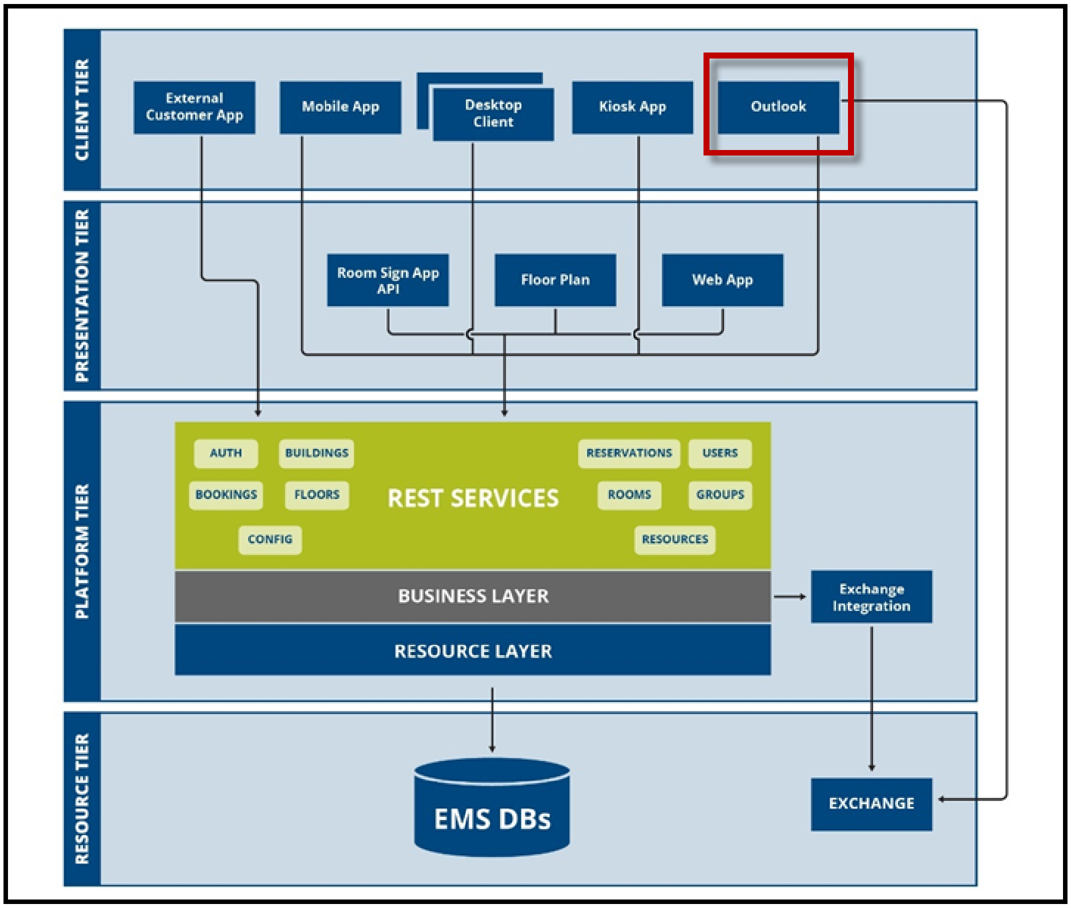
OPERATING SYSTEM	IIS
Windows Server 2008 R2	7/7.5
Windows Server 2012	8
Windows Server 2012 R2	8.5

.NET Framework	4.6.1
Application Pool	4.0

SYSTEM ARCHITECTURE

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 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 the EMS Customer Portal.
2. From the **Downloads** dropdown, click the **EMS Software** link.
3. From the **Software and Documents** library, click the **44.1 Releases & Patches** link.
4. 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.

> **TIP:** 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 the EMS Customer Portal.
2. From the **Downloads** dropdown, click the **EMS Software** link.
3. From the **Software and Documents** library, click the **44.1 Releases & Patches** link.

4. Download the **EMSPlatformServices.msi** file.
5. 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.

6. When all prompts have been completed, click **Install**. The API is installed on your web server.
7. 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]/EMSPlatform/** [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/** [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).
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.

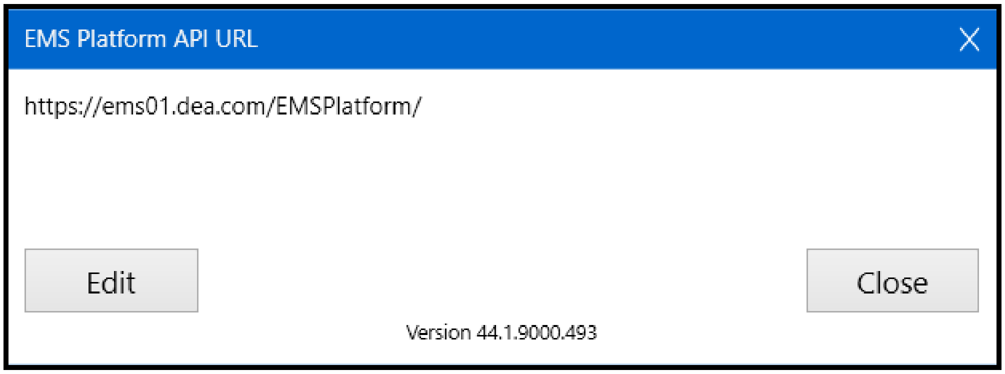
1. Verify that the Requirements and Prerequisites have been met.
2. Download the **EMSForOutlook.msi** file onto the user’s desktop.
3. Close Outlook.
4. Run **EMSForOutlook.msi**.
5. The first screen welcomes you to the EMS Outlook Add-in Setup Wizard.
6. Click the **Next** button to begin the installation 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).
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.

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 may 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.



EMS Platform API URL

https://ems01.dea.com/EMSPlatform/

Version 44.1.9000.493

> **NOTE:** Only your IT System Administrator should perform this step. See Also: Integration to Microsoft® Exchange.

2. Click the **Edit** button.

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.

