# EMS WEB APP Installation Guide

## V44.1

**Last Updated: March 5, 2018**

 © 2018 EMS Software, LLC. All Rights Reserved.

# Table of Contents


CHAPTER 1: EMS Web App Introduction ..... 1

Contact Customer Support ..... 2

CHAPTER 2: System Architecture ..... 3

CHAPTER 3: Requirements and Prerequisites ..... 5

Prerequisites ..... 5

Database Requirements ..... 6

Web Server ..... 6

Web Application Requirements ..... 7

EMS Web App (Mobile) ..... 8

EMS for Outlook Requirements ..... 8

EMS Platform Services ..... 9

Prerequisites ..... 10

10

EMS Integration for Exchange ..... 10

CHAPTER 4: Obtain the Installation Files ..... 11

CHAPTER 5: Install or Upgrade to the EMS Web App ..... 12

CHAPTER 6: Upgrade Considerations ..... 18

Time Zone Settings ..... 19

Best Practices ..... 19

Configuration and Parameter Settings ..... 19

Web Menus ..... 21

Functional Changes ..... 22

Help Text Records ..... 23

CSS (Style) Settings ..... 25

Language Translation ..... 25

All Other Customizations ..... 25

CHAPTER 7: Optional EMS Web App Features ..... 26

Integrated Authentication ..... 26

Integration with Microsoft® Exchange ..... 26

Floor Plans ..... 27

CHAPTER 8: Customize EMS Web App ..... 28

Customize the Logo ..... 29

Customize Style Sheets ..... 29

Customize Links ..... 30

Customize JavaScript ..... 35

Contact Customer Support ..... 37

CHAPTER 9: EMS Mobile Web Application ..... 38

CHAPTER 10: Launch EMS Web App ..... 39

CHAPTER 11: Windows Server 2008/2008 R2 Web Server Setup Guide ..... 40

CHAPTER 12: Best Practices: Setting Up Your Web Server 2008 or 2008 R2 ..... 41

To Install .NET Framework 3.5 ..... 42

To Install .NET Framework 4.5: Regics Only ..... 43

To Install Internet Information Services (IIS) ..... 43

To Add Role Services ..... 45

Common HTTP Features ..... 46

Application Development ..... 47

Health and Diagnostics ..... 49

Security ..... 50

Performance ..... 51

Management Tools ..... 51

CHAPTER 13: Install .NET Framework 2008 ..... 52

Install .NET Framework 3.5 ..... 52

Install .NET Framework 4.5: Regics Only ..... 53

CHAPTER 14: Install Internet Information Services (IIS) ..... 54

CHAPTER 15: Add Role Services ..... 56

Common HTTP Features ..... 57

Application Development ..... 58

Health and Diagnostics ..... 59

Security ..... 60

Performance ..... 61

Management Tools ..... 62

CHAPTER 16: Windows Server 2012/2012 R2 Web Server Setup Guide ..... 63

CHAPTER 17: Best Practices: Setting Up Your Web Server 2012 or 2012 R2 ..... 64

To Install .NET Framework 3.5 ..... 65

To Install .NET Framework 4.5: Regics Only ..... 66

To Install Internet Information Services (IIS) ..... 66

To Add Role Services ..... 68

Common HTTP Features ..... 69

Application Development ..... 70

Health and Diagnostics ..... 71

Security ..... 72

Performance ..... 73

Management Tools ..... 74

Windows Server 2012/2012 R2 ..... 74

To Install .NET Framework 4.5: Regics Only ..... 83

To Add Role Services ..... 84

Common HTTP Features ..... 85

Application Development ..... 86

Health and Diagnostics ..... 87

Security ..... 88

Performance ..... 89

Management Tools ..... 89

CHAPTER 18: Install .NET Framework for Windows Server 2012/2012 R2 ..... 91

Install .NET Framework 3.5 and .NET Framework 4.5 ..... 91

Install .NET Framework 4.5: Regics Only ..... 93

CHAPTER 19: Install Internet Information Services (IIS) ..... 96

CHAPTER 20: Add Role Services ..... 98

Common HTTP Features ..... 99

Application Development ..... 100

Health and Diagnostics ..... 101

Security ..... 102

Performance ..... 103

Management Tools ..... 104

CHAPTER 21: Authentication Options ..... 105

CHAPTER 22: Introduction ..... 106

What is Integrated Windows Authentication? ..... 108

What is Portal or Federated Authentication? ..... 109

What is LDAP Authentication? ..... 110

Contact Customer Support ..... 113

CHAPTER 23: Integrated Authentication Considerations ..... 114

LDAP Integration ..... 114

Pros ..... 114

Cons ..... 115

Integrated Authentication ..... 115

Pros ..... 115

Cons ..... 115

Portal Authentication ..... 116

CHAPTER 24: VPAT for EMS Web App (V44.1) ..... 117

EMS Accessibility Conformance Report ..... 117

Standards/Guidelines ..... 117

Table Information ..... 118

Terms ..... 119

WCAG 2.0 Report ..... 119

Table 2. Conformance Criteria, Level AA ..... 130

Table 3. Conformance Criteria, Level AAA ..... 133

Table 4. WCAG Conformance Requirements ..... 134

2017 Section 508 Report ..... 137

Functional Performance Criteria ..... 137

Hardware ..... 138

Software ..... 138

Support Documentation and Services ..... 143

Contact Support ..... 144

CHAPTER 25: Integrated Windows Authentication ..... 145

Activate Integrated Windows Authentication for IIS 6.0 ..... 146

Activate Integrated Windows Authentication for IIS 7.x/8.x ..... 148

CHAPTER 26: Manage Everyday Users For Integrated Authentication ..... 150

Manual Everyday User Account Creation ..... 150

Automatic Everyday User Account Creation ..... 151

EMS Web App Parameters ..... 152

Portal/Federated Authentication Parameters ..... 152

HR Toolkit (for EMS Workplace, EMS Campus, EMS Enterprise, EMS District, and EMS Legal only) ..... 153

Automatic Template Assignment to Users ..... 154

Existing Everyday User Accounts ..... 154

CHAPTER 27: LDAP Authentication ..... 156

Overview ..... 156

Configure EMS Web App to Use LDAP Authentication ..... 158

Configure EMS Web App Security ..... 160

Configure Communication Options ..... 162

Core Properties ..... 163

Non-AD Configuration ..... 164

LDAP Queries ..... 165

Save Your Configuration ..... 166

Test Your Configuration ..... 167

Configure Authentication for EMS Mobile App ..... 168

CHAPTER 28: Portal or Federated Authentication ..... 169

Portal Authentication Overview ..... 169

Installation/Configuration ..... 171

Redirect User Log In to Your SSO Provider ..... 172

Specify a Different Default Home Page for Guest Users ..... 173

CHAPTER 29: Portal Authentication Methods ..... 174

Server Variable Method (Header Variable) ..... 175

Server Variable Method - Federated (SAML) ..... 175

Method 1: Locally installed Service Provider ..... 175

Method 1 configuration Steps ..... 176

Method 2 ..... 176

Method 2 Configuration Steps ..... 177

EMS Configuration ..... 177

Session Method ..... 178

Form Method ..... 179

Cookie Method ..... 180

Query String Method ..... 182

CHAPTER 30: Authentication Options for EMS Web App and Virtual EMS 183

(VEMS) .....

Integrated Windows Authentication .....183

LDAP .....184

Portal .....184

# CHAPTER 1: EMS Web App Introduction

EMS Web App is an optional web application to access online. EMS Web App lets you see your schedule, create new reservations, and change existing reservations.

If you have deployed an older version of EMS Web App and are upgrading to the newest version, please encourage users at your facility to review {see What's New} before they begin working with the new version of the software. Doing so will streamline the adoption of the new release and help your users benefit from new features and functions that they might not otherwise discover.

**Concept: The EMS Web App also runs on a mobile device such as a tablet or handheld.** ***Click for more...***

Due to the smaller screen size and resolution of tablets and smartphones, pages may display differently but most of the same functionality is still available.

EMS Mobile App, by contrast, is an app designed specifically for smartphones. It offers functionality specifically for everyday users who need access to EMS while they're on the go. The EMS Mobile App also runs on tablets that run iOS

or Android, but the screen layout is optimized for smartphones and does not take advantage of larger displays.

See Also: EMS Web App Configuration Guide

## CONTACT CUSTOMER SUPPORT

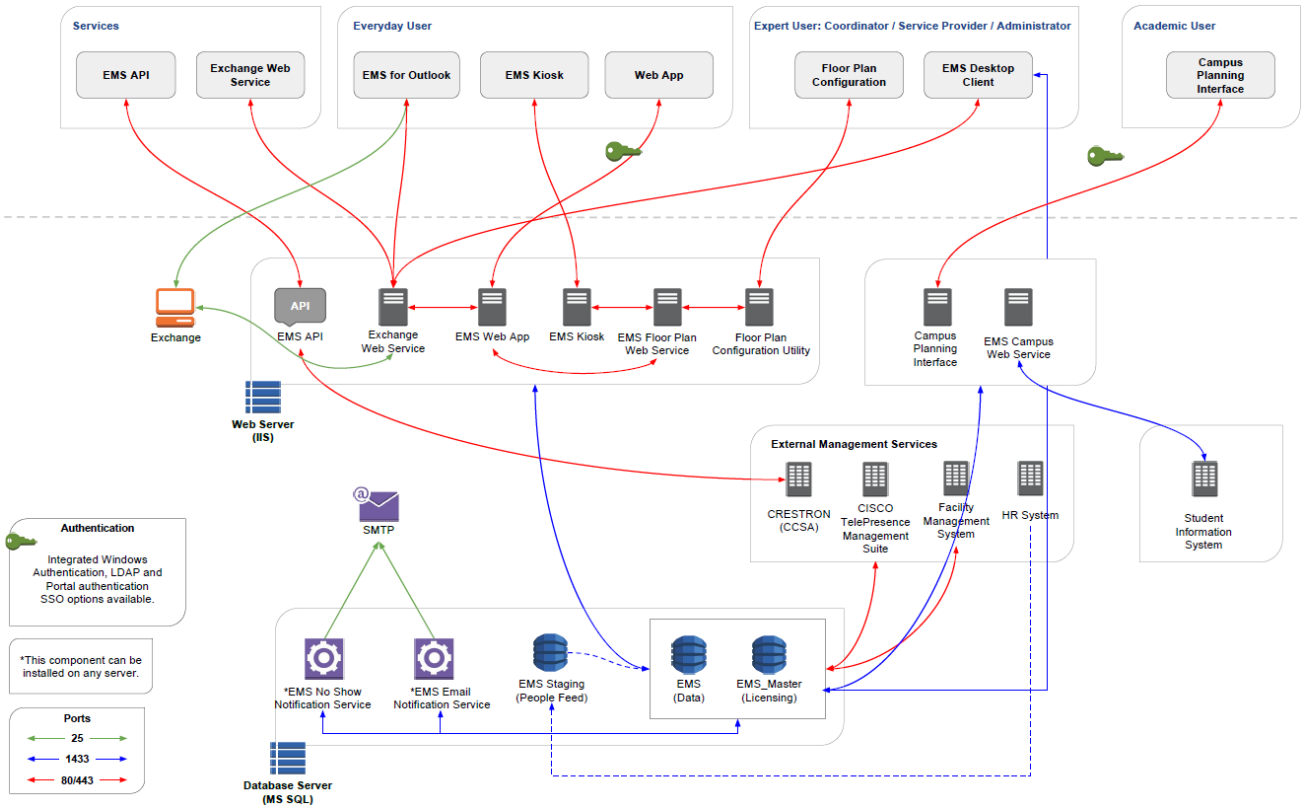
- **Option 1 (Recommended):** Search the Knowledge Base available in the EMS Support Portal.
- **Option 2:** Submit a Case directly via the EMS Support Portal.
- **Option 3:** Email support@emssoftware.com.
- **Option 4 (Recommended for critical issues only):** Phone (800) 288-4565

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

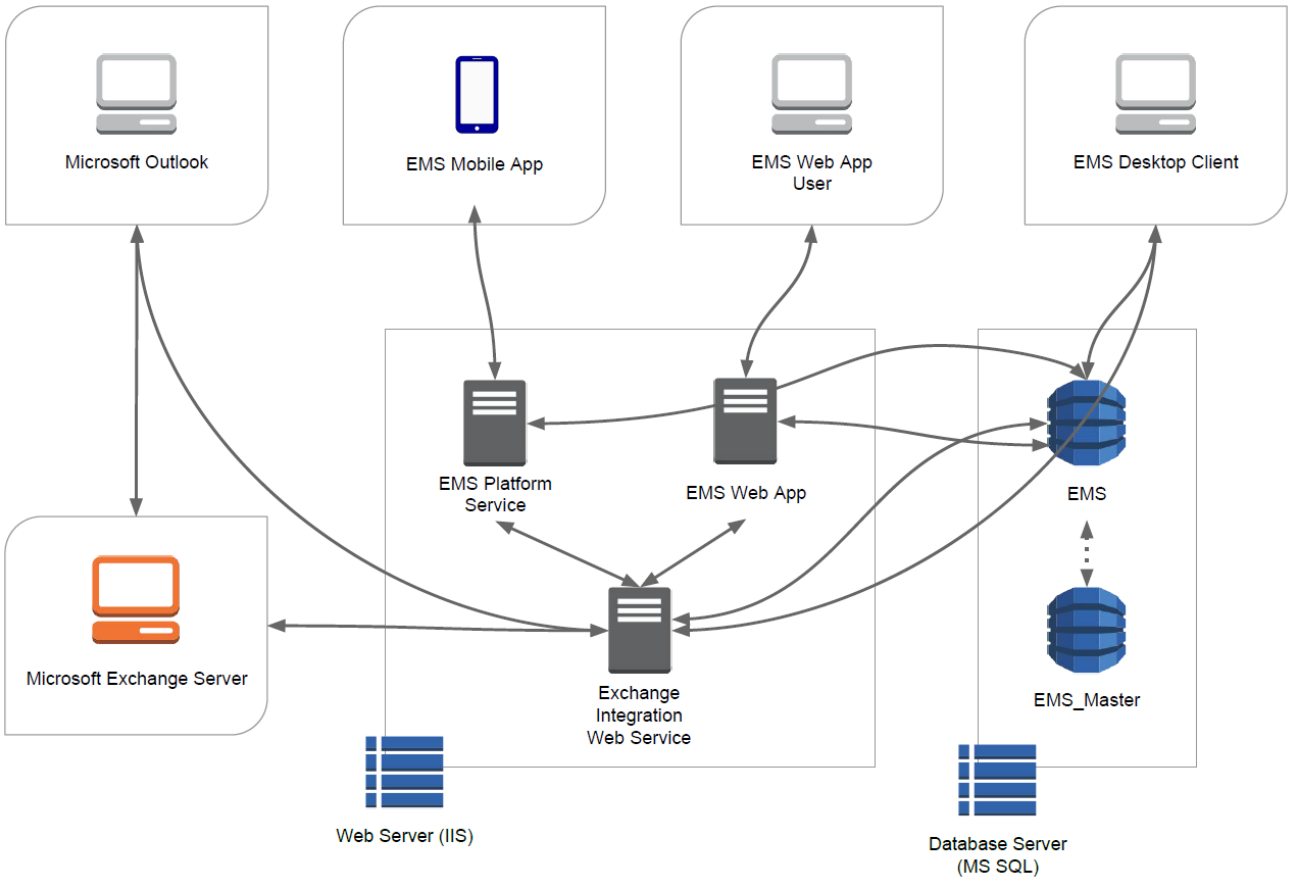
# CHAPTER 2: System Architecture

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

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



The diagram below shows how EMS Everyday Applications interact with EMS Desktop Clients, your web and database servers, and Microsoft® Exchange.



# CHAPTER 3: Requirements and Prerequisites

Before beginning the installation process, please install or upgrade your EMS databases as outlined in the EMS Web App Installation Instructions.

Installation will prompt you to enter a web server. Special setup guides are available for Windows 2008/2008 R2 Web Server and Windows 2012/2012 R2 Web Server.

Existing versions of EMS Web App must be manually uninstalled. Please make sure to copy-off and save any files that have been customized.

## PREREQUISITES

- Before beginning the installation process, please install or upgrade your EMS databases as outlined in the EMS Web App (V44.1) Installation Guide.
- Installation will prompt you to enter a web server. Special setup guides are available for Windows Server 2008/2008 R2 Web Server Setup Guide and Windows Server 2012/2012 R2 Web Server Setup Guide.
- Existing versions of EMS Web App must be manually uninstalled. Please make sure to copy-off and save any files that have been customized.