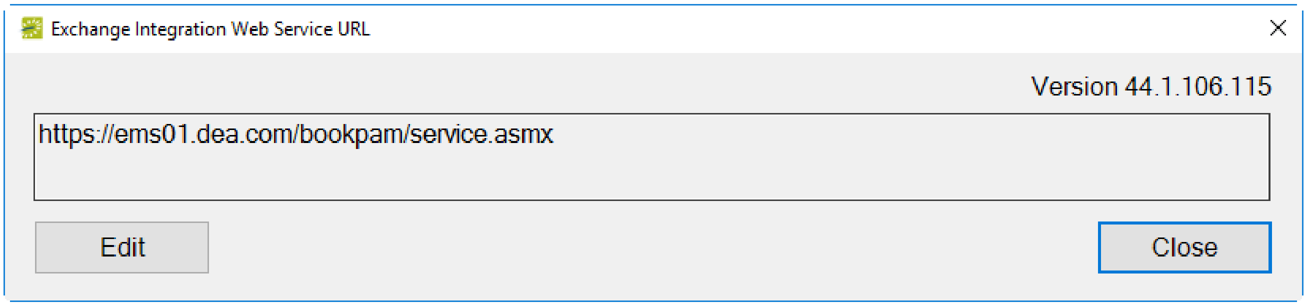
Use the following command to establish an Unattended/Silent installation of the **EMSForOutlook.msi** (replace <url> with your URL):

```
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.



Version 44.1.106.115

https://ems01.dea.com/bookpam/service.asmx

CHAPTER 9: Authentication Options

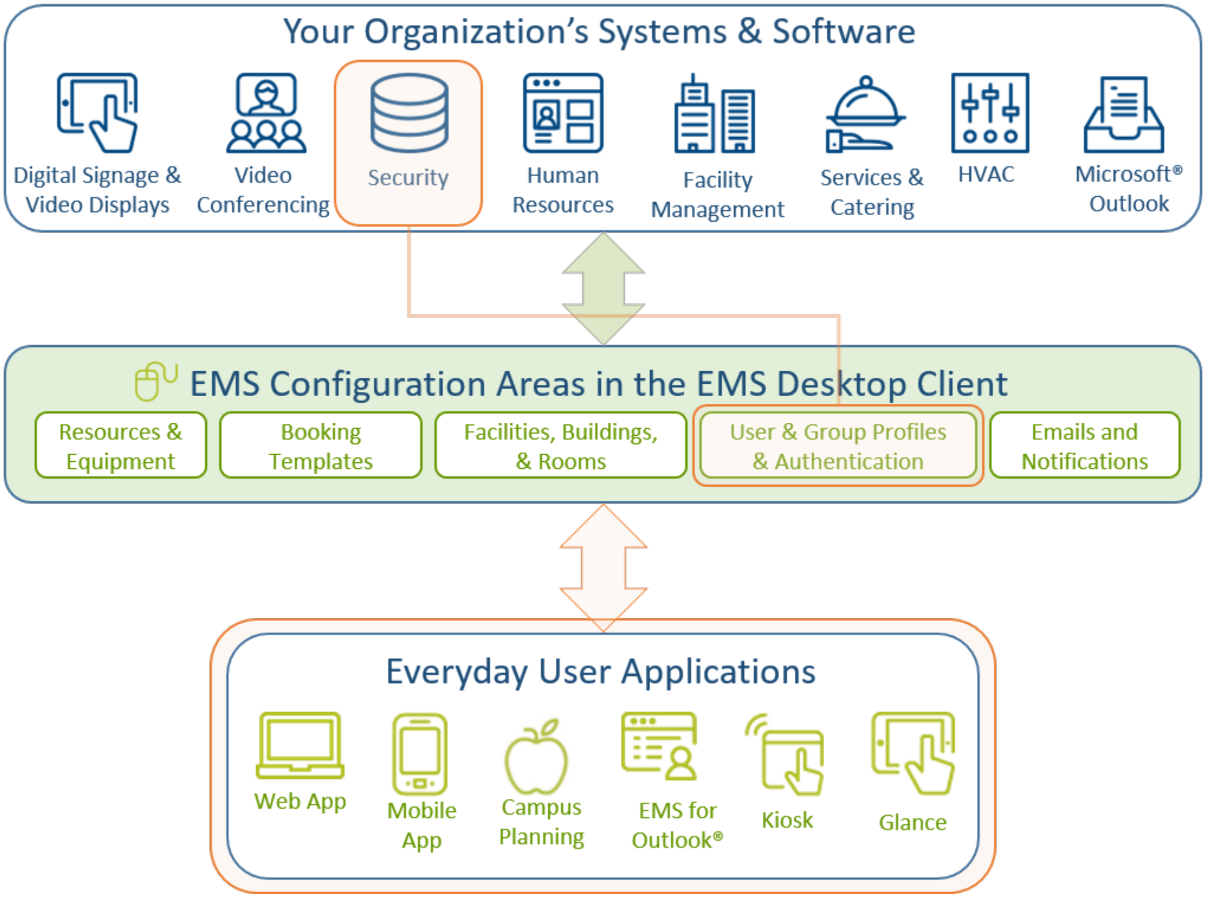
This guide provides configuration instructions for System Administration and IT users. This topic will provide the following information on Integrated Authentication:

CHAPTER 10: Introduction

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

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

Integration Diagram



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

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

WHAT IS INTEGRATED WINDOWS AUTHENTICATION?

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

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

WHAT IS PORTAL OR FEDERATED AUTHENTICATION?

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

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

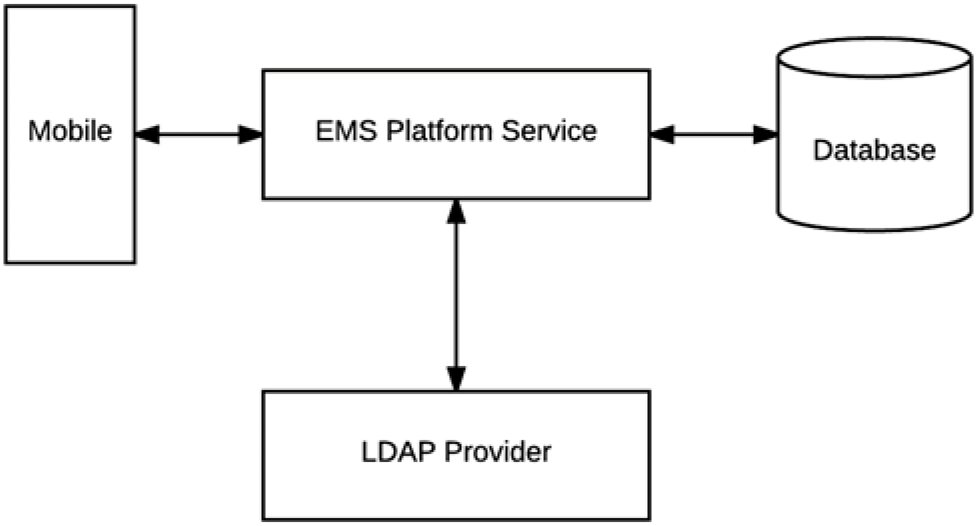
Several built-in authentication methods to pass-in credentials are available including:

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

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

WHAT IS LDAP AUTHENTICATION?

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



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

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

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

Notes:

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

CONTACT CUSTOMER SUPPORT

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

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

CHAPTER 11: 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 Setup 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 12: 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

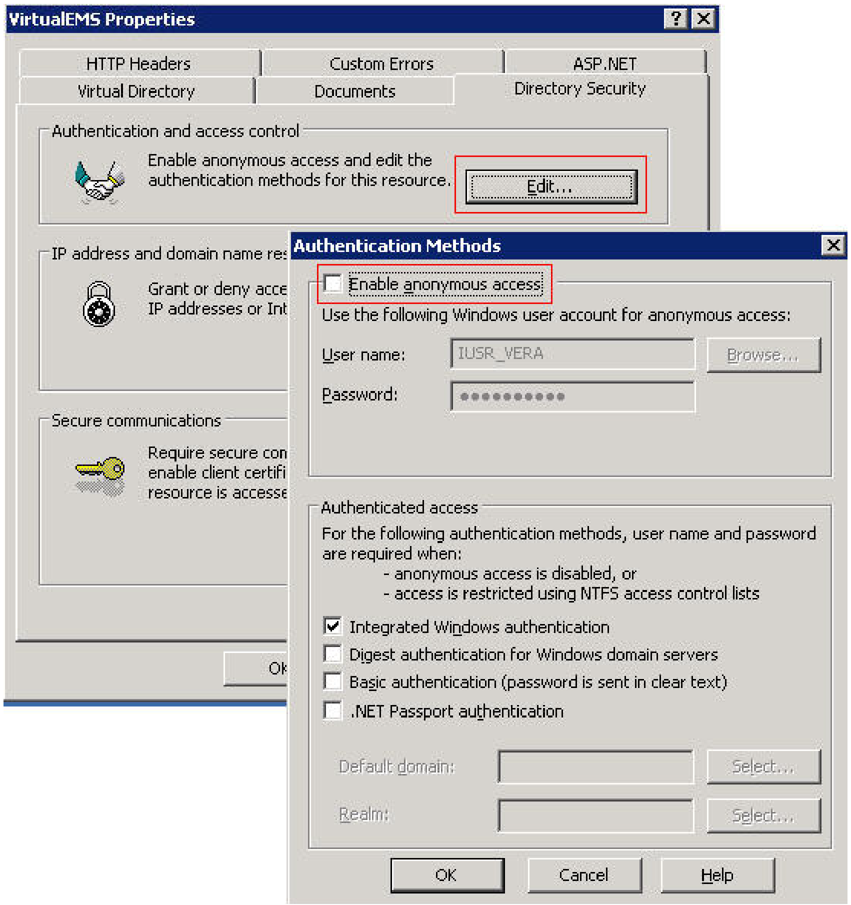
When a domain user who is logged on to a networked PC accesses an EMS Everyday User application, such as EMS Web App, EMS Mobile App, or EMS for Outlook, their Active Directory credentials (Domain\User ID) are compared against corresponding Domain\User ID information recorded in the **Network ID** and\or **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.



VirtualEMS Properties

HTTP Headers | Custom Errors | ASP.NET | Virtual Directory | Documents | Directory Security

Authentication and access control

Enable anonymous access and edit the authentication methods for this resource. [Edit...]

IP address and domain name res

Grant or deny acce IP addresses or Int

Secure communications

Require secure con enable client certifi resource is accesse

Authentication Methods

□ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: IUSR_VERA [Browse...]

Password: ••••••••••

Authenticated access

For the following authentication methods, user name and password are required when:

- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☑ Integrated Windows authentication

□ Digest authentication for Windows domain servers

□ Basic authentication (password is sent in clear text)

□ .NET Passport authentication

Default domain: [Select...]