# DATABASE REQUIREMENTS

| OPERATING SYSTEM |
| --- |
| Microsoft SQL Server 2008 R2 |
| Microsoft SQL Server 2012 SP2 |
| Microsoft SQL Server 2012 SP3 |
| Microsoft SQL Server 2014 SP1, Compatibility Level 110 |

# WEB SERVER

| 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* | |

| OPERATING SYSTEM | IIS APP POOL |
| --- | --- |
| Minimum System Requirements | |
| Processor: 2.0 GHz and 4 cores or faster | |
| 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. | |

*= varies per EMS Software Application

# WEB APPLICATION REQUIREMENTS

| DESKTOP BROWSER |
| --- |
| Internet Explorer 11 (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 the EMS 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 |

# EMS FOR OUTLOOK 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 |

| OPERATING SYSTEM | IIS |
|---|---|
| Application Pool | 4.0 |
| **Prerequisites** | |
| HTTPPlatformHandler IIS Module | Download Version 1.2 here OR download the installer see here. |
| PowerShell | 5+ Version |
| ASP.NET Version 4.6 | Under Web Server (IIS)->Web Server->Application Development:<br>» ISAPI Extensions<br>» ISAPI Filters<br>» .NET Extensibility 4.6 |

# EMS INTEGRATION FOR EXCHANGE

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

Exchange Web Services (EWS) impersonation

# CHAPTER 4: Obtain the Installation Files

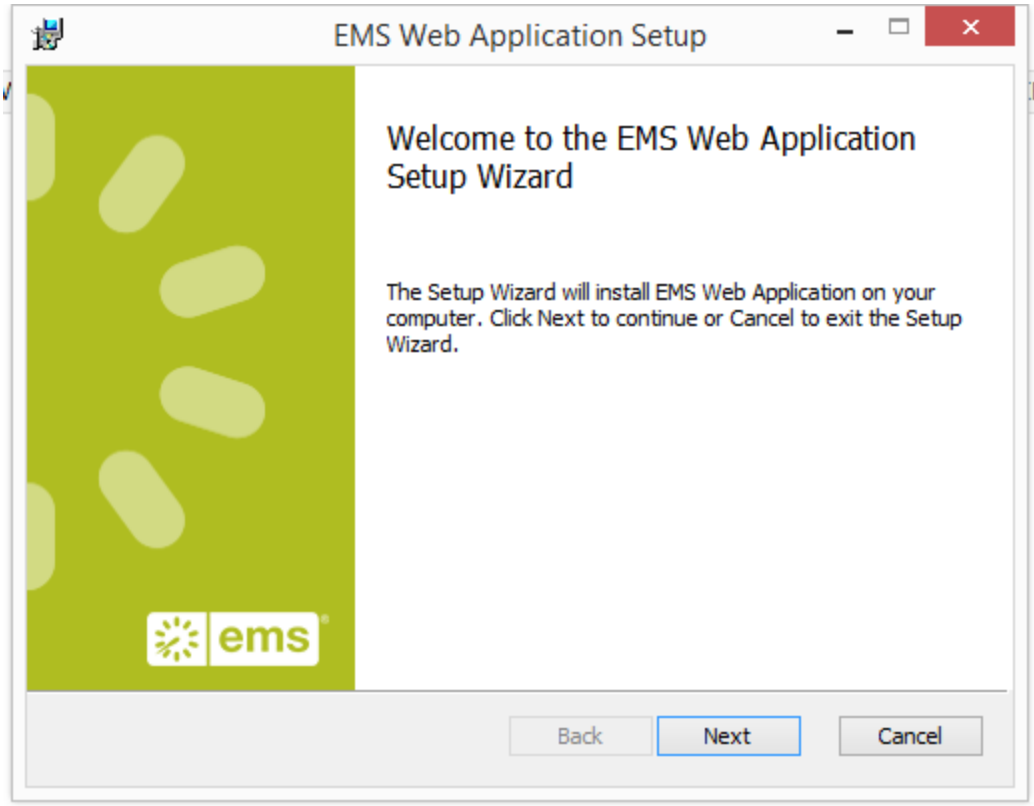
The latest release of EMS Web App can be downloaded from the online Support Center.

1. Log into the EMS Customer Portal.
2. Click the Software and Docs library link.
3. Click the 44.1 Releases & Patches link.
4. Download **EMSWebApplication.msi**. (Required for both first time installations and upgrades.)

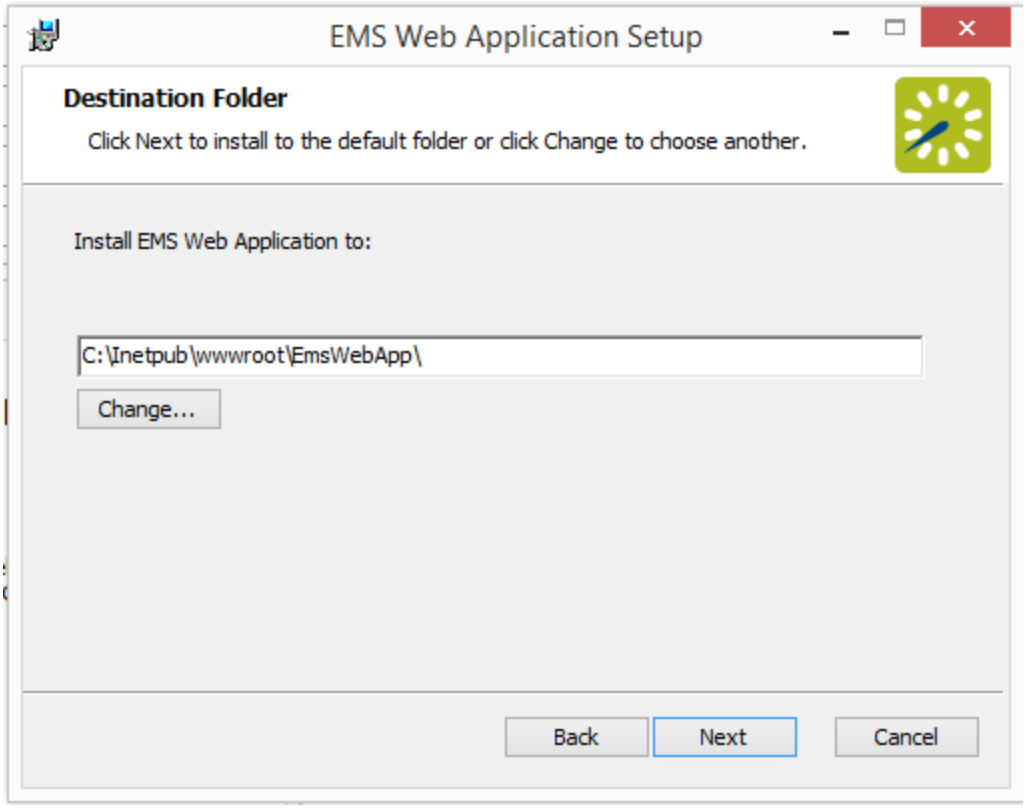
# CHAPTER 5: Install or Upgrade to the EMS Web App

1. Manually **uninstall** any previous versions of VEMS or EMS Web App on your web server.
2. Verify that Requirements and Prerequisites have been met.
3. Download the **EMSWebApplication.msi** file onto the web server that will be running EMS Web App.
4. Run **EMSWebApplication.msi**.
5. The first screen welcomes you to the EMS Web App Setup Wizard. Click **Next** to

begin the installation process.



6. In the Destination Folder screen, select the destination folder.




The installation process will create a new physical directory on your web server based on the destination folder path you entered. Click **Next**.

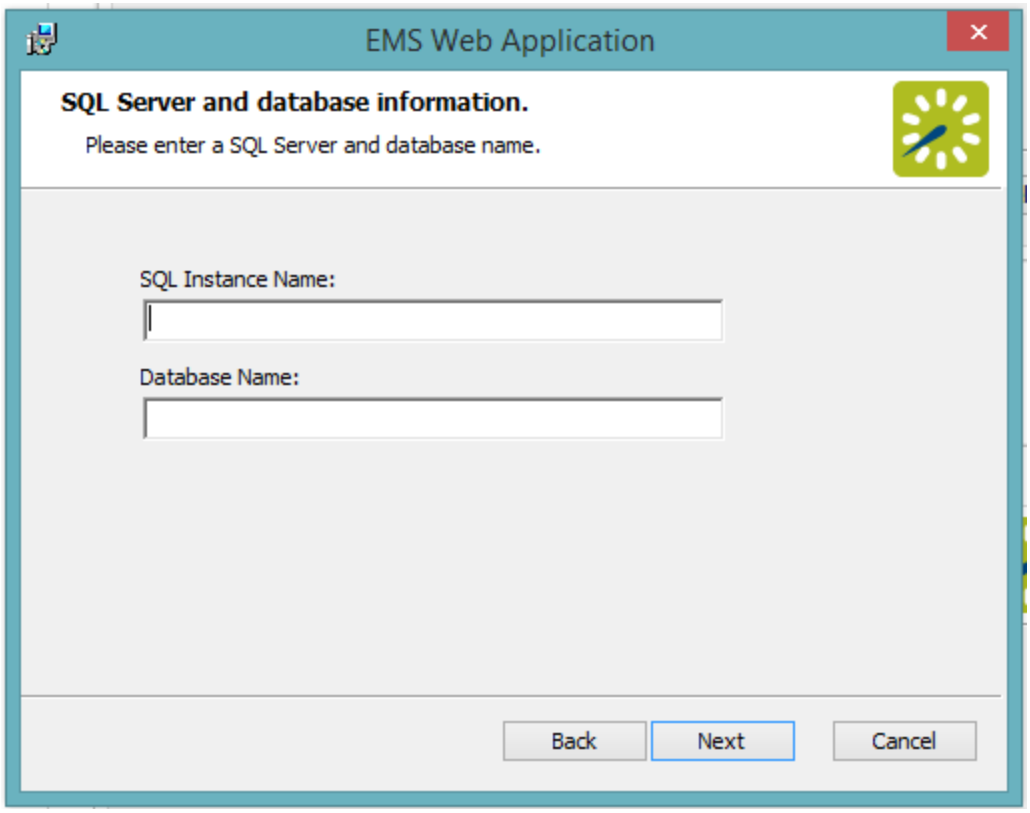
> Tip: Choosing a folder above other than the default will create a new physical directory on your web server at that location. If your

> organization uses Internet Information Services (IIS), make sure that the user account used for IIS (IUSR and/or IIS_IUSRS) has access to this new installation directory. To learn more, see Windows Server 2008/2008 R2 Web Server Setup Guide or Windows Server 2012/2012 R2 Web Server Setup Guide.

> Note: EMS Web App should **not** be installed in the same physical directory as other EMS web-based products OR under a site running another version of VEMS or EMS Web App.

7. In the SQL Server and database information screen that appears, enter your SQL Instance Name and your Database Name and click **Next**.

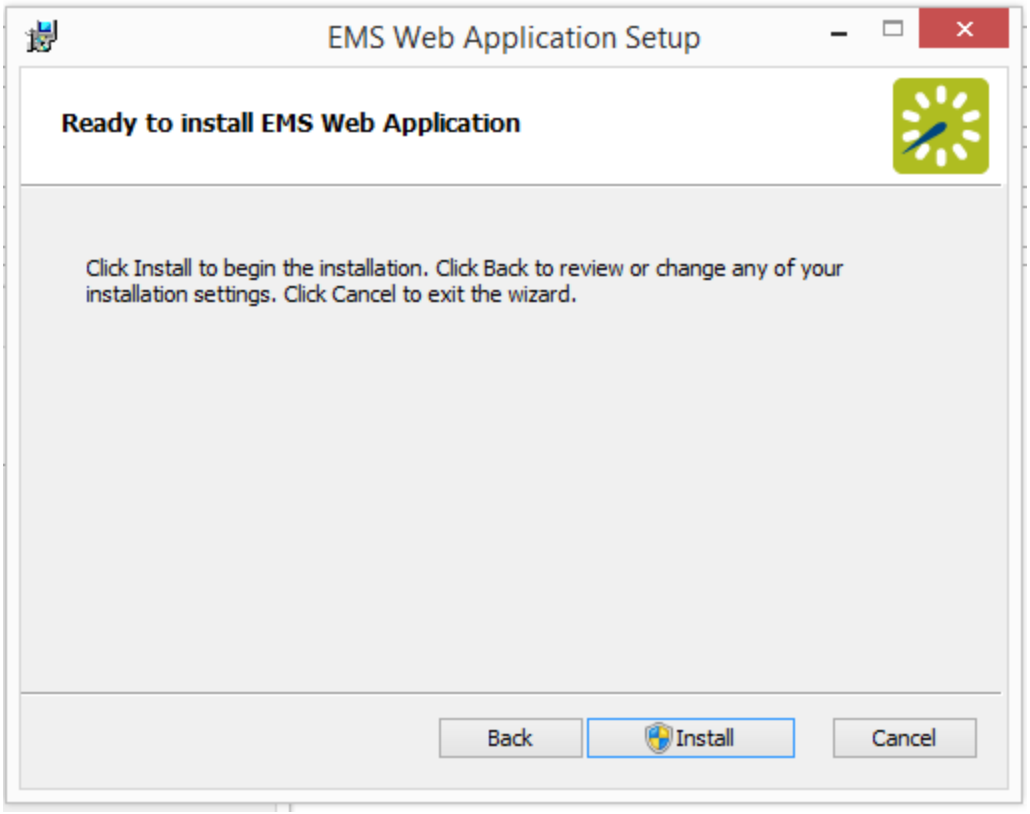
> Tip: The database name is typically “EMS.”




8. In the Virtual Directory information screen that appears, the Virtual Directory Name will default to the destination folder you specified (in Step 6 above). 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 ("EmsWebApp" in the example above). Click **Next**.

Warning: EMS Web App should not be installed in the same virtual directory as other EMS web-based products OR under a site running another version of EMS Web App.

9. On the Ready to install EMS Web Application screen that appears, click **Install**.




10. On the Completed the EMS Web App Setup Wizard screen that appears, click **Finish**.

# CHAPTER 6: Upgrade Considerations

When planning to upgrade from previous versions of VEMS to the new EMS Web App, you should take the new features, functionality, and default settings into consideration. Please encourage users at your facility to review What's New before they begin working with the new version of the software. Doing so will streamline the adoption of the new release and help your users benefit from new features and functions that they might not otherwise discover.

This topic provides information on the following:


- Time Zone Settings
- Best Practices
- Configuration and Parameter Settings
- Web Menus
- Functional Changes
- Help Text Records
- CSS (Style) Settings
- Language Translation
- All Other Customizations

# TIME ZONE SETTINGS

Web Users should be assigned to a time zone for an optimal experience.

# BEST PRACTICES

Display settings and other environmental factors greatly affect the performance of EMS Floorplan. For an optimal floorplan experience, please follow these Best Practices.

# CONFIGURATION AND PARAMETER SETTINGS

- Due to a change in product naming, you will need to update the name of the Exchange Integration Web Service URL parameter. See Also: EMS Web App System Parameters.
- For an optimal user-interface experience, we recommend keeping text-based fields and notes (e.g., Room Descriptions, Process Template Descriptions, Event Names, etc.) as brief as possible.
- New parameters have been introduced:
  - For organizations who direct everyday users to manually create their own accounts:
    - Sign Up Confirmation Email
    - Sign Up Success Email

- Request Received Email
- Password Reset Email
- Password Reset Success Email

- Default Home Page of Site Home or My Home (My Home is the default).
- Show Infographics on My Home (No is the default).
- Default Cancel Reason

- Some parameters have been updated:
  - Default Account Status for Newly-Created User (formerly Security Status for User) - Options are Active or Pending. Inactive option has been removed.
  - Browse Events - Display Format - Reduced to Daily, Weekly, and Monthly options.
  - Setup Type Validation Rule - No longer affects room searching. Will still handle Setup Type display and validating attendance against capacties.
  - Allow Access to System Check Pages from Any Machine? - No longer applies to EMS Web App as SystemCheck.aspx has been removed for this application.
  - Default Value for Attendance - Default is now "1." Existing configurations of this parameter for any value other than "0" will not be affected upon upgrade.

- Some parameters have been removed for V44.1:
  - Note Label on Account Management - Field is no longer exposed to the every-day user.
  - Number of Hours to Show on Browse for Space - No longer applicable.

- Maximum Number of Events/Day to Display - No longer applicable. Maximums now set per view (Daily, Weekly, or Monthly).
- Secondary Event Sort (After Date/Time) - No longer applicable. All columns are sortable.
- Devices to redirect to mobile site - No longer applicable as EMS Web App is now mobile-responsive.
- Display Areas as Filter - Areas are incorporated into Locations for searching.
- Allow User to Change Setup Count in Selected Locations Area - Permanently enabled as part of the new UX design.

# WEB MENUS

- **All custom menus should be reviewed and updated/removed prior to updating in a live environment.**
- Custom menus can be parented under the Links or Help icon (for organization-specific help pages). Upgrading will re-parent all custom menus under Links.
- Process templates can be sequenced under Create a Reservation menu but can no longer be moved to different menus.
- Due to the new UI design, system-generated menus cannot be re-sequenced or relabeled, and you cannot modify their URLs.

# FUNCTIONAL CHANGES

The following changes will show in your new installation due to the new UI design:

- The EMS Web App has been made mobile-responsive. Therefore, mobile-specific pages such as MobileLogin.aspx have been removed. Everyday users can instead access mobile-responsive versions of the same pages used when accessing the EMS Web App on a desktop machine.
- New Validated checkbox for everyday users:
  - Only applies to manual authentication creation and approval process, but check-box appears for all users regardless.
  - Will be automatically selected for new users created in the EMS desktop client and via EMS Human Resources Toolkit.
  - New EMS Human Resources Toolkit installations will have the Validated checkbox included in update logic.
- For tighter security, the SystemCheck.aspx page and the Ctrl+Shift+U keystroke shortcut to access SystemCheck.aspx have been removed for the EMS Web App. Some information previously included on SystemCheck.aspx has been relocated to options within the Web Administrator menu of the EMS Web App:
  - Clear Cache option
  - License information
  - Server and database connection string

- Error Log Files
- Application version and information (relocated to the About page)

- Services, videoconferencing, and reservation management will not be available on the mobile version of the EMS Web App nor on the EMS Mobile App.
- Template personalization will be automatically enabled for all process templates, which means that users will be able to set favorite templates to streamline navigation during the booking process. Favorite templates, for example, will be listed in a dropdown when the user begins booking space.
- For organizations using the optional Floor Map module, the SVG file format is no longer supported for floor map icons/images.

# HELP TEXT RECORDS

- **All help text records should be reviewed and updated/removed prior to updating in a live environment.**
- Home page web text records will now belong under Site Home and can differ for unauthenticated users vs. authenticated users.
- For organizations who direct everyday users to manually create their own accounts, a new text record for Terms of Use has been introduced.
- Some help text records have been removed (listed alphabetically by the database value LookupKey for tblWebText):
  - MenuItem
  - VEMSAccountManagementHelp
  - VEMSAddBookingHelpPopup

- VEMS_BadBrowserHelp
- VEMSBillingReferenceLookupHelp
- VEMSClassicRequestPopup
- VEMSEditAccountHelp
- VEMSEditBookingHelpPopup
- VEMSGroupLookupOnPage
- VEMSLdapConfigurationHelp
- VEMSLoginHelp
- VEMSLoginPageMainContent
- VEMSLogoutPageMainContent
- VEMSLogoutScreenMessage
- VEMSMissingOrInvalidExpectedQuerystring
- VEMSPONumberLookupHelp
- VEMSReservationDetailsHelp
- VEMSReservationRecurrenceHelp
- VEMSReservationSummaryCheckInSuccess
- VEMSReservationSummaryCheckInUnavailable
- VEMSRoomRequestHelpPopup
- VEMSUDFDetailsHelp
- VEMSUserPersonalizationHelp

- Application title help record only applies to Default.aspx (HTML not recommended for this page).

# CSS (STYLE) SETTINGS

- **All custom CSS should be reviewed and updated/removed prior to upgrading in a live environment.**
- Custom.CSS now saved under EMSWebApp/Content/Custom/Custom.CSS instead of the Styles folder.

# LANGUAGE TRANSLATION

- Language translation is still supported, but administrators should review the new site design to apply new translations where necessary.

# ALL OTHER CUSTOMIZATIONS

- **Any custom logos, custom JavaScript, and all other customizations should be reviewed and updated/removed prior to updating in a live environment.**

# CHAPTER 7: Optional EMS Web App Features

If you currently do not own one of optional, separately-licensed modules outlined below, but are interested in more information, please contact your Account Executive.

## INTEGRATED AUTHENTICATION

The Integrated Authentication module is a component for EMS Web App that provides single-sign-on capability using Integrated Windows Authentication, your organization's portal or LDAP. See Also: Integrated Authentication Configuration Instructions for installation instructions.

## INTEGRATION WITH MICROSOFT® EXCHANGE

Integration with Exchange is a component for EMS Web App that integrates with Exchange. With this module, web users can view the availability of both meeting rooms and attendees, and send Outlook-compatible meeting invitations–all from within EMS Web App. See Also: Integration to Microsoft Exchange for installation instructions.

# FLOOR PLANS

EMS Floor Plans allows web users to search for, view and reserve available space from an interactive floor plan within EMS Web App. Floor plans and associated available/unavailable indicator images are configured in the EMS Desktop Client. See Also: Floor Plan Module Installation Instructions.

# CHAPTER 8: Customize EMS Web App

After you have installed the EMS Web App, you can customize many aspects of it. You can change the *look and feel* of the EMS Web App by inserting your own logo. Experienced web developers can also modify the system's style sheet to change fonts and colors.

> **IMPORTANT:** Do not alter any of the EMS Web App web page files themselves. **THE MAINTENANCE AGREEMENT FOR EMS WEB APP EXTENDS TO THE ORIGINAL PAGE CONTENT ONLY.**

This topic provides information on the following:


- Customize the Logo
- Customize Style Sheets
- Customize Links
- Customize JavaScript

# CUSTOMIZE THE LOGO

The logo that appears in the upper left corner of all pages within the EMS Web App comes from a file named LOGO.GIF found in the \EMSWebApp\Images folder of the web server. If you choose to have the system display a different logo, create a new file called CUSTOMLOGO in the same folder (any graphics file type, such as .gif, .png, etc. will suffice). If the system detects CUSTOMLOGO, the system will use that file rather than the default LOGO.GIF file. The advantage of creating the new file instead of simply replacing the LOGO.GIF file is that, in an upgrade to a new version of EMS Web App, the LOGO.GIF file is overwritten whereas CUSTOMLOGO is not. If you create a custom logo file, you may need clear your browser's cache before you see the new image.

> **TIP:** Be sure to maintain the aspect ratio of 135px wide X 40px high.The system will accept nearly any size logo image, but you should avoid images more than 200 pixels wide and images that are too tall to avoid extra scrolling.

# CUSTOMIZE STYLE SHEETS

Experienced web developers are can modify the look and feel of EMS Web App using a custom style sheet, which controls fonts and colors throughout the

application. To do so:

1. Create EMSWebApp/Content/Custom folder on your web server.
2. Name your custom style sheet CUSTOM.CSS and place it in the EMSWebApp/Content/Custom folder. If the system detects this file, it will use the styles found there rather than those in the system's default style sheet, VEMS.CSS. The advantage of creating the new file instead of overwriting the default file is that, in an upgrade to a new version of EMS Web App, VEMS.CSS is overwritten whereas CUSTOM.CSS is not.

## CUSTOMIZE LINKS

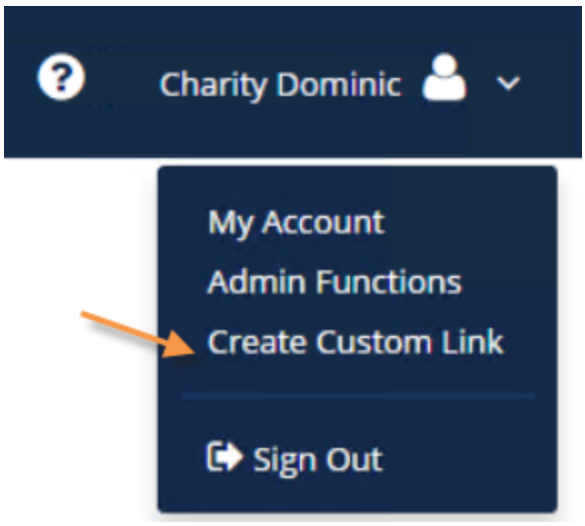
The EMS Web App Browse Events page allows users to view all events scheduled in EMS that display to everyday users. You have the option to automatically filter this list of events by facility, room, event type, event name or group name as part of a customized Browse Events page. This customized page is referred to as a Custom Link.

> **TIP:** A Custom Link enables you to build a link based on the Browse Events page that will display only events meeting your specified criteria. For example, you can create a link that only displays events in a specific Building or of a specific Event Type. Essentially, the link pre-filters the event listing

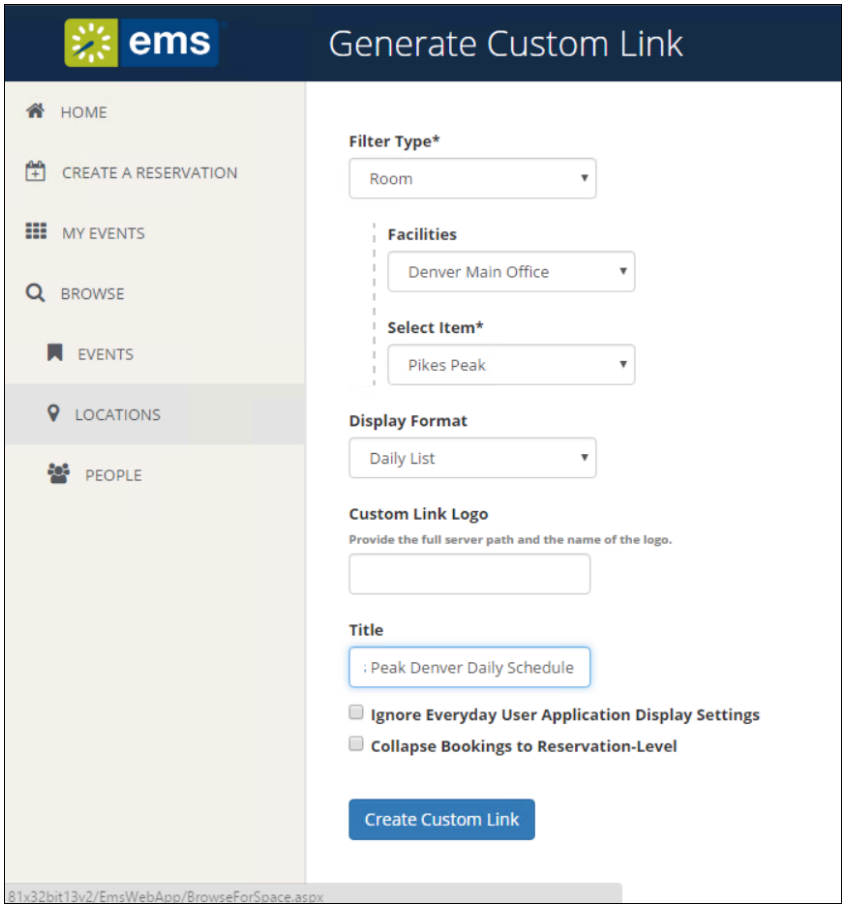
displayed to a specific building, event type, Group, etc. Once you generate the link, then you can insert it in emails or websites.

To create a Custom Link, follow the steps outlined below.

1. Log into EMS Web App using a user ID that belongs to a Everyday User Security Template containing the Web Administrator Role. For information on how to configure a user and/or Everyday User Security Template, see Configure Everyday Users and Configure Security Templates.
2. Under the dropdown menu next to your name, click **Create Custom Link**.



3. Specify the pre-filters that will control what displays when users click your custom link.




**TIPS:** To display a custom logo other than the default logo used for your EMS Web App site, enter the logo filename and server path in the

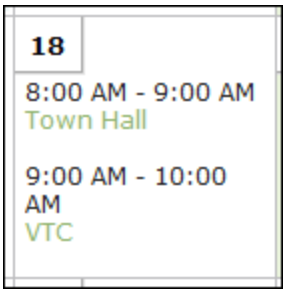
Logo field. The logo needs to be stored in the EMS Web App physical directory on your web server (typically, C:\inetpub\wwwroot\EMSWebApp\).

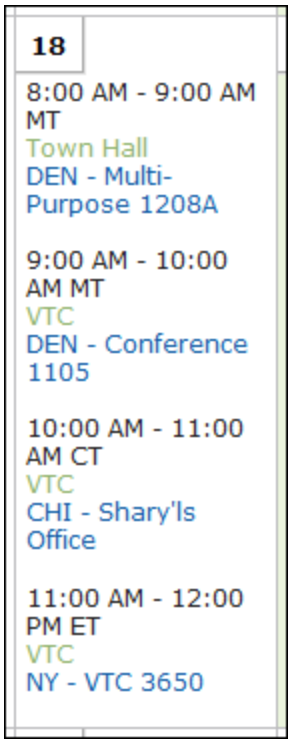
Select the **IGNORE EVERYDAY USER APPLICATION DISPLAY SETTINGS** option if you want all events within your criteria to display to users using this link regardless of everyday user display settings (essentially, ignoring configuration rules that would normally hide certain events from view).

Select the **COLLAPSE BOOKINGS TO RESERVATION-LEVEL** option to collapse booking information so that only the reservation information shows.

***Collapse Bookings to Reservation Level Enabled***

***Collapse Bookings to Reservation Level Disabled***




4. Click the **Generate Link** button to display a friendly URL and HTML code that can be added to a web page, email, etc. The URL can also be used to test your Custom Link.

# CUSTOMIZE JAVASCRIPT

With custom JavaScript, you can extend the functionality of EMS Web App to suit your business needs.

> **WARNING:** Including custom JavaScript on EMS Web App pages can affect performance.

When EMS Web App receives a request for a page, it checks for the existence of a CustomJs folder. If the folder exists, EMS Web App checks for any files that match the name of the page. For instance, on the RoomRequest.aspx page, if there is a file called RoomRequest.js in the CustomJs folder, EMS Web App will include the RoomRequest.js file on the page.

In addition to the name-matched file, EMS Web App will also check for and include the file named global.js on EVERY page.

Perform the following steps to enable Custom JavaScript:

1. Enable Custom JavaScript.
2. Open the EMS Web App web.config file (typically, C:\inet-pub\wwwroot\EMSWebApp\web.config).

   > **TIP FOR EMS CLOUD CUSTOMERS:** Modifications to the web.config file must be performed by EMS Cloud Operations. To request these changes, please contact EMS Support.

3. Locate the following node under the <appSettings> node:

   ```
   <add key="allowCustomJs" value="false" />
   ```

4. Change the false value to true.
5. Save the file.
6. Create the CustomJs folder within the root of your EMS Web App Install Directory (typically, C:\inetpub\wwwroot\EMSWebApp\CustomJs).

You are now ready to implement your Custom JavaScript using one of several options:

- In the newly-created CustomJs folder, create a file for each of the above pages you wish to include your custom JavaScript on (such as RoomRequest.js, EditReservation.js, or Default.js).
- In the newly-created CustomJs folder, create one file called global.js that will be included on every page in the system.

Your custom JavaScript should be included on global.js **or** on each of the applicable page-specific JavaScript files.

> **WARNING:** If you include the script in both places, it could cause problems.

# 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 9: EMS Mobile Web Application

The EMS Web App also runs on a mobile device such as a tablet or handheld. Due to the smaller screen size and resolution of tablets and smartphones, pages may display differently but most of the same functionality is still available.

EMS Mobile App, by contrast, is an app designed specifically for smartphones. It offers functionality specifically for everyday users who need access to EMS while they're on the go. The EMS Mobile App also runs on tablets that run iOS or Android, but the screen layout is optimized for smartphones and does not take advantage of larger displays.

See Also: Web App Installation Guide and Web App Configuration Guide.

# CHAPTER 10: Launch EMS Web App

1. After obtaining the latest version of EMS Web App, verify your installation by opening a browser and entering the EMS Web App address:

   http://[ServerName]/WebApp/

   (replace [ServerName] with the name of your web server)

   The format above assumes you used the default values at installation.

2. The first time you launch EMS Web App, it may take a few extra moments for the website to display. If you encounter any issues, please contact Customer Support for assistance.
3. For information on how to configure EMS Web App, please refer to EMS Desktop Client Configuration Guide.

# CHAPTER 11: Windows Server 2008/2008 R2 Web Server Setup Guide

Follow this guide to install EMS on a new web server, to support EMS web applications such as EMS Web App, VEMS, EMS for Outlook, and EMS Mobile App.


- Best Practices: Setting Up Your Web Server 2008 or 2008 R2
- Install .NET Framework 2008
- Install Internet Information Services (IIS)
  - Add Role Services

# CHAPTER 12: Best Practices: Setting Up Your Web Server 2008 or 2008 R2

This section guides you in best practices in setting up a Web Server for installation of EMS web-based products and is intended for experienced System Administrators. Please be aware that we can only provide instructions for modifying your web server as tested in our facilities, and cannot guarantee results for your configuration. Lastly, after completing these modifications, you will need to perform your own adjustments to system security etc.

For information on Web Server 2012, see Best Practices: Setting Up Your Web Server 2012 or 2012 R2.

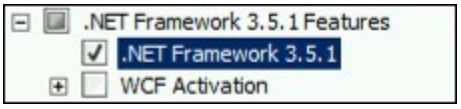
> Note: Before beginning the installation process, please review EMS System Requirements before proceeding. The minimum hardware requirements must be met to continue with the configuration below. Administrative rights will be necessary to enable the roles and features listed for each Windows Server.

This topic provides information on the following:


- To Install .NET Framework 3.5
- To Install .NET Framework 4.5: Regics Only
- To Install Internet Information Services (IIS)
  - To Add Role Services


# TO INSTALL .NET FRAMEWORK 3.5

1. Navigate to Start > All Programs > Administrative Tools > Server Manager.
2. In the Server Manager interface, click Features to view all the installed Features in the right pane.
3. In the Server Manager interface, select Add Features to lists possible features.
4. In the Select Features interface, expand .NET Framework 3.5.1 Features.
5. Once expanded, select .NET Framework 3.5.1 and click Next.




6. In the Confirm Installation Selections interface, review the selections, then click Install.
7. Once the installation process completes, click Close.

# TO INSTALL .NET FRAMEWORK 4.5: REGICS ONLY

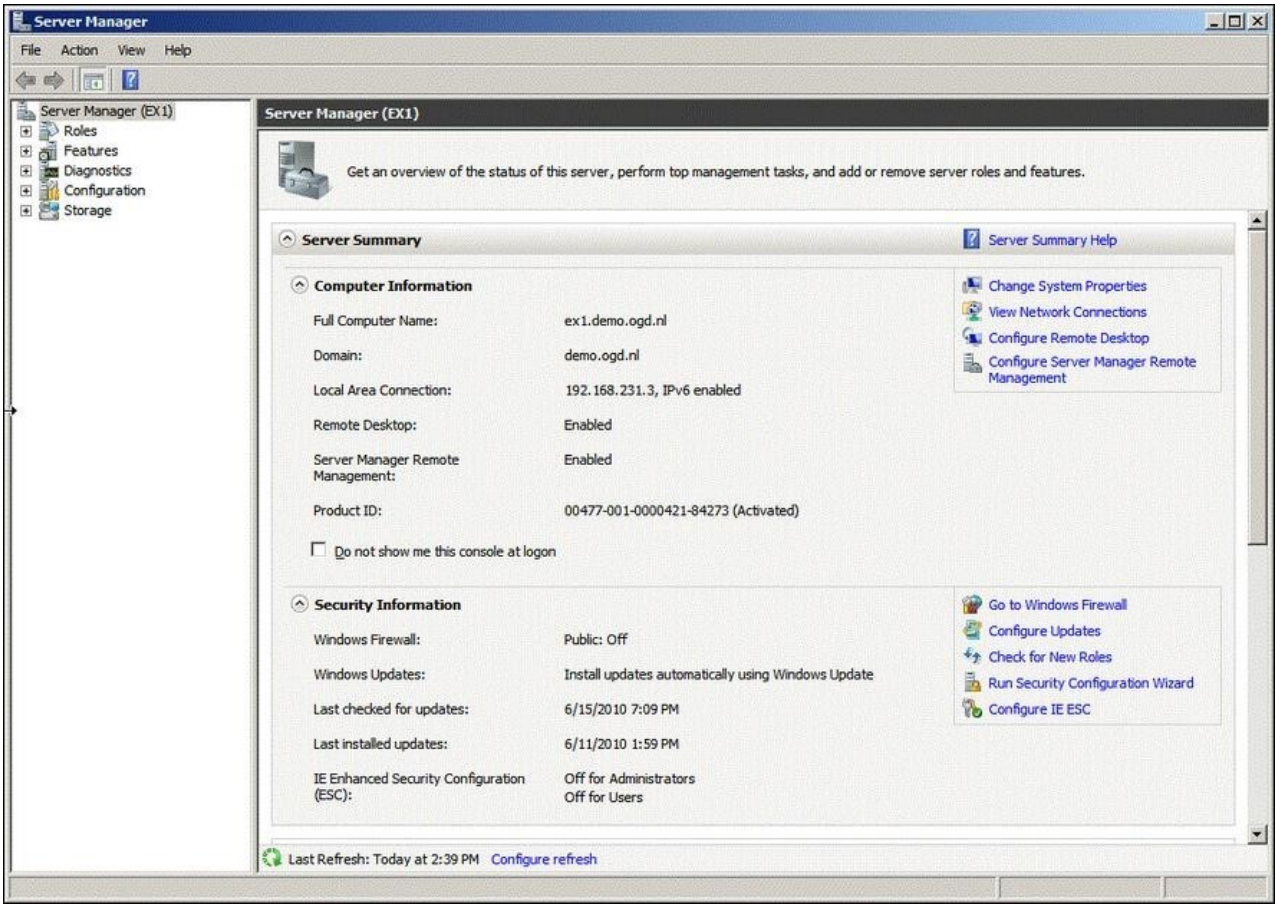
Windows Server 2008/2008 R2 does not have a built-in option to install .NET Framework 4.5. In order to install .NET Framework 4.5, the Server Administrator will need to download the following redistributable to the server and install it following the instructions.