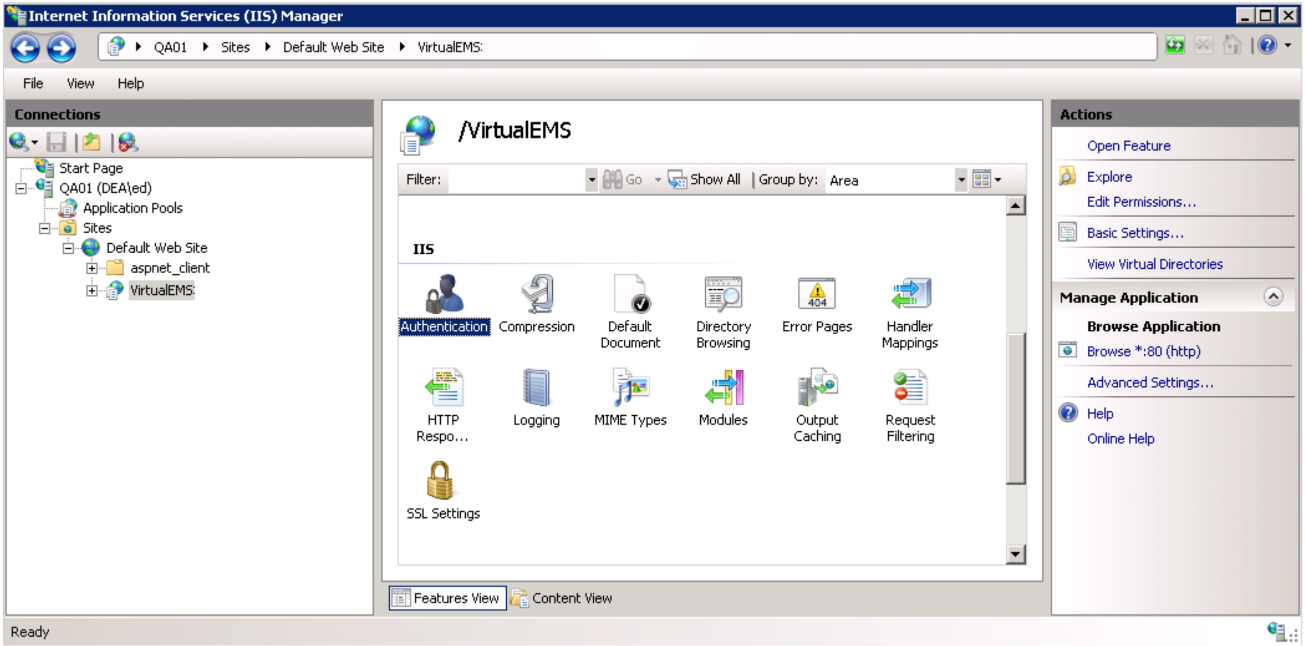
Realm: [Select...]

[OK] [Cancel] [Help]

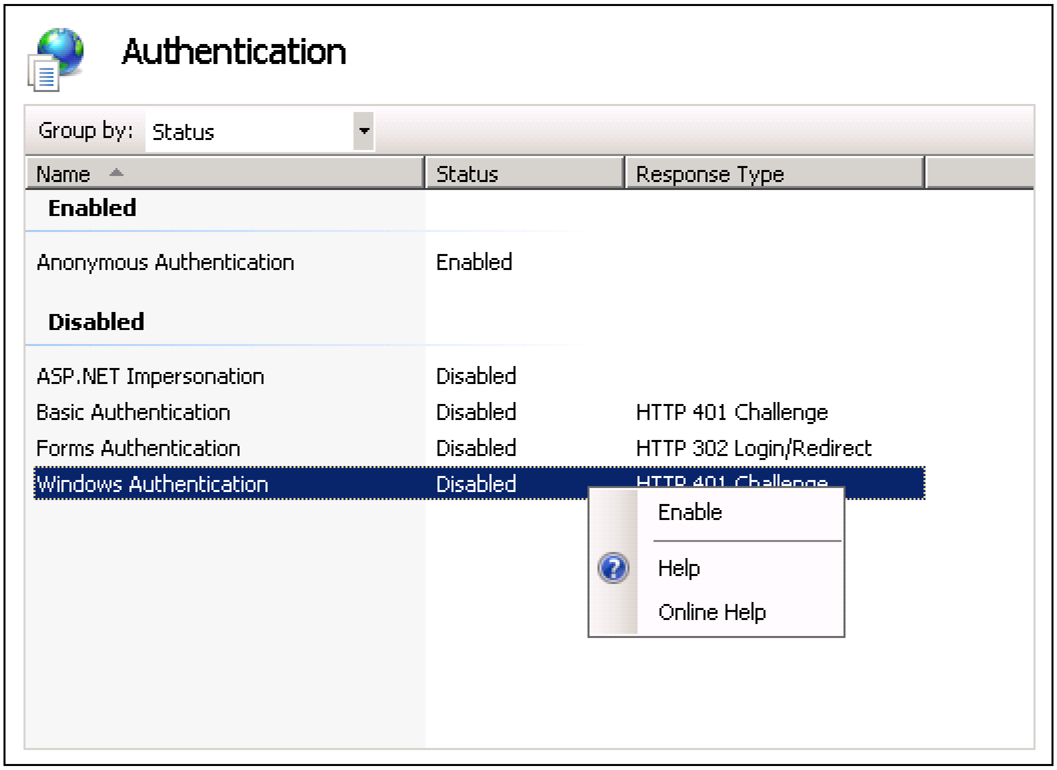
6. Click **OK** to exit the Authentication Methods screen. Click **OK** again to exit the Properties screen. You have completed the necessary IIS configuration steps for IIS 6.0.

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.



Authentication

Group by: Status

Name	Status	Response Type
Enabled		
Anonymous Authentication	Enabled	
Disabled		
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

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 13: 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.

You can create Everyday User accounts within EMS in several ways:

- Manually Create Everyday User Accounts
- Automatically Create Everyday User Accounts
- Modify Existing Everyday User Accounts

MANUAL EVERYDAY USER ACCOUNT CREATION

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.

AUTOMATIC EVERYDAY USER ACCOUNT CREATION

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	*Must be specified*
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	*Must be specified*
Authentication	Portal Authentication External Reference Variable	*Must be specified*
Authentication	Portal Authentication Fax Variable	*Must be specified*
Authentication	Portal Authentication Name Variable	*Must be specified*
Authentication	Portal Authentication Phone Variable	*Must be specified*

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.

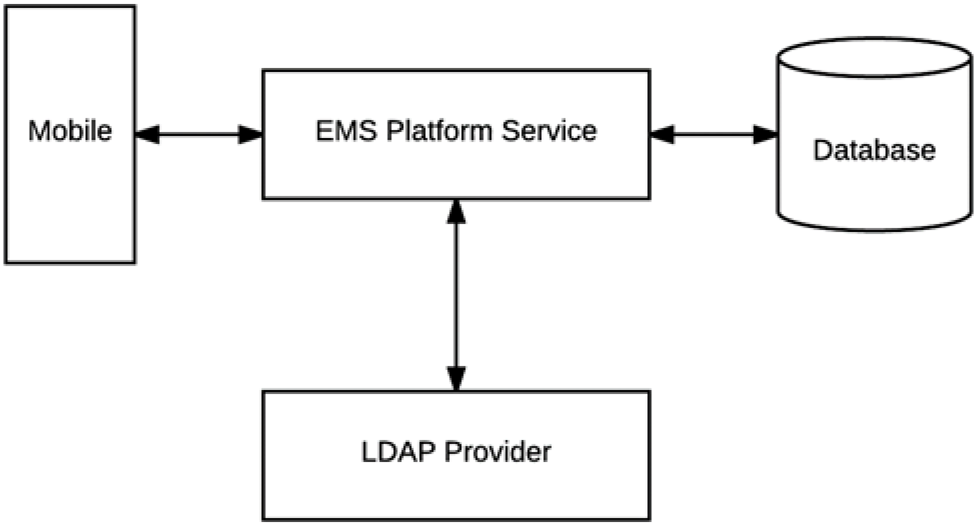
EXISTING EVERYDAY USER ACCOUNTS

> **Warning for 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 14: 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.

Notes:

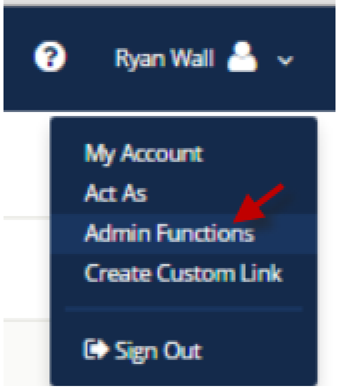
- The EMS Web App LDAP-Process Template assignment process requires that your implementation of LDAP stores group information (e.g., staff, student, department, etc.) as a Directory Service object containing a property (i.e., member) that contains the users that belong to your various groups.

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

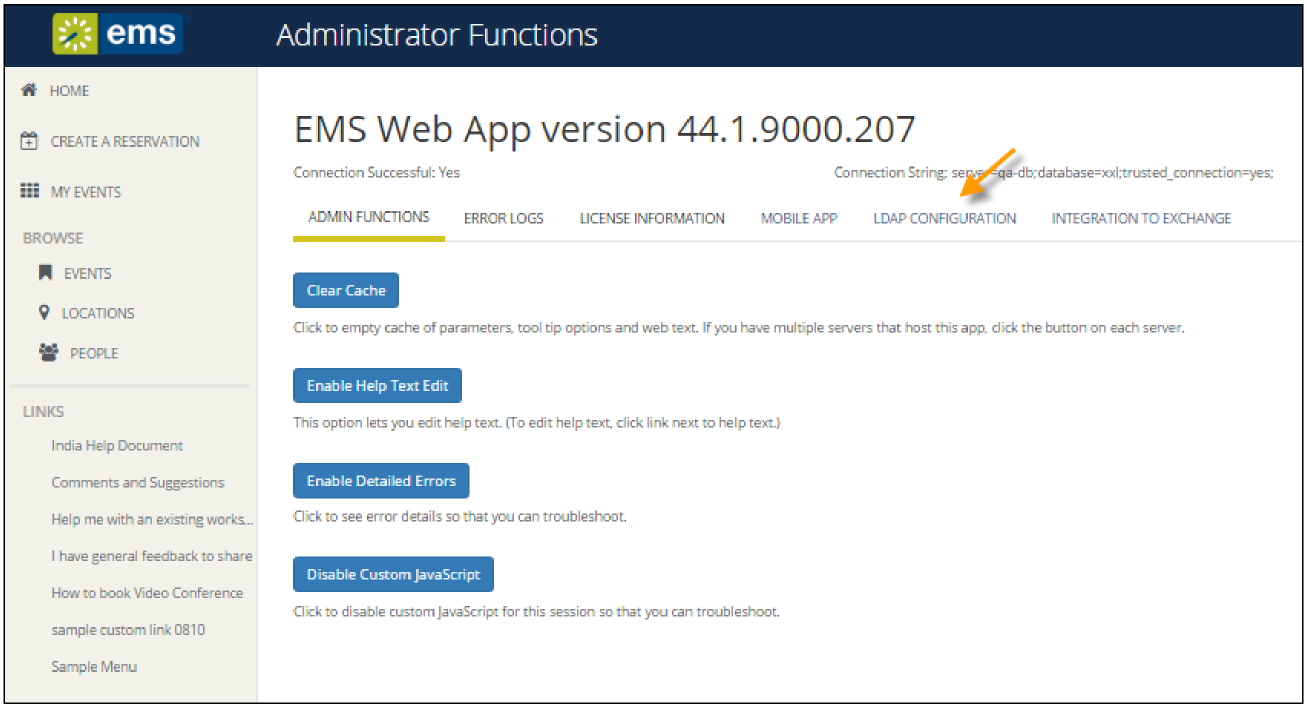
CONFIGURE EMS WEB APP TO USE LDAP AUTHENTICATION

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.



EMS Web App version 44.1.9000.207

Connection Successful: Yes

Connection String: server=qa-db;database=xxl;trusted_connection=yes;

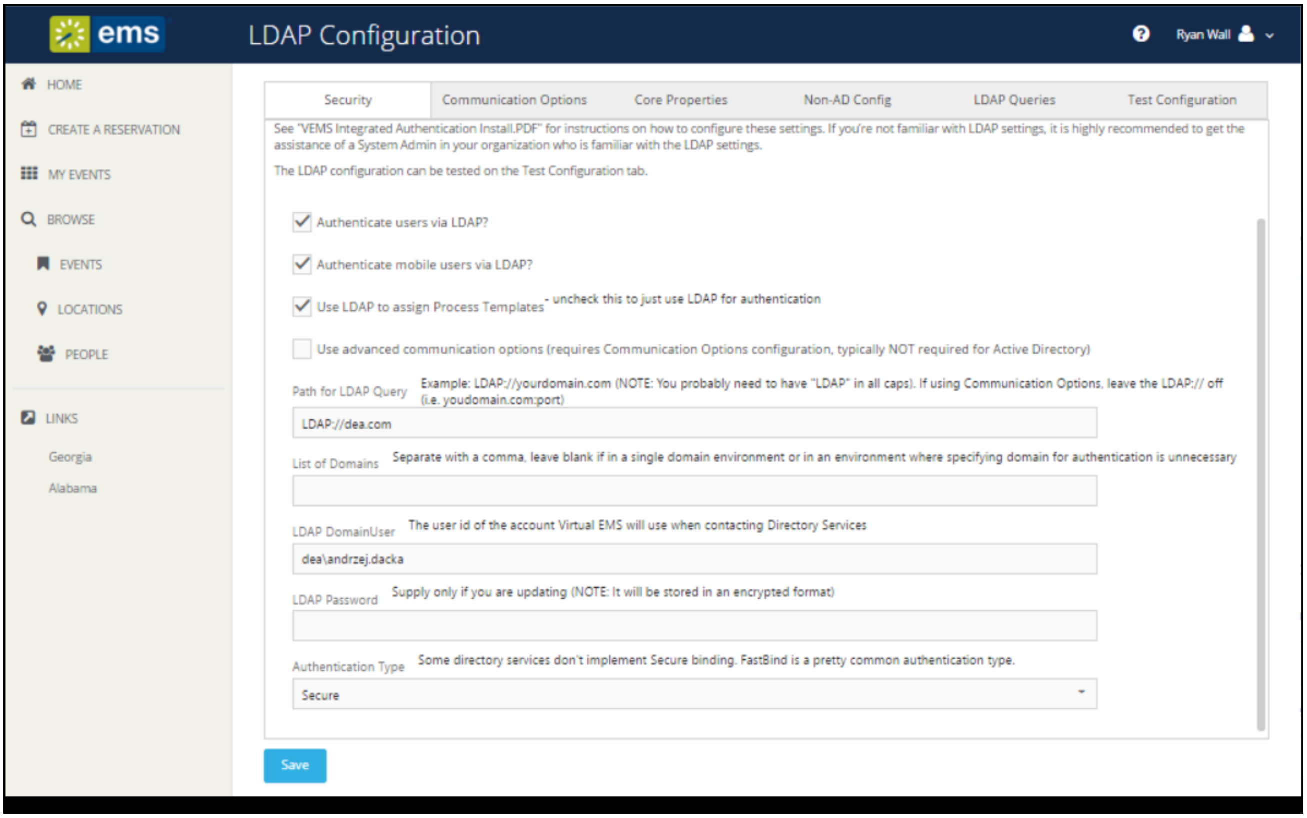
Click to empty cache of parameters, tool tip options and web text. If you have multiple servers that host this app, click the button on each server.

This option lets you edit help text. (To edit help text, click link next to help text.)

Click to see error details so that you can troubleshoot.

Click to disable custom JavaScript for this session so that you can troubleshoot.

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



See "VEMS Integrated Authentication Install.PDF" for instructions on how to configure these settings. If you're not familiar with 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 LDAP configuration can be tested on the Test Configuration tab.

☑ Authenticate users via LDAP?

☑ Authenticate mobile users via LDAP?

☑ Use LDAP to assign Process Templates - uncheck this to just use LDAP for authentication