Microsoft® .NET Framework 4.5

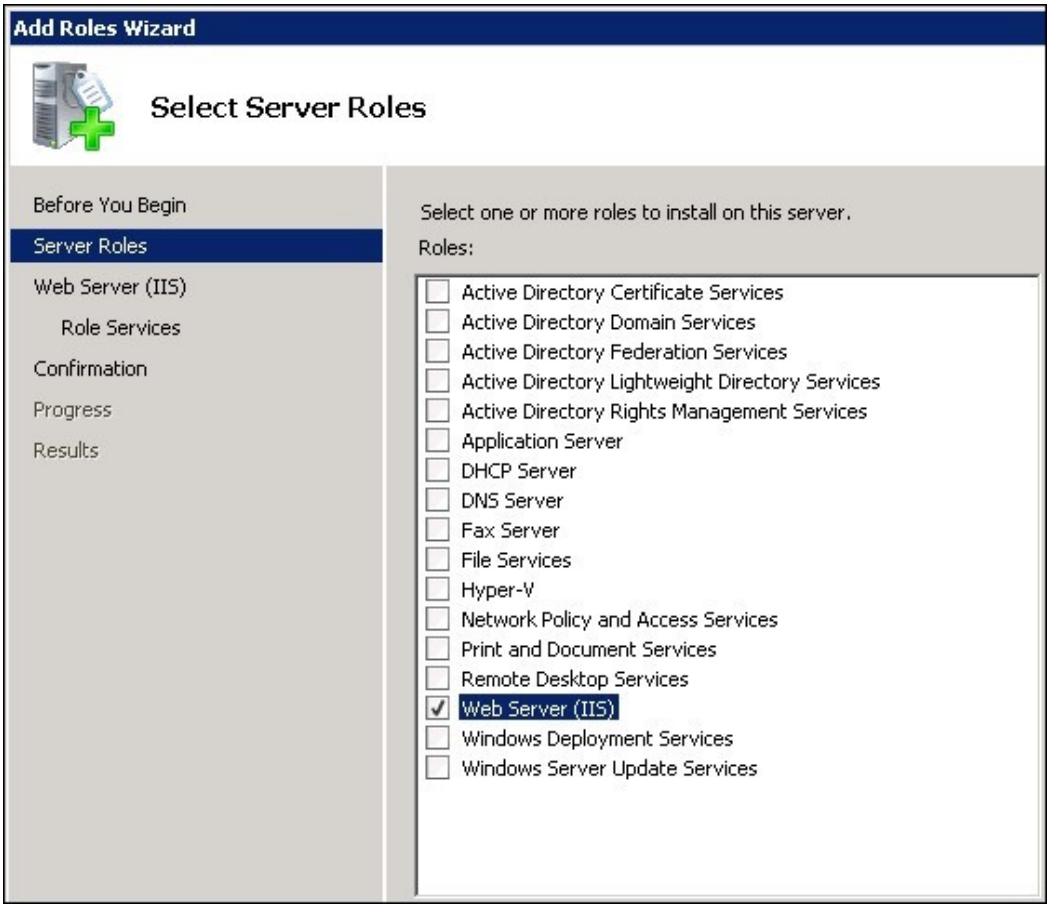
# TO INSTALL INTERNET INFORMATION SERVICES (IIS)

To install IIS on a Windows Server 2008, follow the instructions below.

1. Navigate to Start > All Programs > Administrative Tools > Server Manager.




2. In the Server Manager window, scroll down to Roles Summary, and then click Add Roles.
3. Select Web Server (IIS) on the Select Server Roles page. An introductory page will open with links for further information.
    a. The Web Server (IIS) role in Windows Server 2012 provides a secure, easy-to-manage, modular and extensible platform for reliably hosting websites, services, and applications.




## TO ADD ROLE SERVICES

When adding IIS using the Add Roles Wizard, only the default installation is executed, which has a minimum set of role services. For EMS products, it is necessary to add role services for the programs to function properly. If role services are added after installing IIS, the Server Administrator will need to navigate to the Role Services page by following the above directions and then clicking Next.

Select the following IIS Role Services to be installed:

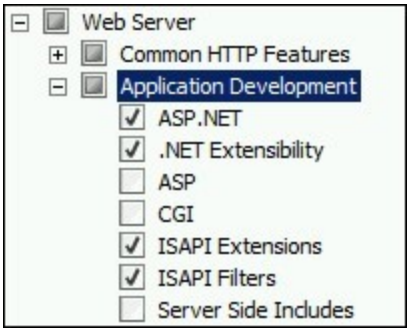
- Common HTTP Features
- Application Development
- Health and Diagnostics
- Security
- Performance
- Management Tools

## COMMON HTTP FEATURES

1. Static Content – Static Content lets the Web server publish static Web file formats, such as HTML pages and image files. Use Static Content to publish files on a Web server that users can then view using a Web browser.
2. Default Document – Default Document lets organizations configure a default file for the Web server to return when users do not specify a file in a URL. Default documents make it easier and more convenient for users to reach an organizations Web site.

3. Directory Browsing – Directory Browsing lets users see the contents of a directory on a Web server. Use Directory Browsing to enable an automatically generated list of all directories and files available in a directory when users do not specify a file in a URL and default documents are either disabled or not configured.
4. HTTP Errors – HTTP Errors lets organizations customize the error messages returned to users' browsers when the Web server detects a fault condition. Use HTTP errors to give users a better user experience when they run up against an error message. Consider providing users with an e-mail address for staff who can help them resolve the error.

## APPLICATION DEVELOPMENT

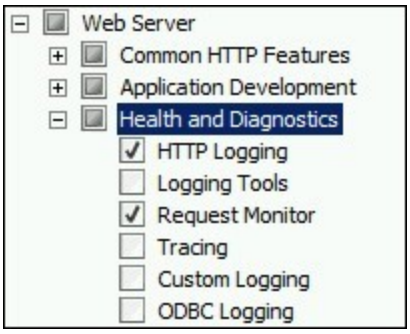



1. **ASP.NET** – ASP.NET provides a server side object-oriented programming environment for building Web sites and Web applications that use managed code. ASP.NET is not just a new version of ASP. ASP.NET provides a robust infrastructure for building Web applications, and it has been completely re-architected to provide a highly productive programming experience based on the .NET

Framework.

2. **.NET Extensibility** – .NET Extensibility lets managed code developers change, add, and extend Web server functionality in the request pipeline, the configuration, and the UI. Developers can use the familiar ASP.NET extensibility model and rich .NET APIs to build Web Server features that are just as powerful as those written using the native C++ APIs.
3. **ISAPI Extensions** – Internet Server Application Programming Interface (ISAPI) Extensions provides support for dynamic Web content development using ISAPI extensions. An ISAPI extension runs when requested, just like any other static HTML file or dynamic ASP file. Since ISAPI applications are compiled code, they are processed much faster than ASP files or files that call COM+ components.
4. **ISAPI Filters** – Internet Server Application Programming Interface (ISAPI) Filters provides support for Web applications that use ISAPI filters. ISAPI filters are files that can extend or change the functionality provided by IIS. An ISAPI filter reviews every request made to the Web server, until the filter finds one that it needs to process.

## HEALTH AND DIAGNOSTICS

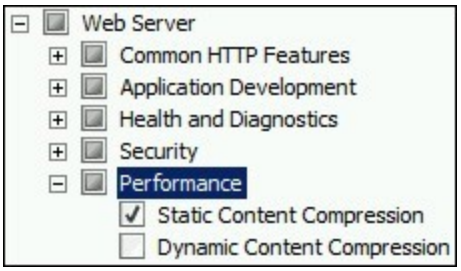



1. **HTTP Logging** – HTTP Logging provides logs site activity for this server. When a loggable event (usually an HTTP transaction) occurs, IIS calls the selected logging module, which then writes to one of the logs stored in the file system of the Web server. These logs are kept in addition to those provided by the operating system.
2. **Request Monitoring** – Request Monitor provides infrastructure to monitor Web application health by capturing information about HTTP requests in an IIS worker process. Administrators and developers can use Request Monitor to understand which HTTP requests are executing in a worker process when the worker process has become unresponsive or very slow.

## SECURITY

1. **Windows Authentication** – Windows Authentication is a low cost authentication solution for internal Web sites. This authentication scheme allows administrators in a Windows domain to take advantage of the domain infrastructure for authenticating users. Do not use Windows authentication if users who must be authenticated access an organizations Web site from behind firewalls and proxy servers.
2. **Request Filtering** – Request Filtering screens all incoming requests to the server and filters these requests based on rules set by the administrator. Many malicious attacks share common characteristics, such as very long URLs, or requests for an unusual action. Filtering requests, can attempt to reduce the impact of these types of attacks.

## PERFORMANCE




3. **Static Content Compression** – Static Content Compression provides infrastructure to configure HTTP compression of static content. This provides more efficient use of bandwidth. Unlike dynamic responses, compressed static responses can be cached without degrading CPU resources.

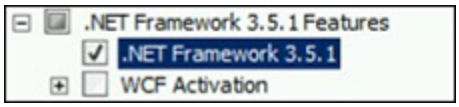
## MANAGEMENT TOOLS

4. **IIS Management Console** – IIS Manager provides infrastructure to manage IIS by using a graphical user interface. IIS Manager can be used to manage a local or remote Web server that runs IIS.

# CHAPTER 13: Install .NET Framework 2008

## INSTALL .NET FRAMEWORK 3.5

1. Navigate to **Start** > **All Programs** > **Administrative Tools** > **Server Manager**.
2. In the Server Manager interface, click **Features** to display all the installed Features in the right pane.
3. In the Server Manager interface, select **Add Features** to displays a list of possible features.
4. In the Select Features interface, expand **.NET Framework 3.5.1 Features**.




5. Check the box next to **.NET Framework 3.5.1** and click **Next**.
6. In the Confirm Installation Selections interface, review the selections and then click **Install**.
7. Allow the installation process to complete and then click **Close**.

# INSTALL .NET FRAMEWORK 4.5: REGICS ONLY

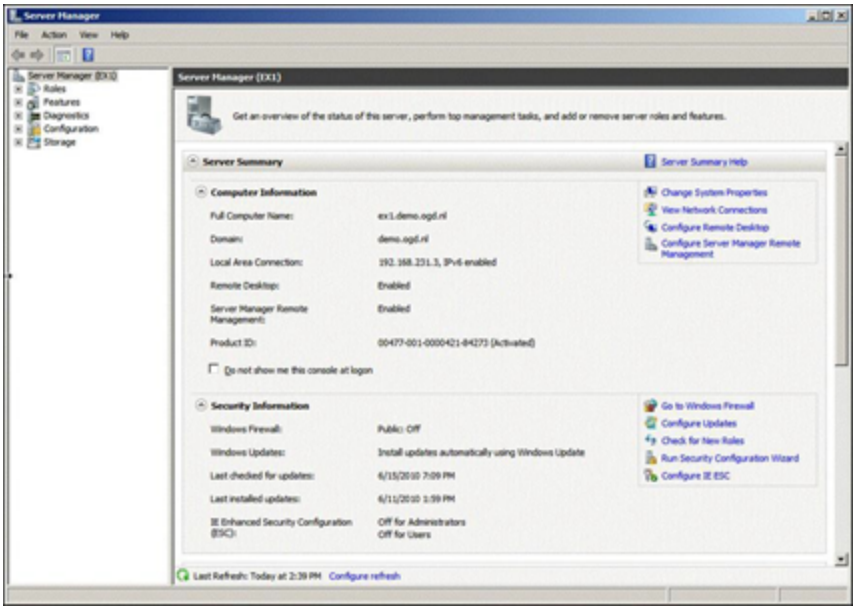
Windows Server 2008/2008 R2 does not have a built in way to install .NET Framework 4.5. To install .NET Framework 4.5, the server admin will need to download the following redistributable to the server and install it following the instructions.

Download Link: .NET Framework 4.5

# CHAPTER 14: Install Internet Information Services (IIS)

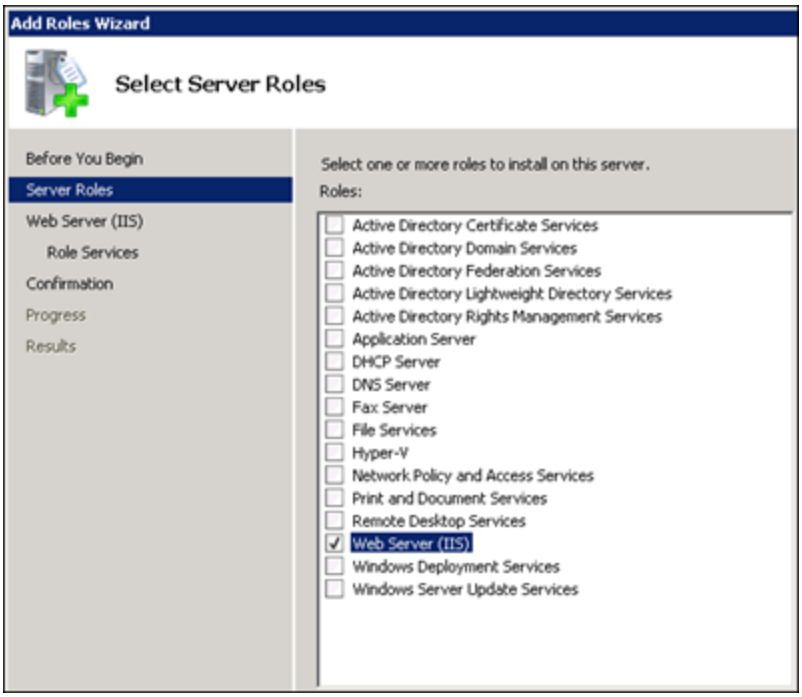
To install IIS on a Windows Server 2008 follow the instructions below.

1. Navigate to Start > All Programs > Administrative Tools > Server Manager.




2. In the Server Manager window, scroll down to Roles Summary, and then click Add Roles.
3. Select Web Server (IIS) on the Select Server Roles page. An introductory page will open with links for further information. The Web Server (IIS) role in Windows Server 2012 provides a secure, easy-to-manage, modular and extensible platform

for reliably hosting websites, services, and applications.



# CHAPTER 15: Add Role Services

When adding IIS using the Add Roles Wizard, only the default installation is executed, which has a minimum set of role services. For EMS products, it is necessary to add role services for the programs to function properly. If role services are added after installing IIS, the Server Administrator will need to navigate to the Role Services page by following the Install Internet Information Services (IIS) directions and then clicking **Next**.

Select the following IIS Role Services to be installed:

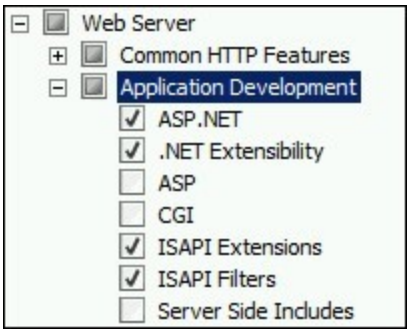
- Common HTTP Features
- Application Development
- Health and Diagnostics
- Security
- Performance
- Management Tools

# COMMON HTTP FEATURES

1. **Static Content** – Static Content lets the Web server publish static Web file formats, such as HTML pages and image files. Use Static Content to publish files on a Web server that users can then view using a Web browser.
2. **Default Document** – Default Document lets organizations configure a default file for the Web server to return when users do not specify a file in a URL. Default documents make it easier and more convenient for users to reach an organizations Web site.
3. **Directory Browsing** – Directory Browsing lets users see the contents of a directory on a Web server. Use Directory Browsing to enable an automatically generated list of all directories and files available in a directory when users do not specify a file in a URL and default documents are either disabled or not configured.
4. **HTTP Errors** – HTTP Errors lets organizations customize the error messages returned to users' browsers when the Web server detects a fault condition. Use HTTP errors to give users a better user experience when they run up against an

error message. Consider providing users with an e-mail address for staff who can help them resolve the error.

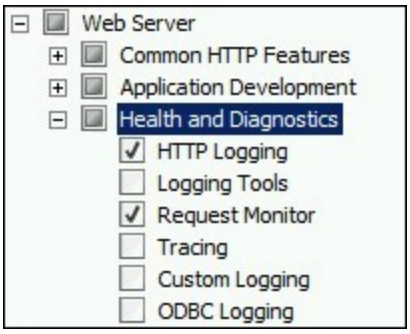
# APPLICATION DEVELOPMENT




1. **ASP.NET** – ASP.NET provides a server side object-oriented programming environment for building Web sites and Web applications that use managed code. ASP.NET is not just a new version of ASP. ASP.NET provides a robust infrastructure for building Web applications, and it has been completely re-architected to provide a highly productive programming experience based on the .NET Framework.
2. **.NET Extensibility** – .NET Extensibility lets managed code developers change, add, and extend Web server functionality in the request pipeline, the configuration, and the UI. Developers can use the familiar ASP.NET extensibility model and rich .NET APIs to build Web Server features that are just as powerful as those written using the native C++ APIs.

3. **ISAPI Extensions** – Internet Server Application Programming Interface (ISAPI) Extensions provides support for dynamic Web content development using ISAPI extensions. An ISAPI extension runs when requested, just like any other static HTML file or dynamic ASP file. Since ISAPI applications are compiled code, they are processed much faster than ASP files or files that call COM+ components.
4. **ISAPI Filters** – Internet Server Application Programming Interface (ISAPI) Filters provides support for Web applications that use ISAPI filters. ISAPI filters are files that can extend or change the functionality provided by IIS. An ISAPI filter reviews every request made to the Web server, until the filter finds one that it needs to process.

# HEALTH AND DIAGNOSTICS




1. **HTTP Logging** – HTTP Logging provides logs site activity for this server. When a loggable event (usually an HTTP transaction) occurs, IIS calls the selected logging module, which then writes to one of the logs stored in the file system of the

Web server. These logs are kept in addition to those provided by the operating system.

2. **Request Monitoring** – Request Monitor provides infrastructure to monitor Web application health by capturing information about HTTP requests in an IIS worker process. Administrators and developers can use Request Monitor to understand which HTTP requests are executing in a worker process when the worker process has become unresponsive or very slow.