□ Use advanced communication options (requires Communication Options configuration, typically NOT required for Active Directory)

Path for LDAP Query — Example: LDAP://yourdomain.com (NOTE: You probably need to have "LDAP" in all caps). If using Communication Options, leave the LDAP:// off (i.e. youdomain.com:port)

LDAP://dea.com

List of Domains — Separate with a comma, leave blank if in a single domain environment or in an environment where specifying domain for authentication is unnecessary

LDAP DomainUser — The user id of the account Virtual EMS will use when contacting Directory Services

dea\andrzej.dacka

LDAP Password — Supply only if you are updating (NOTE: It will be stored in an encrypted format)

Authentication Type — Some directory services don't implement Secure binding. FastBind is a pretty common authentication type.

Secure

CONFIGURE EMS WEB APP SECURITY

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

c. **Use advanced communication options:** Skip this step for Active Directory environments. Enabling this checkbox requires that you complete the settings on the **Communication Options** tab.

d. In the **Path for LDAP Query** field, specify a valid LDAP path (example – LDAP://YourCompany.com)

e. **List of Domains:** Skip this step if your organization uses a single domain. Otherwise, provide a comma separated list of your domains.

f. In the **LDAP Domain\User** field, enter a Domain User account that has rights to query LDAP (example – YourDomain\User)

g. In the **Password** field, enter a valid Password for the User Account entered in the previous step.

h. Specify the appropriate LDAP **Authentication Type** for your environment.

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

CONFIGURE COMMUNICATION OPTIONS

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

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

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

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

- **LDAP Name Property:** The property for user name on the user record in LDAP that will be displayed. Displayname is the default, as it is the most common.

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

NON-AD CONFIGURATION

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

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

- **LDAP Account/User ID Property:** The property in your LDAP store that contains the user name.

Example: If sameaccountname=xxxx, then enter sameaccountname

- **Full LDAP User ID Format:** Leave blank unless authentication requires a full path.

  Example: cn={0},ou=staff,o=yourdomain

- **LDAP Group Category:** The property in your LDAP store that contains the group category.

  Example: If filter should be objectClass=groupOfNames, then property should be groupOfNames

- **LDAP Group Name:** The property in your LDAP store that contains the group name.
- **LDAP Group Member Name:** The property in your LDAP store that contains the name of a single member in the group.

  Example: If member property is member=jdoe, then property should be member

- **LDAP Group Member User Name Attribute:** The property of the user record that corresponds to the group's member property to determine group membership.

LDAP QUERIES

> **Warning:** It is recommended that this tab only be edited with assistance from