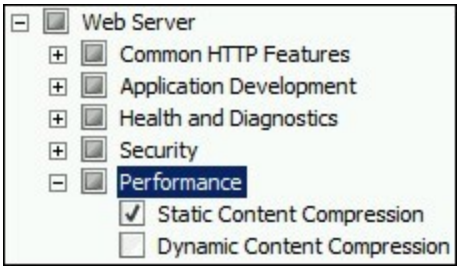
# SECURITY

1. **Windows Authentication** – Windows Authentication is a low cost authentication solution for internal Web sites. This authentication scheme allows administrators in a Windows domain to take advantage of the domain infrastructure for authenticating users. Do not use Windows authentication if users who must be

authenticated access an organizations Web site from behind firewalls and proxy servers.

2. **Request Filtering** – Request Filtering screens all incoming requests to the server and filters these requests based on rules set by the administrator. Many malicious attacks share common characteristics, such as very long URLs, or requests for an unusual action. Filtering requests, can attempt to reduce the impact of these types of attacks.

# PERFORMANCE




**Static Content Compression** – Static Content Compression provides infra-structure to configure HTTP compression of static content. This provides more efficient use of bandwidth. Unlike dynamic responses, compressed static responses can be cached without degrading CPU resources.

# MANAGEMENT TOOLS

**IIS Management Console** – IIS Manager provides infrastructure to manage IIS by using a graphical user interface. IIS Manager can be used to manage a local or remote Web server that runs IIS.

# CHAPTER 16: Windows Server 2012/2012 R2 Web Server Setup Guide

Follow this guide to install EMS on a new web server, to support EMS web applications such as EMS Web App, VEMS, EMS for Outlook, and EMS Mobile App.


- Best Practices: Setting Up Your Web Server 2012 or 2012 R2
- Install .NET Framework for Windows Server 2012/2012 R2
- Install Internet Information Services (IIS)
  - Add Role Services

# CHAPTER 17: Best Practices: Setting Up Your Web Server 2012 or 2012 R2

This section guides you in best practices in setting up a Web Server for installation of EMS web-based products and is intended for experienced System Administrators. Please be aware that we can only provide instructions for modifying your web server as tested in our facilities, and cannot guarantee results for your configuration. Lastly, after completing these modifications, you will need to perform your own adjustments to system security etc.

> Note: Before beginning the installation process, please review EMS System Requirements before proceeding. The minimum hardware requirements must be met to continue with the configuration below. Administrative rights will be necessary to enable the roles and features listed for each Windows Server.

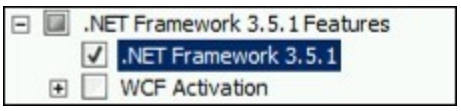
This topic provides information on the following:

» To Install .NET Framework 3.5
» To Install .NET Framework 4.5: Regics Only
» To Install Internet Information Services (IIS)
  » To Add Role Services

» Windows Server 2012/2012 R2
  » To Add Role Services

# TO INSTALL .NET FRAMEWORK 3.5

1. Navigate to **Start** > **All Programs** > **Administrative Tools** > **Server Manager**
2. In the Server Manager interface, click **Features** to view all the installed Features in the right pane.
3. In the Server Manager interface, select **Add Features** to lists possible features.
4. In the Select Features interface, expand **.NET Framework 3.5.1 Features**.
5. Once expanded, select **.NET Framework 3.5.1** and click **Next**.




6. In the Confirm Installation Selections interface, review the selections, then click **Install**.
7. Once the installation process completes, click **Close**.

# TO INSTALL .NET FRAMEWORK 4.5: REGICS ONLY

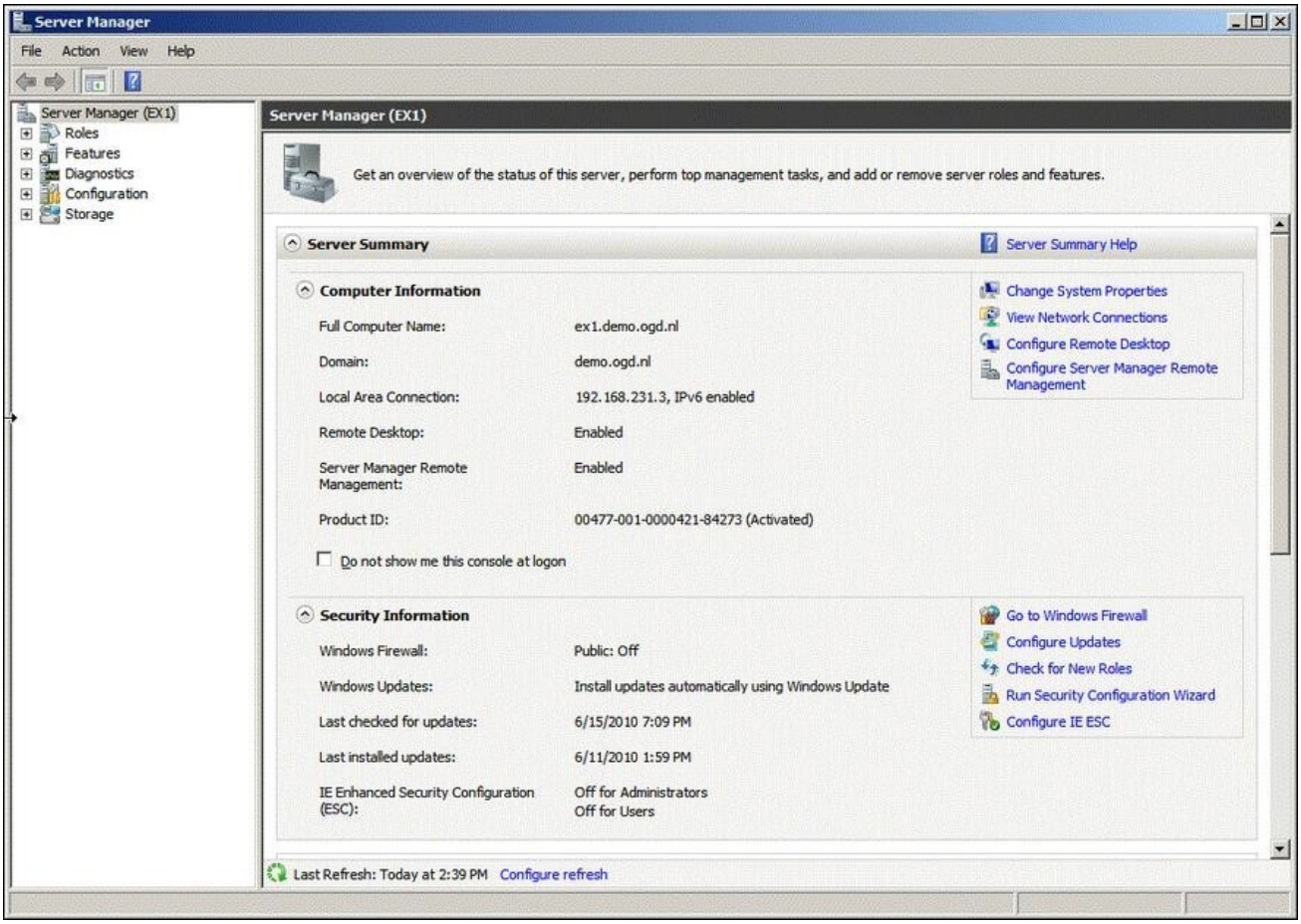
Windows Server 2008/2008 R2 does not have a built-in option to install .NET Framework 4.5. In order to install .NET Framework 4.5, the Server Administrator will need to download the following redistributable to the server and install it following the instructions.

.NET Framework 4.5

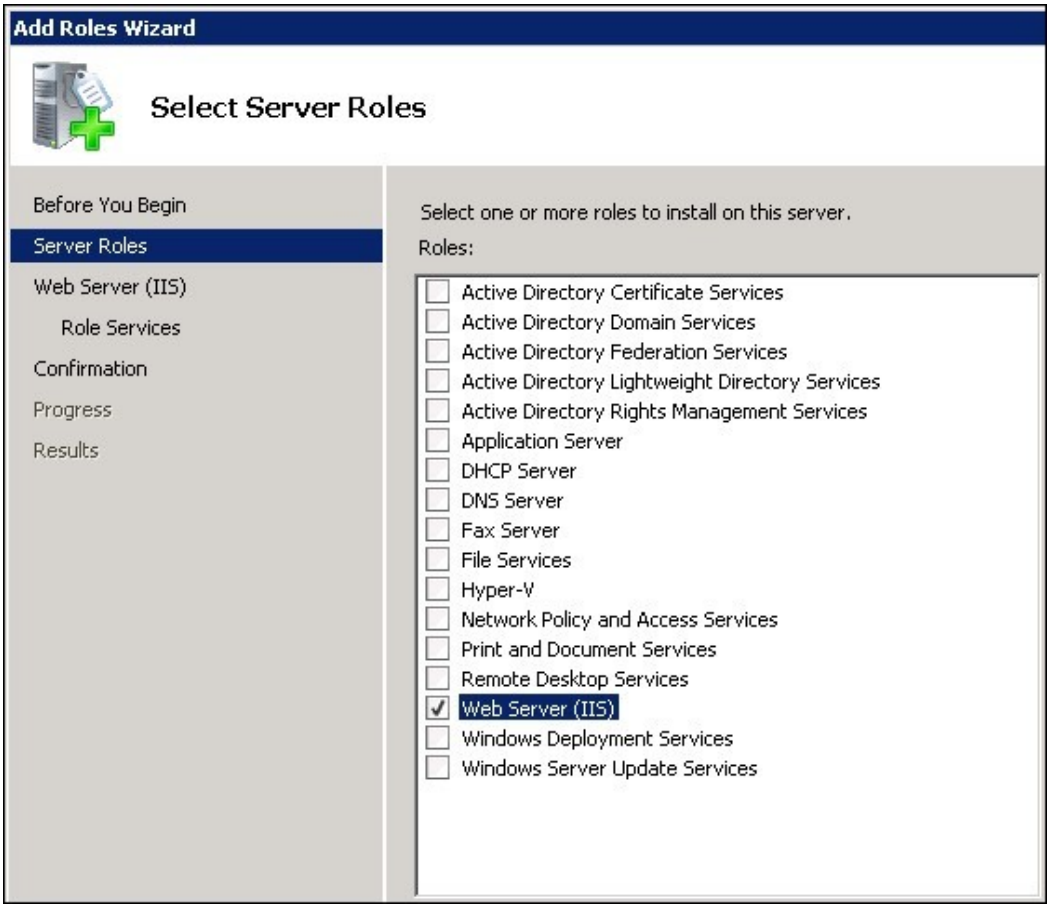
# TO INSTALL INTERNET INFORMATION SERVICES (IIS)

To install IIS on a Windows Server 2008, follow the instructions below.

1. Navigate to **Start** > **All Programs** > **Administrative Tools** > **Server Manager**.




2. In the Server Manager window, scroll down to **Roles Summary**, and then click **Add Roles**.
3. Select **Web Server (IIS)** on the Select Server Roles page. An introductory page will open with links for further information.
    a. The Web Server (IIS) role in Windows Server 2012 provides a secure, easy-to-manage, modular and extensible platform for reliably hosting websites, services, and applications.




## TO ADD ROLE SERVICES

When adding IIS using the Add Roles Wizard, only the default installation is executed, which has a minimum set of role services. For EMS products, it is necessary to add role services for the programs to function properly. If role services are added after installing IIS, the Server Administrator will need to navigate to the Role Services page by following the above directions and then clicking **Next**.

Select the following IIS Role Services to be installed:

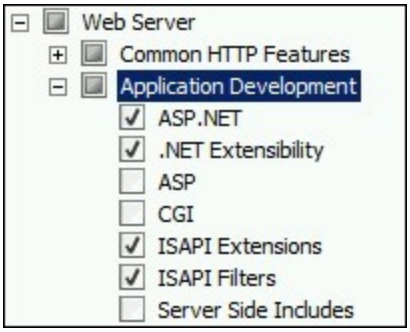
- Common HTTP Features
- Application Development
- Health and Diagnostics
- Security
- Performance
- Management Tools

## COMMON HTTP FEATURES

1. **Static Content** – Static Content lets the Web server publish static Web file formats, such as HTML pages and image files. Use Static Content to publish files on a Web server that users can then view using a Web browser.
2. **Default Document** – Default Document lets organizations configure a default file for the Web server to return when users do not specify a file in a URL. Default documents make it easier and more convenient for users to reach an organizations Web site.

3. **HTTP Errors** – HTTP Errors lets organizations customize the error messages returned to users' browsers when the Web server detects a fault condition. Use HTTP errors to give users a better user experience when they run up against an error message. Consider providing users with an e-mail address for staff who can help them resolve the error.

## APPLICATION DEVELOPMENT




1. **ASP.NET** – ASP.NET provides a server side object-oriented programming environment for building Web sites and Web applications that use managed code. ASP.NET is not just a new version of ASP. ASP.NET provides a robust infrastructure for building Web applications, and it has been completely re-architected to provide a highly productive programming experience based on the .NET Framework.
2. **.NET Extensibility** – .NET Extensibility lets managed code developers change, add, and extend Web server functionality in the request pipeline, the configuration, and the UI. Developers can use the familiar ASP.NET extensibility model and rich

.NET APIs to build Web Server features that are just as powerful as those written using the native C++ APIs.

3. **ISAPI Extensions** – Internet Server Application Programming Interface (ISAPI) Extensions provides support for dynamic Web content development using ISAPI extensions. An ISAPI extension runs when requested, just like any other static HTML file or dynamic ASP file. Since ISAPI applications are compiled code, they are processed much faster than ASP files or files that call COM+ components.
4. **ISAPI Filters** – Internet Server Application Programming Interface (ISAPI) Filters provides support for Web applications that use ISAPI filters. ISAPI filters are files that can extend or change the functionality provided by IIS. An ISAPI filter reviews every request made to the Web server, until the filter finds one that it needs to process.

## HEALTH AND DIAGNOSTICS

1. **HTTP Logging** – HTTP Logging provides logs site activity for this server. When a loggable event (usually an HTTP transaction) occurs, IIS calls the selected logging

module, which then writes to one of the logs stored in the file system of the Web server. These logs are kept in addition to those provided by the operating system.

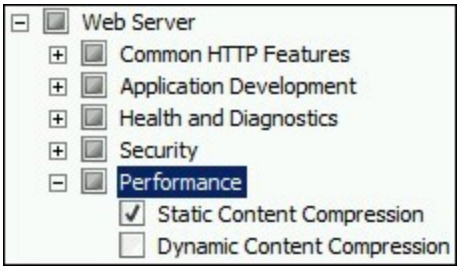
2. **Request Monitoring** – Request Monitor provides infrastructure to monitor Web application health by capturing information about HTTP requests in an IIS worker process. Administrators and developers can use Request Monitor to understand which HTTP requests are executing in a worker process when the worker process has become unresponsive or very slow.

## SECURITY

1. **Windows Authentication** – Windows Authentication is a low cost authentication solution for internal Web sites. This authentication scheme allows administrators in a Windows domain to take advantage of the domain infrastructure for authenticating users. Do not use Windows authentication if users who must be authenticated access an organizations Web site from behind firewalls and proxy servers.

2. **Request Filtering** – Request Filtering screens all incoming requests to the server and filters these requests based on rules set by the administrator. Many malicious attacks share common characteristics, such as very long URLs, or requests for an unusual action. Filtering requests, can attempt to reduce the impact of these types of attacks.

## PERFORMANCE




**Static Content Compression** – Static Content Compression provides infrastructure to configure HTTP compression of static content. This provides more efficient use of bandwidth. Unlike dynamic responses, compressed static responses can be cached without degrading CPU resources.

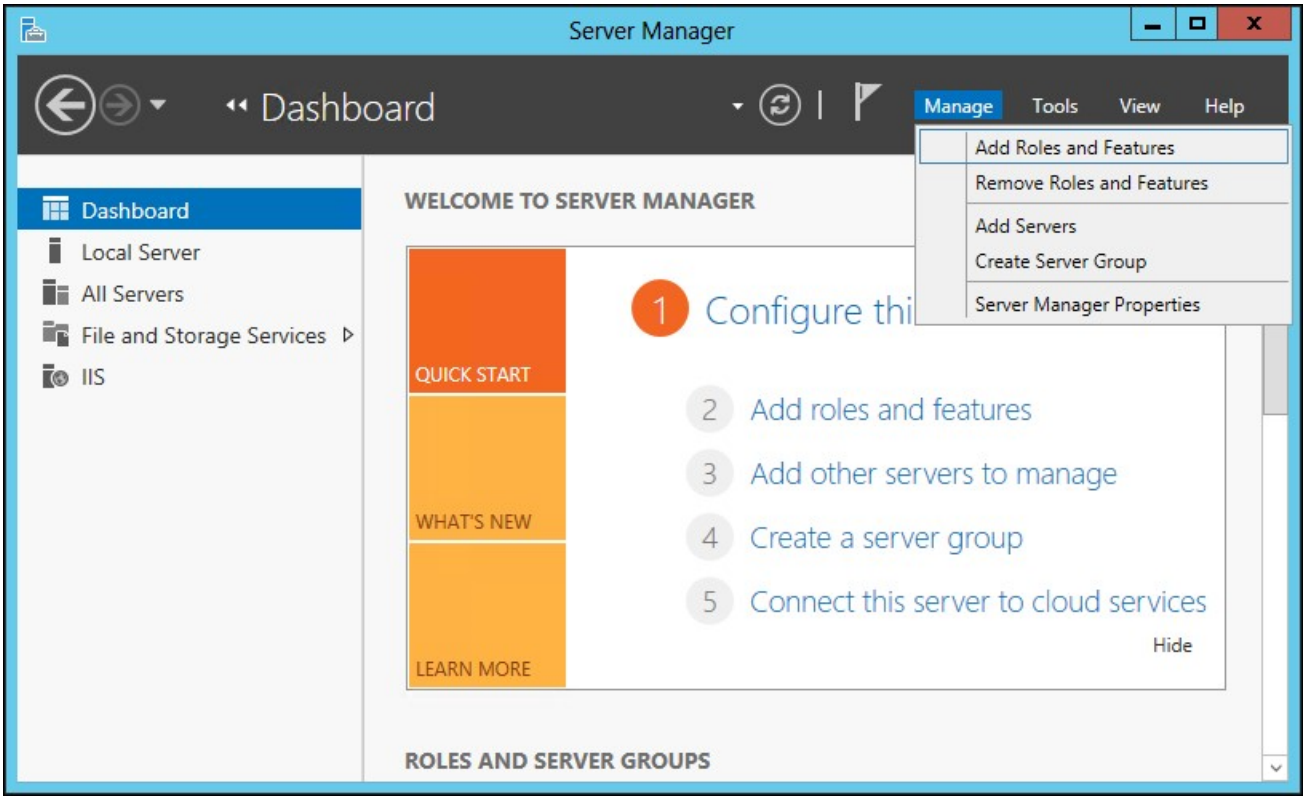
### MANAGEMENT TOOLS

**IIS Management Console** – IIS Manager provides infrastructure to manage IIS by using a graphical user interface. IIS Manager can be used to manage a local or remote Web server that runs IIS.