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

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

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

SAVE YOUR CONFIGURATION

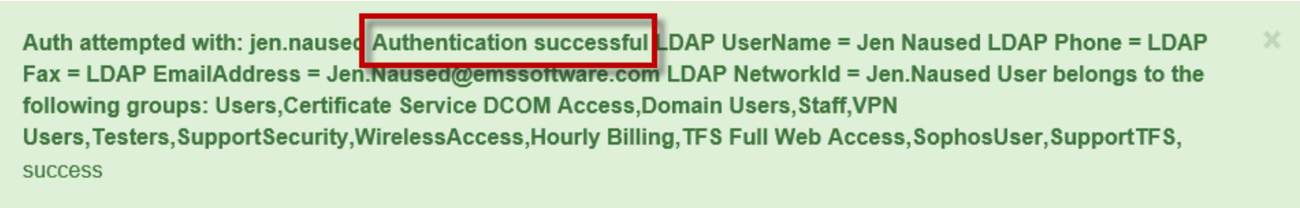
1. Click **Save**.

> Note: If you want Everyday Users to inherit Everyday User Process Templates based on the LDAP Group(s) with which they belong, proceed to Step 7. 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.naused Authentication successful LDAP UserName = Jen Naused LDAP Phone = LDAP Fax = LDAP EmailAddress = Jen.Naused@emssoftware.com LDAP NetworkId = Jen.Naused 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 15: Portal or Federated Authentication

This topic provides information on the following:

PORTAL AUTHENTICATION OVERVIEW

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

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

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

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

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

INSTALLATION/CONFIGURATION

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

AREA	DESCRIPTION	VALUE
Authentication	Portal Authentication Cookie Key	Required if Portal Authentication Method = Cookie
Authentication	Portal Authentication Method	Server Variable Session Form Cookie Query String
Authentication	Portal	User variable to be compared against the

AREA	DESCRIPTION	VALUE
	Authentication Variable	EMS Everyday User External Reference/Network ID field

2. Direct users to the default EMS Web App page. If the default installation settings were used, the default page is:

   (http://[ServerName]/EMSWebApp/Default.aspx)
   (replace [ServerName] with the name of your web server)

REDIRECT USER LOG IN TO YOUR SSO PROVIDER

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

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

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

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

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

SPECIFY A DIFFERENT DEFAULT HOME PAGE FOR GUEST USERS

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

CHAPTER 16: Portal Authentication Methods

This topic provides information about the following:

- Server Variable Method (Header Variable)
- Server Variable Method - Federated (SAML)
  - Method 1: Locally installed service provider
  - Method 2
- EMS 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.

Code example:

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)

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, configure the EMS Web App parameter “Portal Authentication Method”
5. In EMS, 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 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 Application 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, configure the EMS Web App parameter “Portal Authentication Method”
5. In EMS, configure the applicable Portal Authentication Variables.
6. In EMS, 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 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@ems-software.com"

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

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

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

```
%>
```

QUERY STRING METHOD

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

Code example:

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

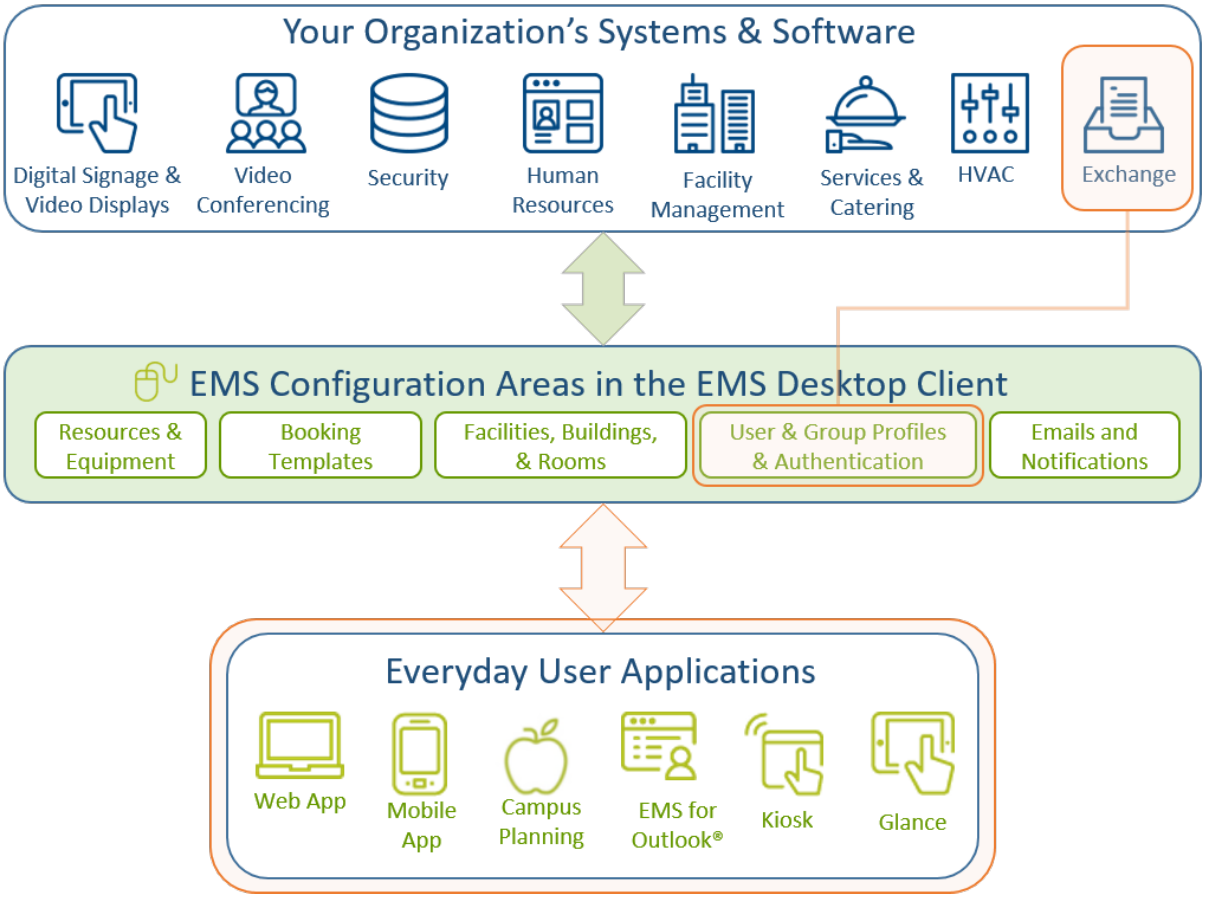
To use the query string method, set the Portal Authentication Method parameter to **Query String** and type the appropriate variable for the Portal Authentication Variable parameter.

CHAPTER 17: Introduction to Integration to Microsoft Exchange

This guide provides instruction in installing Integration to Microsoft Exchange for System Administration and IT users.

EMS Integration with 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.

EXCHANGE INTEGRATION FLOW


Your Organization's Systems & Software
Digital Signage & Video Displays
Video Conferencing
Security
Human Resources
Facility Management
Services & Catering
HVAC
Exchange
EMS Configuration Areas in the EMS Desktop Client
Resources & Equipment
Booking Templates
Facilities, Buildings, & Rooms
User & Group Profiles & Authentication
Emails and Notifications
Everyday User Applications
Web App
Mobile App
Campus Planning
EMS for Outlook®
Kiosk
Glance

You must be licensed for EMS, EMS Web App, and EMS Integration with Microsoft® Exchange in order to configure and use this feature. If you are unsure if your organization is licensed for EMS Integration with

Microsoft® Exchange, or if you would like to learn more about it, please contact your Account Executive.

To install and configure EMS Integration with Exchange, you will:

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

SYSTEM REQUIREMENTS

You must be licensed for EMS, EMS Web App, and Integration with Exchange in order 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 Microsoft® Exchange:

- EMS and/or EMS Web App Installed

EMS must be installed and operational.

- Valid Outlook Integration License

You must be licensed for EMS, EMS Web App and Integration with Exchange in order 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.

WEB APPLICATION REQUIREMENTS

DESKTOP BROWSER
Internet Explorer 11 (please see Tip below)
Microsoft Edge (latest)
Firefox (latest)
Chrome (latest)
Safari (Mac) (latest)

*= varies per application

TIP: 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 Web App V44.1.

EMS WEB APP (MOBILE)

MOBILE BROWSER	PLATFORM
Internet Explorer for Mobile 8.1	Windows
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.

WEB SERVER REQUIREMENTS

OPERATING SYSTEM	IIS APP POOL
Windows Server 2008 R2	7/7.5
Windows Server 2012	8
Windows Server 2012 R2	8.5
Prerequisites	
Application Pool Running 4.0*	
.NET Framework 4.6.1*	
Minimum System Requirements	
Processor: 2.0 GHz and 4 cores or faster	
Memory: 8 GB or more*	
Hard-Disk Space: 1 GB or more	

OPERATING SYSTEM	IIS APP POOL
*For up to 100 concurrent users. Increased specs required for 100+ concurrent users.	

*= varies per EMS Software Application

EXCHANGE INTEGRATION REQUIREMENTS

Microsoft® Office	365
Outlook	2010, 2013, 2016
.NET Framework	4.6.1
Microsoft® Visual Studio 2010 Tools for Office Runtime	VSTOR 2010
Prerequisites	
EMS Web App	Latest

On User Workstations	Desktop requirements for Microsoft® Outlook Windows 7, 8, or 10

EMS PLATFORM SERVICES

OPERATING SYSTEM	IIS
Windows Server 2008 R2	7/7.5
Windows Server 2012	8
Windows Server 2012 R2	8.5
.NET Framework	4.6.1
Application Pool	4.0
Prerequisites	
HTTPPlatformHandler IIS Module	Download Version 1.2 here OR download the installer here.

OPERATING SYSTEM	IIS
PowerShell	5+ Version
ASP.NET Version 4.6	Under Web Server (IIS)->Web Server->Application Development: » ISAPI Extensions » ISAPI Filters » .NET Extensibility 4.6

EMS INTEGRATION FOR EXCHANGE

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

Configure EWS Impersonation for Microsoft® Exchange

CHAPTER 17: System Requirements for Integration to Microsoft® Exchange

You must be licensed for EMS, EMS Web App, and Integration with Exchange in order 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 Microsoft® Exchange:

- EMS and/or EMS Web App Installed

EMS must be installed and operational.

- Valid Outlook Integration License

WEB APPLICATION REQUIREMENTS

DESKTOP BROWSER
Internet Explorer 11 (please see Tip below)
Microsoft Edge (latest)
Firefox (latest)
Chrome (latest)
Safari (Mac) (latest)

*= varies per application

> **TIP:** 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 Web App V44.1.

EMS WEB APP (MOBILE)

MOBILE BROWSER	PLATFORM
Internet Explorer for Mobile 8.1	Windows
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.

WEB SERVER REQUIREMENTS

OPERATING SYSTEM	IIS APP POOL
Windows Server 2008 R2	7/7.5
Windows Server 2012	8
Windows Server 2012 R2	8.5
Prerequisites	