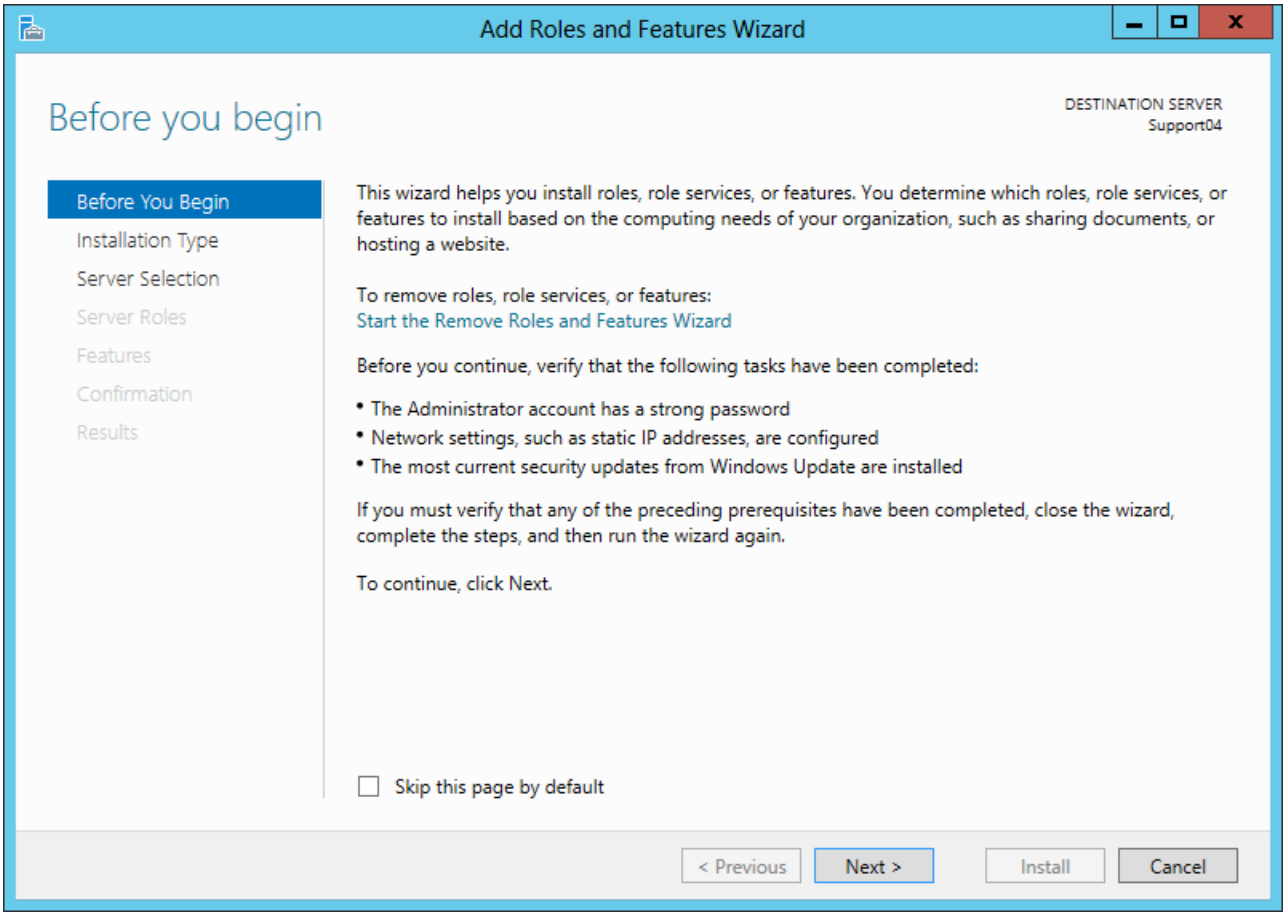
## WINDOWS SERVER 2012/2012 R2

Important: Before beginning the installation process, please see our system requirements. The minimum hardware requirements must be met to continue with the below configuration. Administrative rights will be necessary to enable the roles and features listed for each Windows Server.

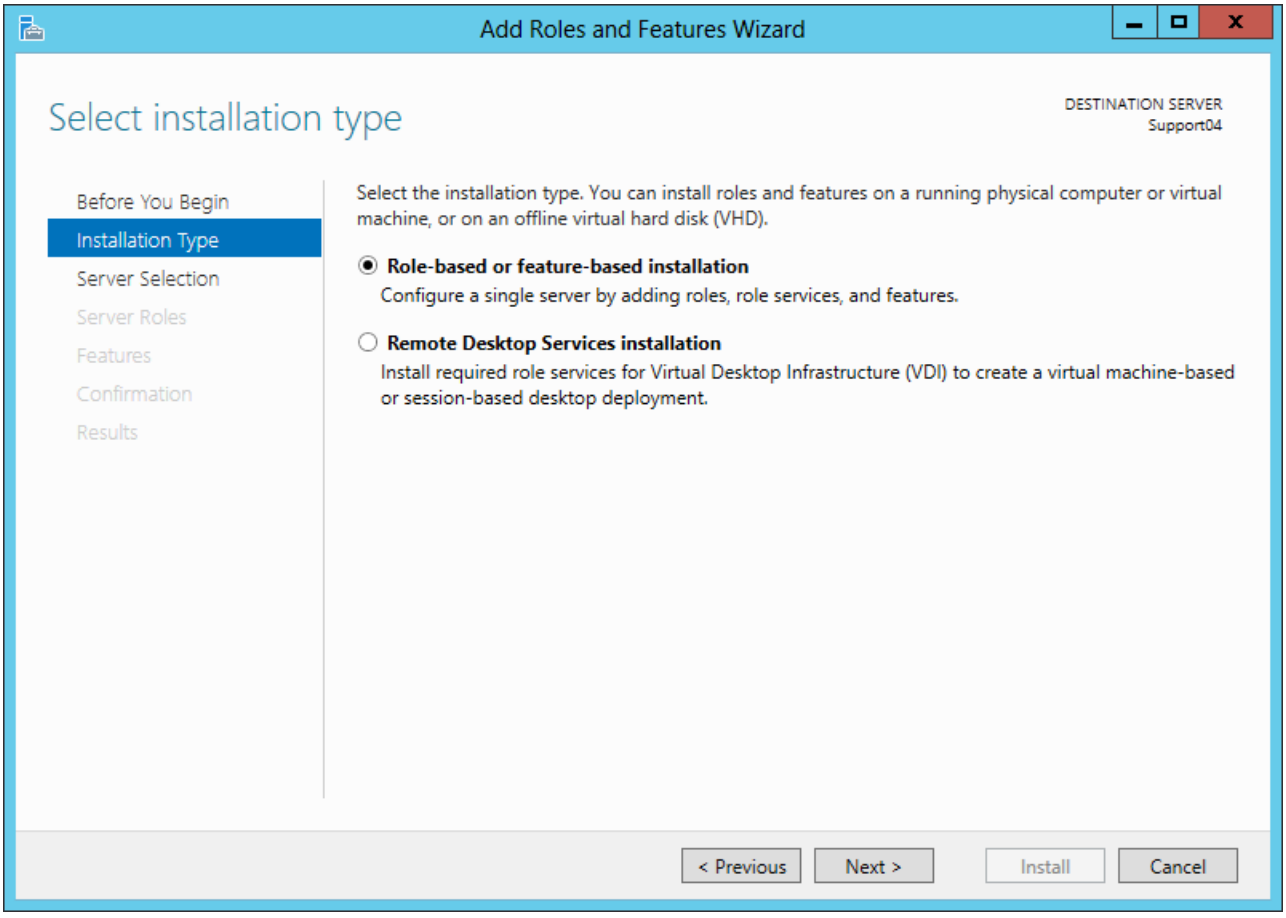
1. In Server Manager, click **Manage** and then select **Add Roles and Features** to start the **Add Roles and Features Wizard**.



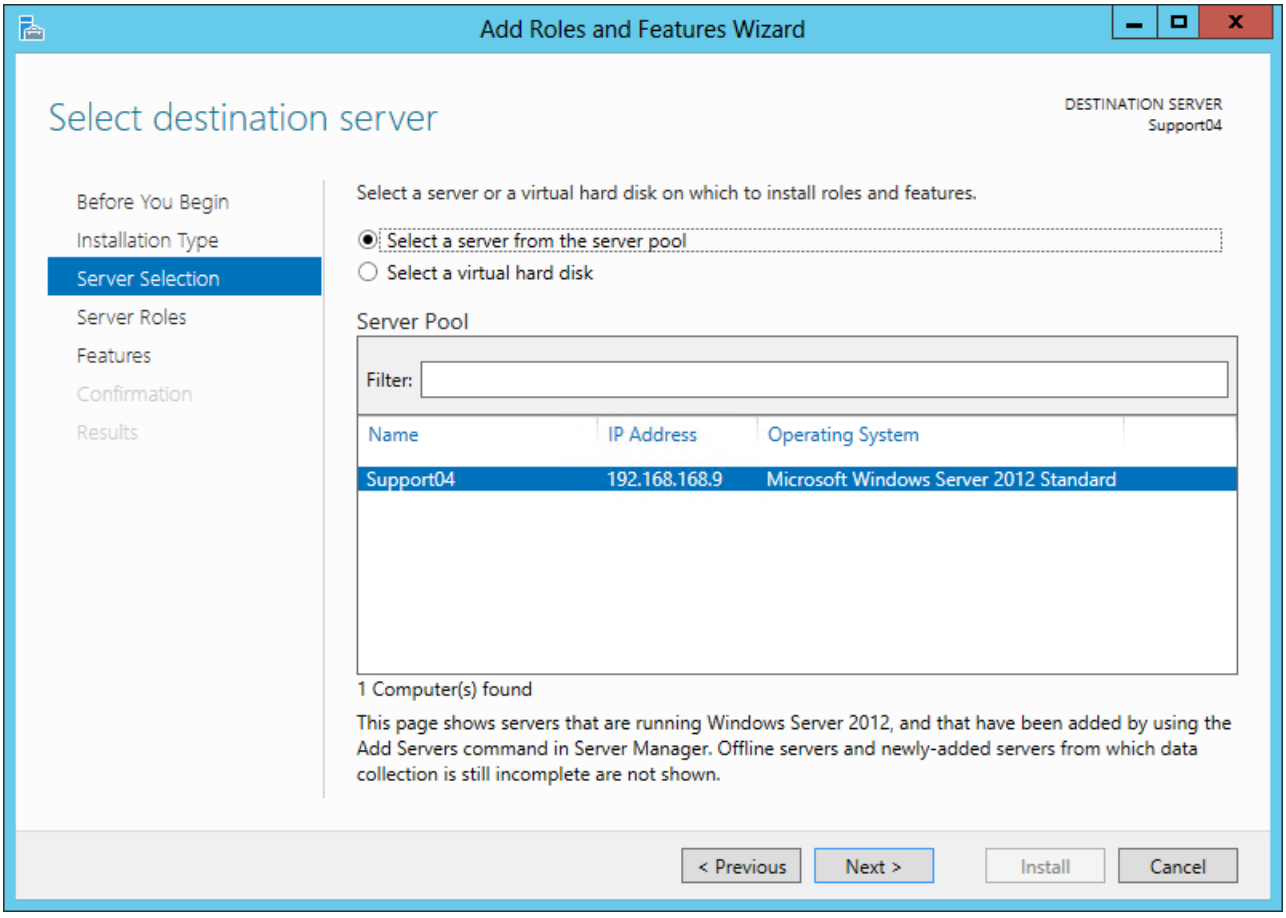

2. On the Select installation type screen, select **Add roles and Features**.
3. Select the target server. The wizard presents a Before you Begin prompt.



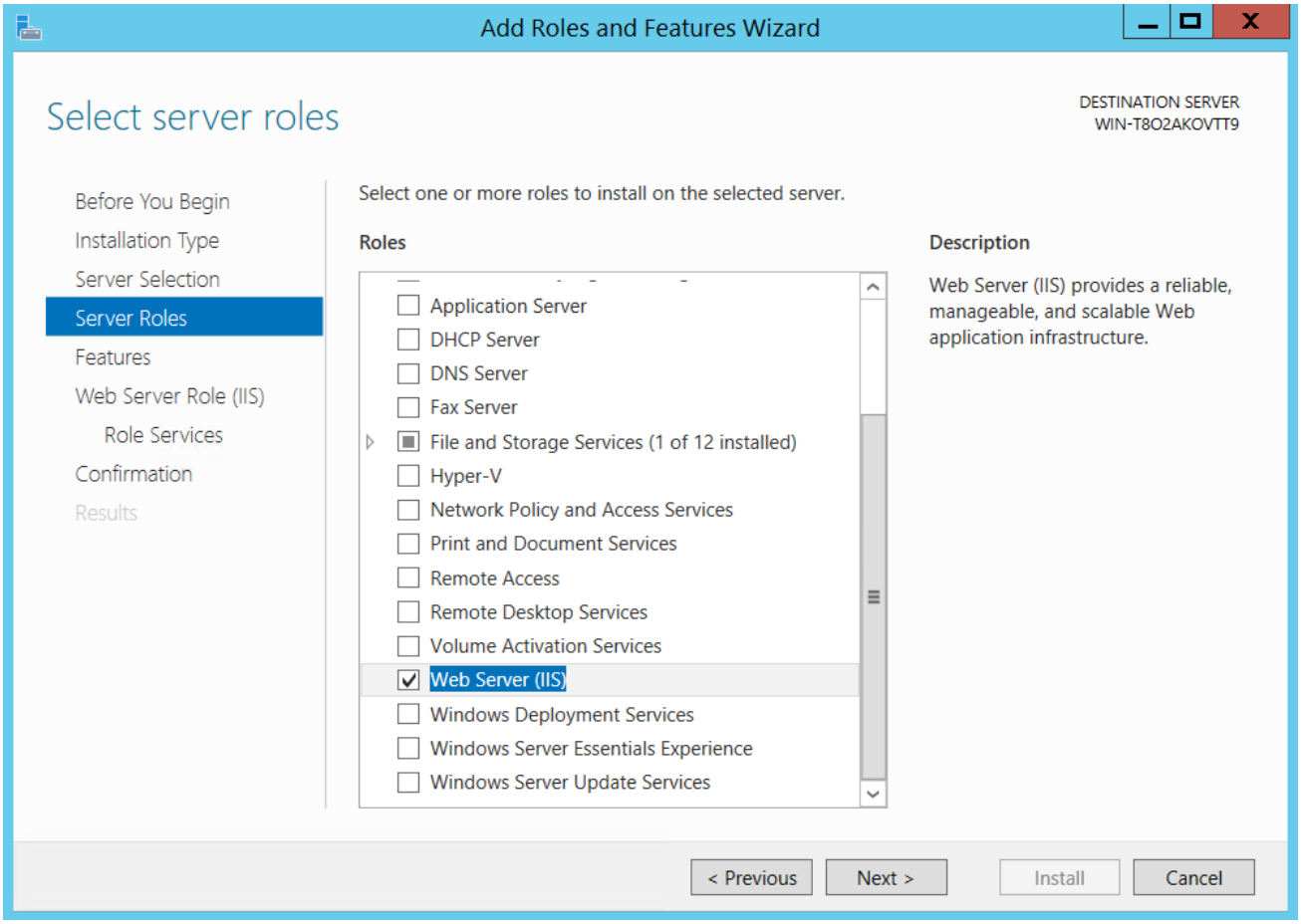

4. Click **Next**. The wizard advances to the Installation Type prompt.



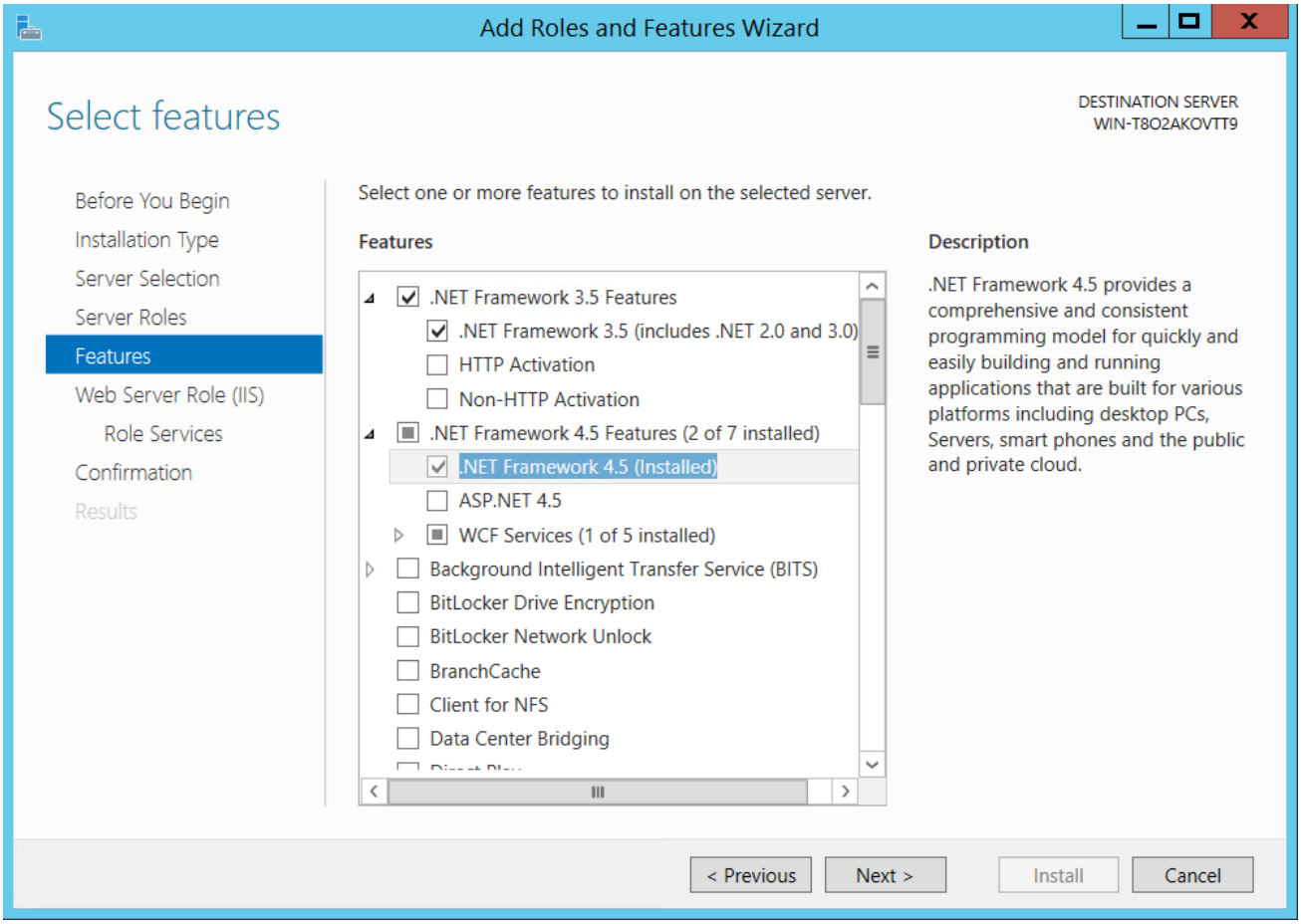

5. Select **Role-based or feature-based installation**.
6. Click **Next**. The wizard advances you to the Server Selection prompt.




7. Select your server and click **Next**. The wizard advances you to the Server Roles prompt.

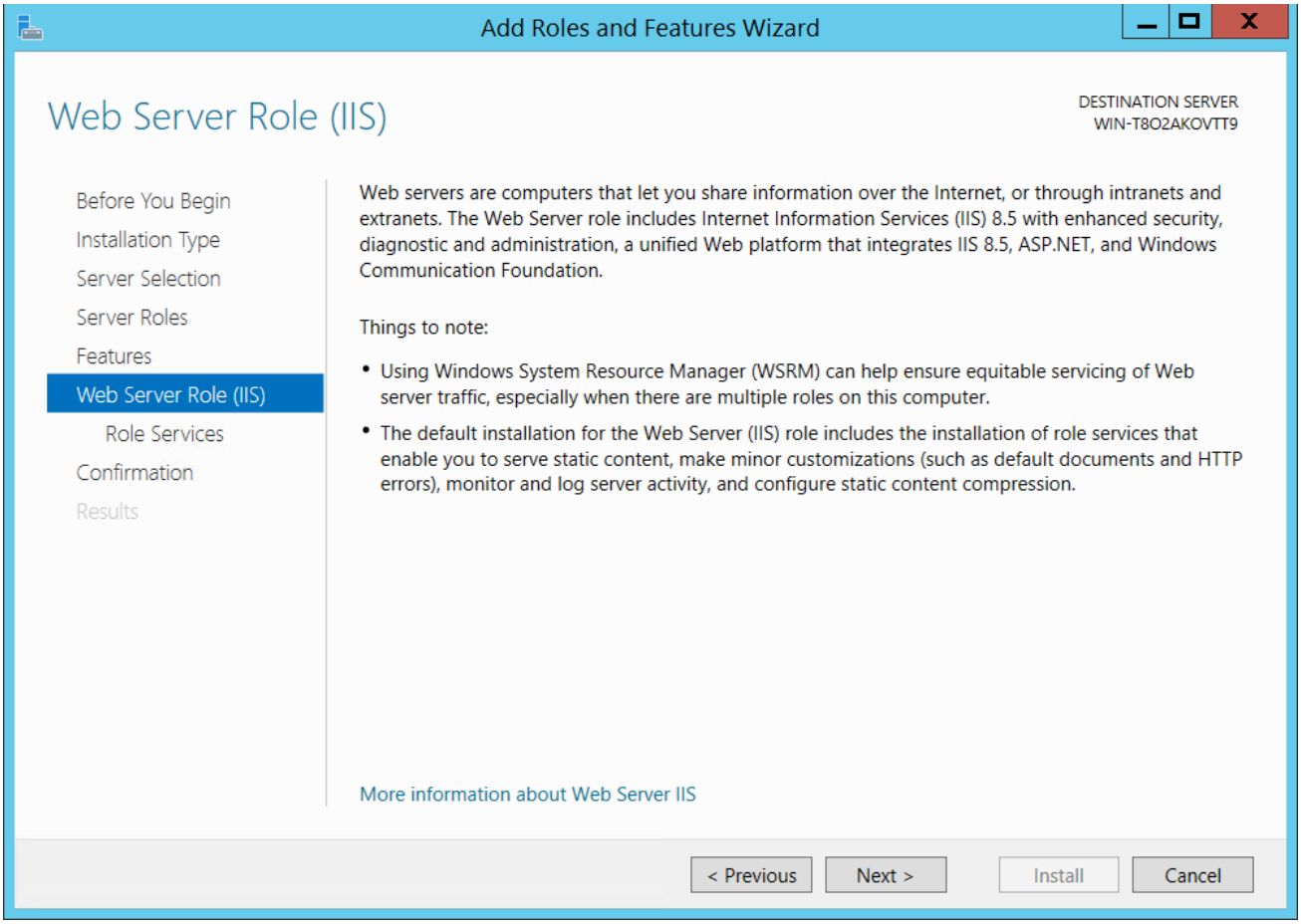



8. Select **Web Server (IIS)** and click **Next**. The wizard advances you to the Features prompt.

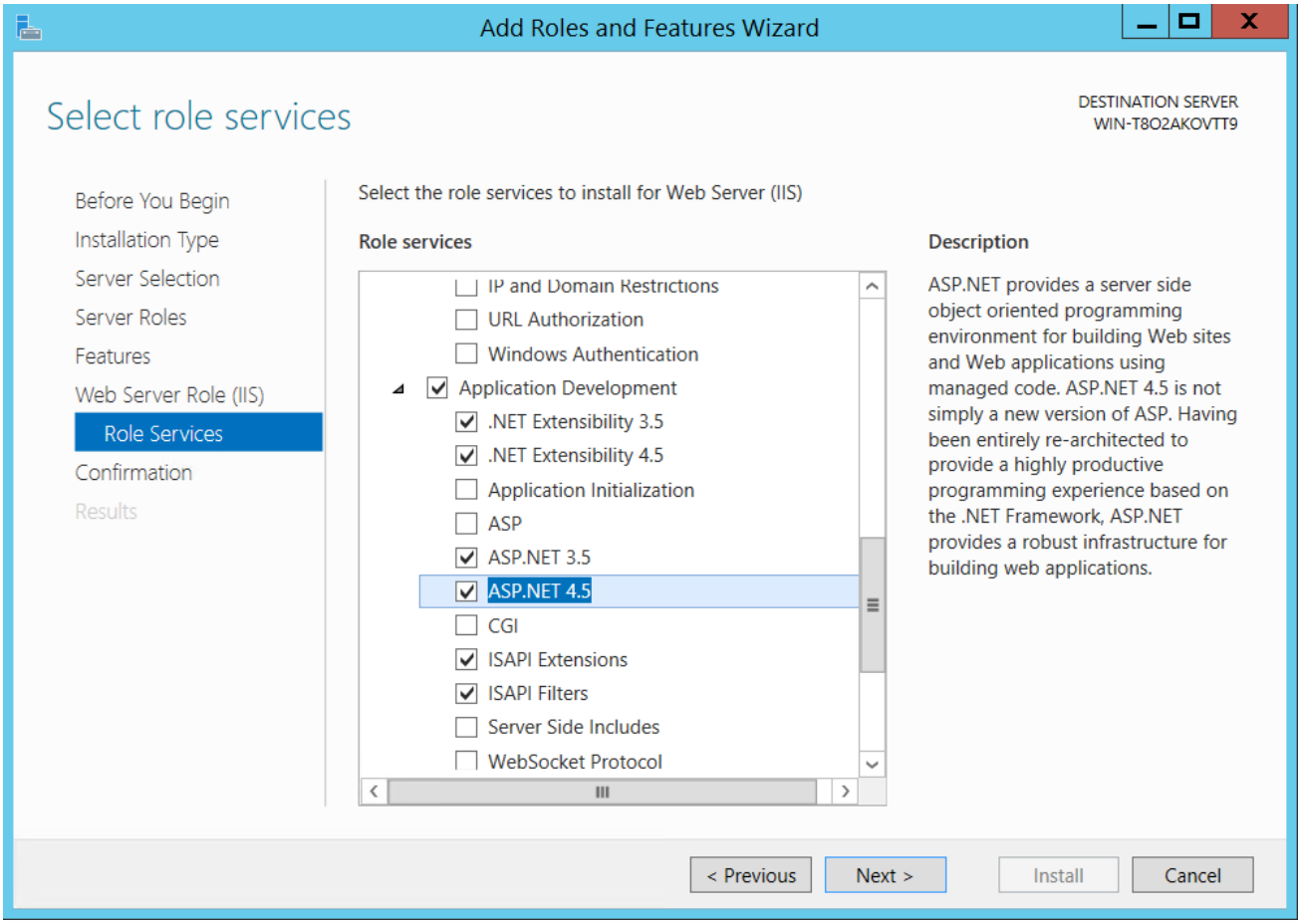



9. Select the **.NET Framework Framework 3.5** and **.NET Framework 4.5** options.

   The wizard prompts you to confirm for each option.



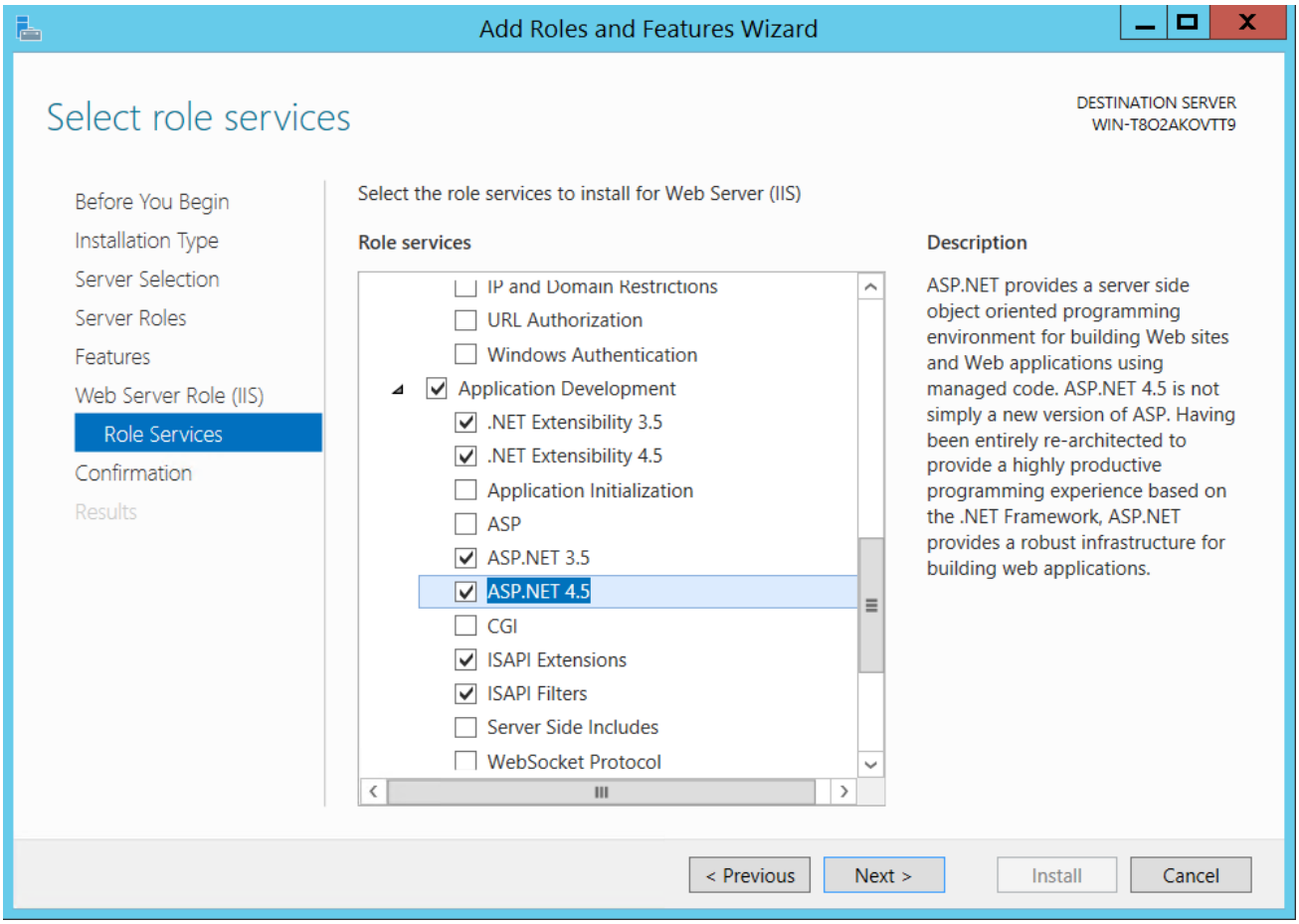

10. Click **Next**. Repeat this confirmation step for the .NET 4.5 server role. The Wizard advances you to the Select Role Services prompt.




11. Select both **ASP .NET 3.5** and **ASP .NET 4.5** options. The wizard advances you to the Confirmation Prompt.
12. Review the selections and then click **Install**.
13. Allow the installation process to complete, review the results that display, and then click **Close**.

# TO INSTALL .NET FRAMEWORK 4.5: REGICS ONLY

1. Repeat Steps 1-10 from the Best Practices: Setting Up Your Web Server 2012 or 2012 R2 section.
2. Once expanded, select both the **.NET Framework 4.5** and **ASP.NET 4.5** options and click **Next**.



3. Review the selections and then click **Install**.
4. Allow the installation process to complete, review the results that display, and then click **Close**.

## TO ADD ROLE SERVICES

When adding IIS using the Add Roles Wizard, only the default installation is executed, which has a minimum set of role services. For EMS products, it is necessary to add role services for the programs to function properly. If role services are added after installing IIS, the Server Administrator will need to navigate to the Role Services page by following the above directions then clicking Next.

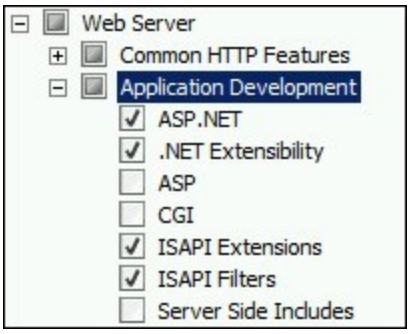
Select the following IIS Role Services to be installed:

- Common HTTP Features
- Application Development
- Health and Diagnostics
- Security
- Performance
- Management Tools

## COMMON HTTP FEATURES

1. **Static Content** – Static Content lets the Web server publish static Web file formats, such as HTML pages and image files. Use Static Content to publish files on a Web server that users can then view using a Web browser.
2. **Default Document** – Default Document lets organizations configure a default file for the Web server to return when users do not specify a file in a URL. Default documents make it easier and more convenient for users to reach an organizations Web site.
3. **Directory Browsing** – Directory Browsing lets users see the contents of a directory on a Web server. Use Directory Browsing to enable an automatically generated list of all directories and files available in a directory when users do not specify a file in a URL and default documents are either disabled or not configured.
4. **HTTP Errors** – HTTP Errors lets organizations customize the error messages returned to users' browsers when the Web server detects a fault condition. Use HTTP errors to give users a better user experience when they run up against an error message. Consider providing users with an e-mail address for staff who can help them resolve the error.

## APPLICATION DEVELOPMENT




1. **ASP.NET** – ASP.NET provides a server side object-oriented programming environment for building Web sites and Web applications that use managed code. ASP.NET is not just a new version of ASP. ASP.NET provides a robust infrastructure for building Web applications, and it has been completely re-architected to provide a highly productive programming experience based on the .NET Framework.
2. **.NET Extensibility** – .NET Extensibility lets managed code developers change, add, and extend Web server functionality in the request pipeline, the configuration, and the UI. Developers can use the familiar ASP.NET extensibility model and rich .NET APIs to build Web Server features that are just as powerful as those written using the native C++ APIs.
3. **ISAPI Extensions** – Internet Server Application Programming Interface (ISAPI) Extensions provides support for dynamic Web content development using ISAPI extensions. An ISAPI extension runs when requested, just like any other static

HTML file or dynamic ASP file. Since ISAPI applications are compiled code, they are processed much faster than ASP files or files that call COM+ components.

4. **ISAPI Filters** – Internet Server Application Programming Interface (ISAPI) Filters provides support for Web applications that use ISAPI filters. ISAPI filters are files that can extend or change the functionality provided by IIS. An ISAPI filter reviews every request made to the Web server, until the filter finds one that it needs to process.

## HEALTH AND DIAGNOSTICS

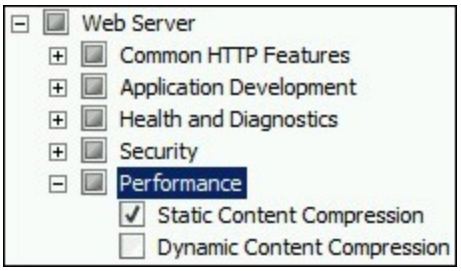
1. **HTTP Logging** – HTTP Logging provides logs site activity for this server. When a loggable event (usually an HTTP transaction) occurs, IIS calls the selected logging module, which then writes to one of the logs stored in the file system of the Web server. These logs are kept in addition to those provided by the operating system.
2. **Request Monitoring** – Request Monitor provides infrastructure to monitor Web application health by capturing information about HTTP requests in an IIS worker process. Administrators and developers can use Request Monitor to understand

which HTTP requests are executing in a worker process when the worker process has become unresponsive or very slow.

## SECURITY

1. **Windows Authentication** – Windows Authentication is a low cost authentication solution for internal Web sites. This authentication scheme allows administrators in a Windows domain to take advantage of the domain infrastructure for authenticating users. Do not use Windows authentication if users who must be authenticated access an organizations Web site from behind firewalls and proxy servers.
2. **Request Filtering** – Request Filtering screens all incoming requests to the server and filters these requests based on rules set by the administrator. Many malicious attacks share common characteristics, such as very long URLs, or requests for an unusual action. Filtering requests, can attempt to reduce the impact of these types of attacks.