Application Pool Running 4.0*	
.NET Framework 4.6.1*	
Minimum System Requirements	
Processor: 2.0 GHz and 4 cores or faster	
Memory: 8 GB or more*	
Hard-Disk Space: 1 GB or more	

OPERATING SYSTEM	IIS APP POOL
*For up to 100 concurrent users. Increased specs required for 100+ concurrent users.	

*= varies per EMS Software Application

EXCHANGE INTEGRATION REQUIREMENTS

Microsoft® Office	365
Outlook	2010, 2013, 2016
.NET Framework	4.6.1
Microsoft® Visual Studio 2010 Tools for Office Runtime	VSTOR 2010
Prerequisites	
EMS Web App	Latest

On User Workstations	Desktop requirements for Microsoft® Outlook Windows 7, 8, or 10

EMS PLATFORM SERVICES

OPERATING SYSTEM	IIS
Windows Server 2008 R2	7/7.5
Windows Server 2012	8
Windows Server 2012 R2	8.5
.NET Framework	4.6.1
Application Pool	4.0
Prerequisites	
HTTPPlatformHandler IIS Module	Download Version 1.2 here OR download the installer here.

OPERATING SYSTEM	IIS
PowerShell	5+ Version
ASP.NET Version 4.6	Under Web Server (IIS)->Web Server->Application Development: » ISAPI Extensions » ISAPI Filters » .NET Extensibility 4.6

EMS INTEGRATION FOR EXCHANGE

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

Configure EWS Impersonation for Microsoft® Exchange

CHAPTER 17: 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 Desktop Client Installation Instructions.
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 17: Configure Integration to Exchange

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 with Microsoft 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 Configuring Exchange Web Service Impersonation.

This topic provides information on the following:

- Configure Integration to Exchange Instructions
- Test Your Exchange Integration

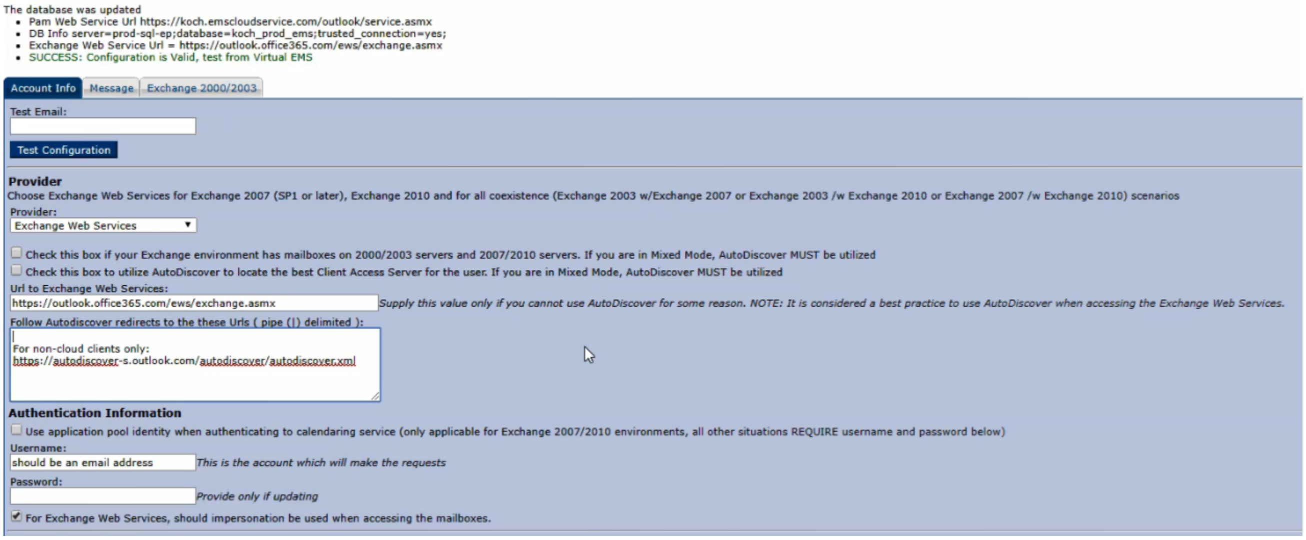
CONFIGURE INTEGRATION TO EXCHANGE INSTRUCTIONS

1. After following the installation instructions, access the Integration with Exchange configuration area by opening a browser and entering the following:

   http://[ServerName]/ExchangeIntegrationWebService/PamConfig.aspx (replace [ServerName] with the name of your web server)

2. Go the **Account Info** tab.

Office 365 Configuration Example



The database was updated

- Pam Web Service Url https://koch.emscloudservice.com/outlook/service.asmx
- DB Info server=prod-sql-ep;database=koch_prod_ems;trusted_connection=yes;
- Exchange Web Service Url = https://outlook.office365.com/ews/exchange.asmx
- SUCCESS: Configuration is Valid, test from Virtual EMS

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

□ 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 user. If you are in Mixed Mode, AutoDiscover MUST be utilized

Url to Exchange Web Services: https://outlook.office365.com/ews/exchange.asmx *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 the these Urls (pipe (|) delimited):

For non-cloud clients only:
https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml

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: should be an email address *This is the account which will make the requests*

Password: *Provide only if updating*

☑ For Exchange Web Services, should impersonation be used when accessing the mailboxes.

3. Select your email system in the Provider dropdown 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 with Exchange Account User Name and Password. The User Name should be prefixed with your

domain (example – YourDomain\Integration with Exchange Account, or Integration with Exchange Account@YourDomain) .

> **TIP:** Make a note of this URL for use later in this topic.

6. (*Optional*) The "Use application pool identity…" option allows you to set the Integration with 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 with 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 with Exchange, the email account that is being used (either on the Test Settings tab or in the "Testing Integration with 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.

Click **Test Configuration**. If any errors are encountered, please verify your configuration. Otherwise, your Integration with Exchange configuration is complete.

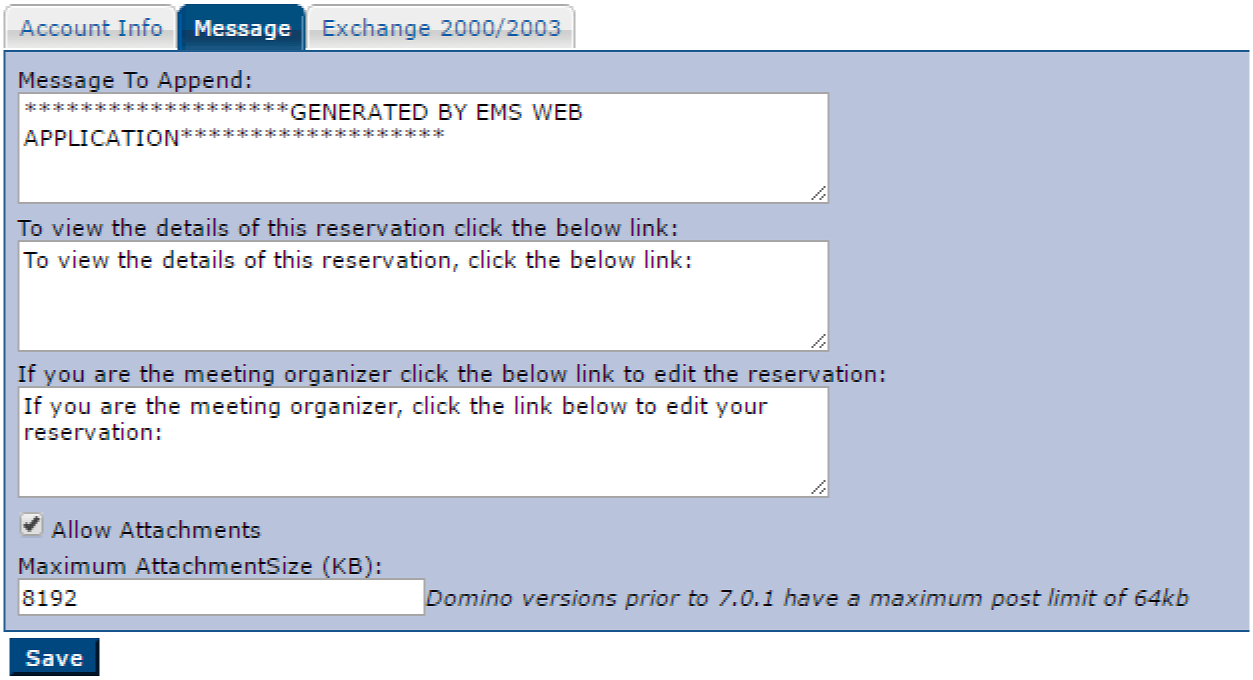
TEST YOUR EXCHANGE INTEGRATION

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

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

OPTIONAL MESSAGING SETTINGS

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



Message 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*

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	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.

FIELD	DESCRIPTION
click the below link	
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. ***Click for more...***

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**.

WARNING: FOR EXTERNALLY EXPOSED WEB APP SITES

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

CHAPTER 17: 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.

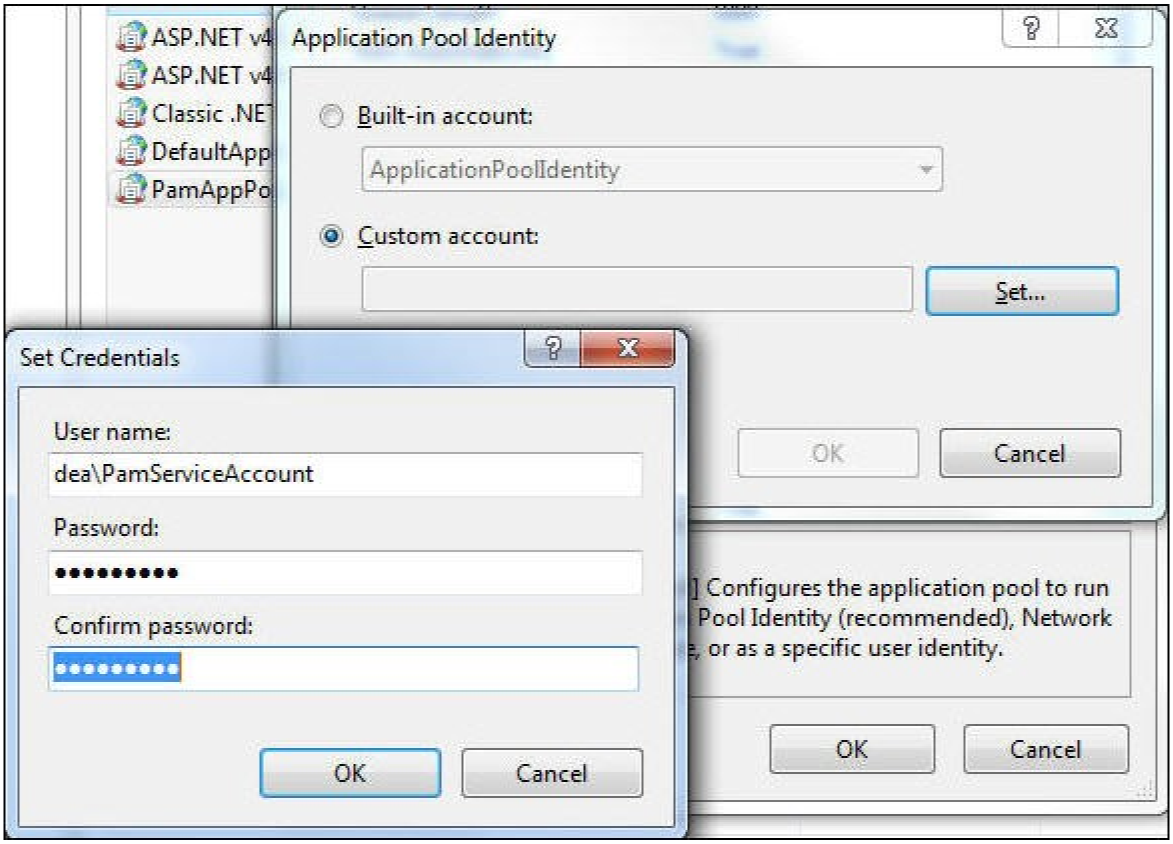
This functionality requires the following:

- 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).



Application Pool Identity

○ Built-in account:

ApplicationPoolIdentity

● Custom account:

] Configures the application pool to run Pool Identity (recommended), Network , or as a specific user identity.

Set Credentials

User name:

dea\PamServiceAccount

Password:

●●●●●●●●●●

Confirm password:

●●●●●●●●●●

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

11. Click **OK** on all remaining dialogs.

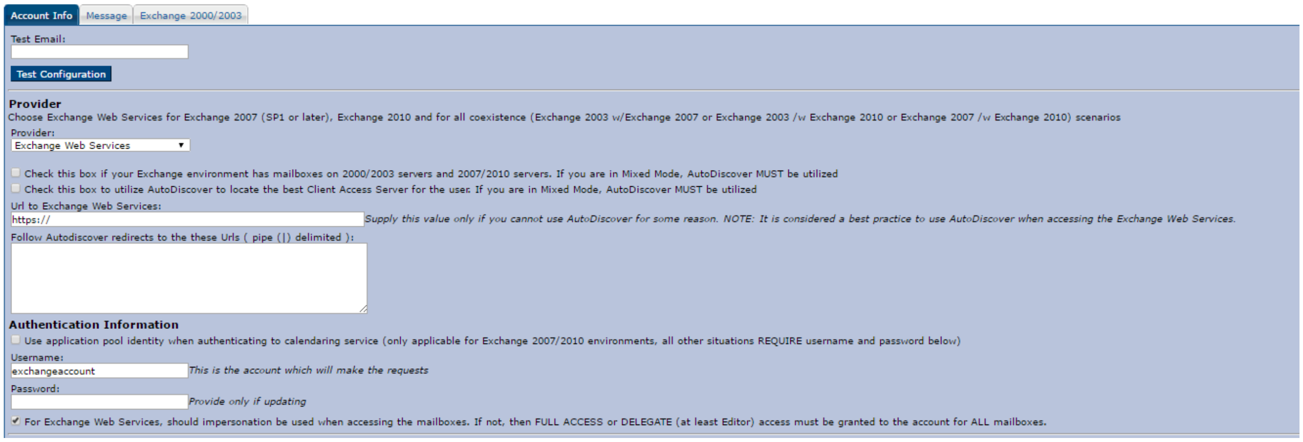
CONFIGURE INTEGRATION FOR EXCHANGE TO USE THE APPLICATION POOL ACCOUNT

1. Navigate to the Integration for Exchange configuration area by opening a browser and entering the following:

   http://[ServerName]/PAMWebService/PAMConfig.aspx (replace [ServerName] with the name of your web server)

2. From the **Account Info** tab, find the Authentication Information section, check the box for **Use application pool identity when authenticating to calendaring service** (see following image).
3. With this option enabled, you can leave the Username and Password fields blank in the Authentication Information section.

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



Test Email:

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 ▾

☐ 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 user. If you are in Mixed Mode, AutoDiscover MUST be utilized

Url to Exchange Web Services: https:// *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 the these Urls (pipe (|) delimited):

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 *This is the account which will make the requests*

Password: *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 17: Configure EWS Impersonation for Microsoft® Exchange

> **TIP:** See Also: What is EWS Impersonation?

1. Log in to the Office 365® Exchange Administration Center.
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.

CHAPTER 17: 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.

What do we lose if we don't allow impersonation?

Without the impersonation account turned on, you can only make "hanger "reservations from EMS for Outlook: meetings made in EMS for Outlook will be locked in EMS Web App and EMS Desktop Client.

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

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

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

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

- The account needs Editor w/Folder owner (so a custom rights set).
- Custom rights, at least through exchange 2010, are not scriptable. This means the delegation account will get set to owner, which is the only built in (read scriptable) option that has all the necessary permissions.
- EMS for Outlook creates a custom property on the Calendar folder, which allows you to programmatically search the folder for items that have the custom property. Once that custom property is created, then Editor will be enough. It is the creation of the custom property at the folder level that requires owner permission.
- While you can use PowerShell to script the permissions and loop through the users and set the permissions (owner), you would need to make sure that the script got applied to any new users and reapplied to any users that have changed the permissions of the delegation account

- Rights are granted to ANY mail client (Outlook, OWA, etc): when using the impersonation account, rights are only granted to Exchange Web Services, so nobody could type in the service account into Outlook and gain the same permissions.
- These rights are visible to the end user. For example, if an account, "EMSExchangeAccount", has been granted, delegation rights (any level) to User1’s calendar, and User1 goes to the Permissions tab of his calendar, he will see the EMSExchangeAccount and the rights it is assigned. Additionally, User1 would be able to change the rights, which would essentially disable the Exchange integration.
- This restricts access only to the calendar

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

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

ADDITIONAL READING

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

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

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

- Delegate Access and EWS in Exchange

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