## PERFORMANCE




**Static Content Compression** – Static Content Compression provides infra-structure to configure HTTP compression of static content. This provides more efficient use of bandwidth. Unlike dynamic responses, compressed static responses can be cached without degrading CPU resources.

## MANAGEMENT TOOLS

**IIS Management Console** – IIS Manager provides infrastructure to manage IIS by using a graphical user interface. IIS Manager can be used to manage a local or remote Web server that runs IIS.

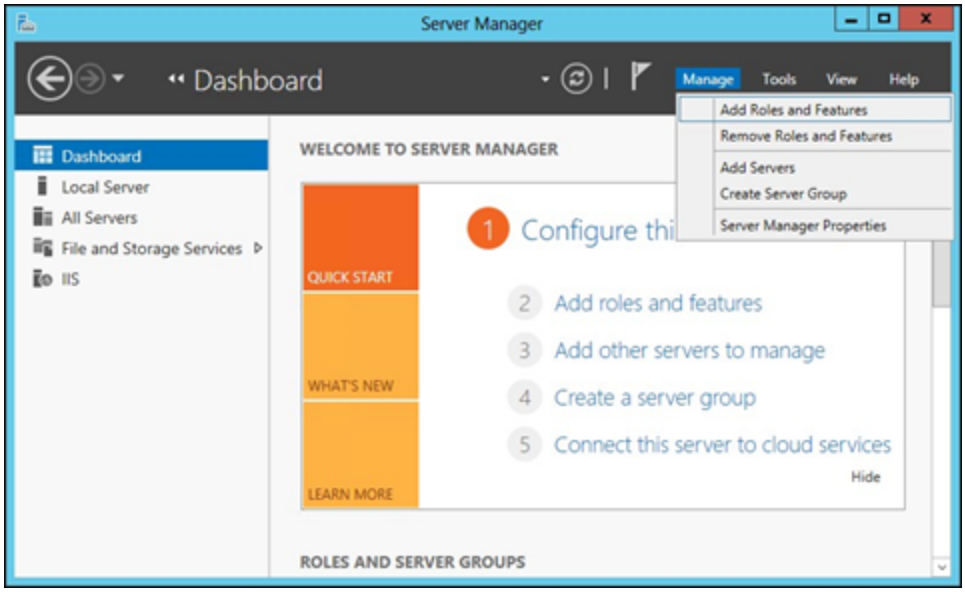
# CHAPTER 18: Install .NET Framework for Windows Server 2012/2012 R2

This topic provides information on the following:

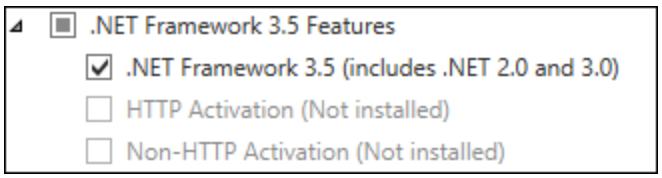

- Install .NET Framework 3.5 and .NET Framework 4.5
- Install .NET Framework 4.5: Regics Only


## INSTALL .NET FRAMEWORK 3.5 AND .NET FRAMEWORK 4.5

1. In Server Manager, click **Manage** and then select **Add Roles and Features** to start the Add Roles and Features Wizard.



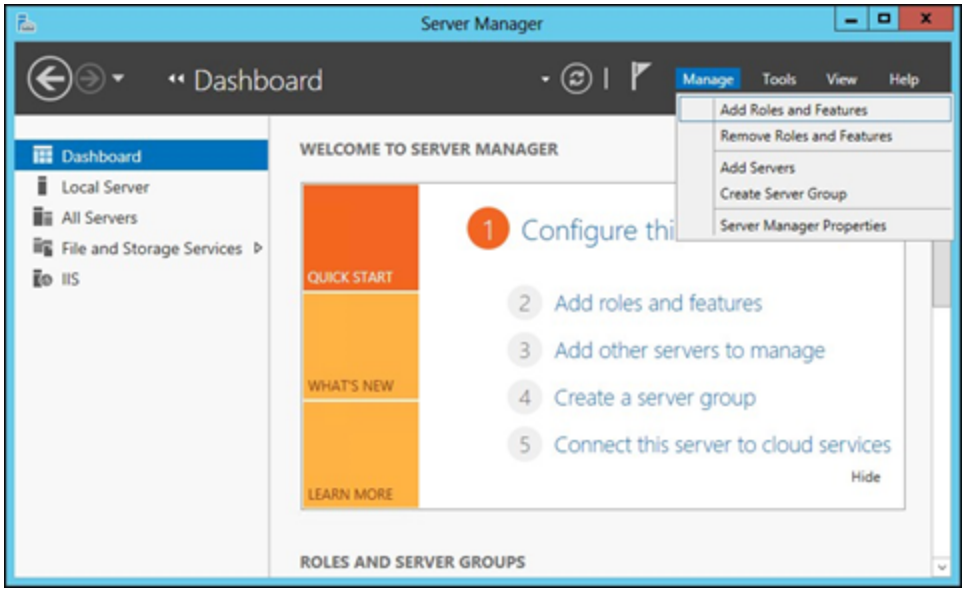

2. In the Confirm Installation Selections interface, review the selections and then click **Install**.
3. Allow the installation process to complete and then click **Close**.
4. On the Select installation type screen, select **Role-based or feature-based installation**.
5. Select the target server.
6. On the **Select Features** screen, check the box next to **.Net Framework 3.5 Features**.



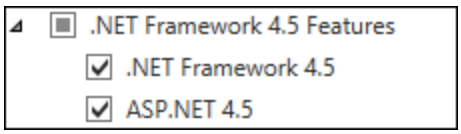

7. In the Select Features interface, expand **.NET Framework 3.5 Features**.
8. Once expanded, there will be three check boxes. One for .NET Framework 3.5 and the other two for HTTP Activation and Non-HTTP Activation. Check the box next to **.NET Framework 3.5** and click **Next**.

# INSTALL .NET FRAMEWORK 4.5: REGICS ONLY

1. In Server Manager, click **Manage** and then select **Add Roles and Features** to start the Add Roles and Features Wizard.




2. On the Select installation type screen, select **Role-based or feature-based installation**.
3. Select the target server.
4. On the Select Features screen, check the box next to **.Net Framework 4.5 Features**.
5. In the Select Features interface, expand **.NET Framework 4.5 Features**.
6. Once expanded, there will be three check boxes. These will be .NET Framework 4.5, APS.NET 4.5 and WCF Services. Check the boxes next to **.NET Framework 4.5** and **ASP.NET 4.5** then click **Next**.

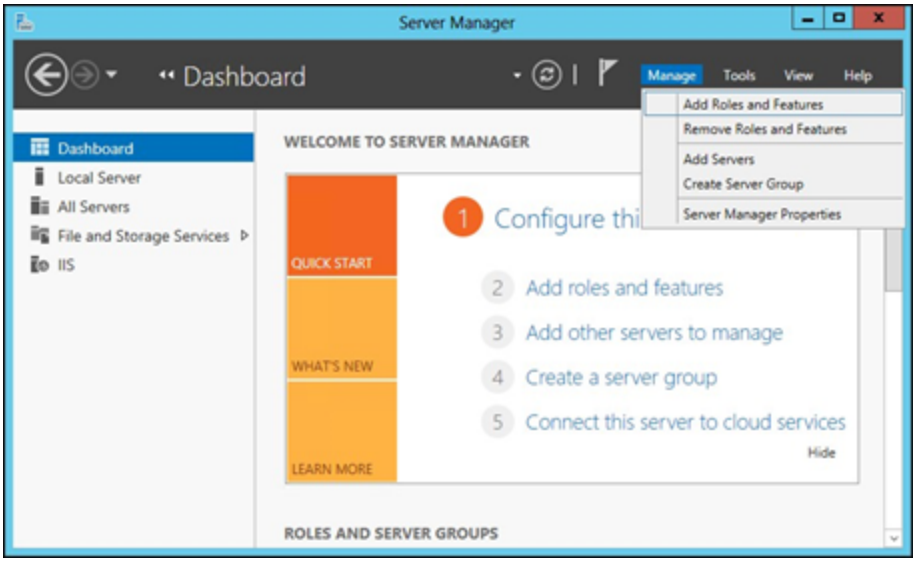



7. In the Confirm Installation Selections interface, review the selections and then click **Install**.
8. Allow the installation process to complete and then click **Close**.

# CHAPTER 19: Install Internet Information Services (IIS)

To install IIS on a Windows Server 2012, do the following:

1. In Server Manager, click Manage and then select Add Roles and Features to start the Add Roles and Features Wizard.




2. On the Select installation type screen, select **role-based** or **feature-based** installation.
3. Select the target server.

4. On the Select Roles screen, check the box next to **Web Server (IIS)**. The Web Server (IIS) role in Windows Server 2012 provides a secure, easy-to-manage, modular and extensible platform for reliably hosting websites, services, and applications.
5. No additional features are needed for IIS, so click **Next.**
6. Customize your installation of IIS by verifying the Role Services are selected and then click Next:
7. In the Confirm Installation Selections interface, review the selections and then click **Install**.
8. Allow the installation process to complete and then click **Close**.

# CHAPTER 20: Add Role Services

1. In Server Manager, click **Manage** and then select **Add Roles and Features** to start the Add Roles and Features Wizard.
2. On the Select installation type screen, select **Role-based or feature-based installation**.
3. Select the target server.
4. On the Select Roles screen, expand **Web Server (IIS)**.

Select the following IIS Role Services to be installed:

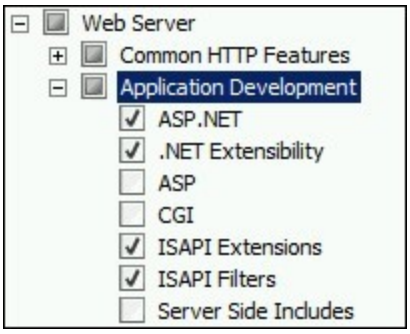
- Common HTTP Features
- Application Development
- Health and Diagnostics
- Security
- Performance
- Management Tools

# COMMON HTTP FEATURES

1. **Static Content** – Static Content lets the Web server publish static Web file formats, such as HTML pages and image files. Use Static Content to publish files on a Web server that users can then view using a Web browser.
2. **Default Document** – Default Document lets organizations configure a default file for the Web server to return when users do not specify a file in a URL. Default documents make it easier and more convenient for users to reach an organizations Web site.
3. **Directory Browsing** – Directory Browsing lets users see the contents of a directory on a Web server. Use Directory Browsing to enable an automatically generated list of all directories and files available in a directory when users do not specify a file in a URL and default documents are either disabled or not configured.
4. **HTTP Errors** – HTTP Errors lets organizations customize the error messages returned to users' browsers when the Web server detects a fault condition. Use HTTP errors to give users a better user experience when they run up against an

error message. Consider providing users with an e-mail address for staff who can help them resolve the error.

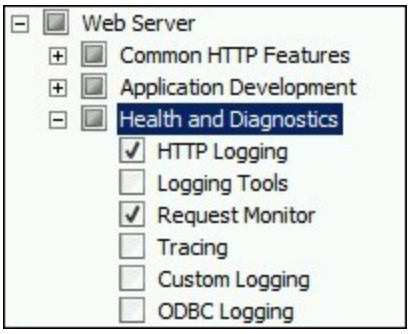
## APPLICATION DEVELOPMENT




1. **ASP.NET** – ASP.NET provides a server side object-oriented programming environment for building Web sites and Web applications that use managed code. ASP.NET is not just a new version of ASP. ASP.NET provides a robust infrastructure for building Web applications, and it has been completely re-architected to provide a highly productive programming experience based on the .NET Framework.
2. **.NET Extensibility** – .NET Extensibility lets managed code developers change, add, and extend Web server functionality in the request pipeline, the configuration, and the UI. Developers can use the familiar ASP.NET extensibility model and rich .NET APIs to build Web Server features that are just as powerful as those written using the native C++ APIs.

3. **ISAPI Extensions** – Internet Server Application Programming Interface (ISAPI) Extensions provides support for dynamic Web content development using ISAPI extensions. An ISAPI extension runs when requested, just like any other static HTML file or dynamic ASP file. Since ISAPI applications are compiled code, they are processed much faster than ASP files or files that call COM+ components.
4. **ISAPI Filters** – Internet Server Application Programming Interface (ISAPI) Filters provides support for Web applications that use ISAPI filters. ISAPI filters are files that can extend or change the functionality provided by IIS. An ISAPI filter reviews every request made to the Web server, until the filter finds one that it needs to process.

# HEALTH AND DIAGNOSTICS




1. **HTTP Logging** – HTTP Logging provides logs site activity for this server. When a loggable event (usually an HTTP transaction) occurs, IIS calls the selected logging module, which then writes to one of the logs stored in the file system of the Web server. These logs are kept in addition to those provided by the operating system.

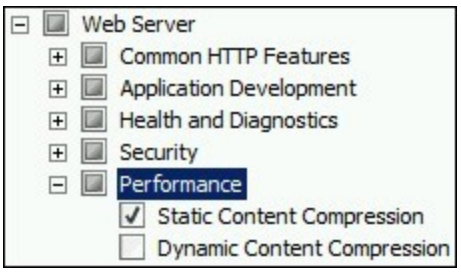
2. **Request Monitoring** – Request Monitor provides infrastructure to monitor Web application health by capturing information about HTTP requests in an IIS worker process. Administrators and developers can use Request Monitor to understand which HTTP requests are executing in a worker process when the worker process has become unresponsive or very slow.

## SECURITY

1. **Windows Authentication** – Windows Authentication is a low cost authentication solution for internal Web sites. This authentication scheme allows administrators in a Windows domain to take advantage of the domain infrastructure for authenticating users. Do not use Windows authentication if users who must be authenticated access an organizations Web site from behind firewalls and proxy servers.
2. **Request Filtering** – Request Filtering screens all incoming requests to the server and filters these requests based on rules set by the administrator. Many malicious

attacks share common characteristics, such as very long URLs, or requests for an unusual action. Filtering requests, can attempt to reduce the impact of these types of attacks.

## PERFORMANCE




**Static Content Compression** – Static Content Compression provides infrastructure to configure HTTP compression of static content. This provides more efficient use of bandwidth. Unlike dynamic responses, compressed static responses can be cached without degrading CPU resources.

# MANAGEMENT TOOLS

**IIS Management Console** – IIS Manager provides infrastructure to manage IIS by using a graphical user interface. IIS Manager can be used to manage a local or remote Web server that runs IIS.

# CHAPTER 21: Authentication Options

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

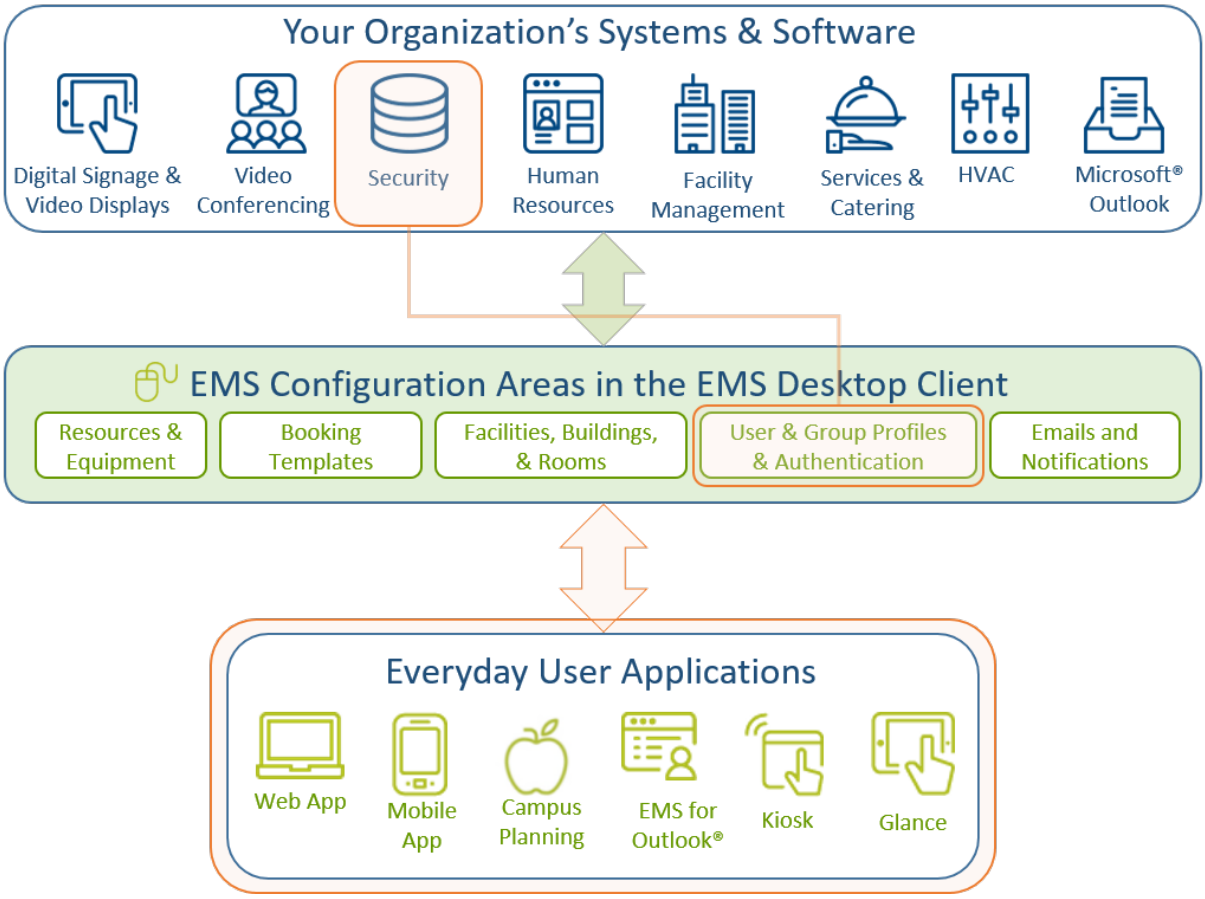

- Introduction
  - Authentication Options for EMS Web App and Virtual EMS (VEMS)
  - Authentication Options for EMS Mobile
  - Authentication Options for EMS Master Calendar
  - Authentication Options for EMS Regics
- Integrated Authentication Considerations
- Integrated Windows Authentication
- Manage Everyday Users For Integrated Authentication
- LDAP Authentication
- Portal or Federated Authentication
- Portal Authentication Methods

# CHAPTER 22: 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.

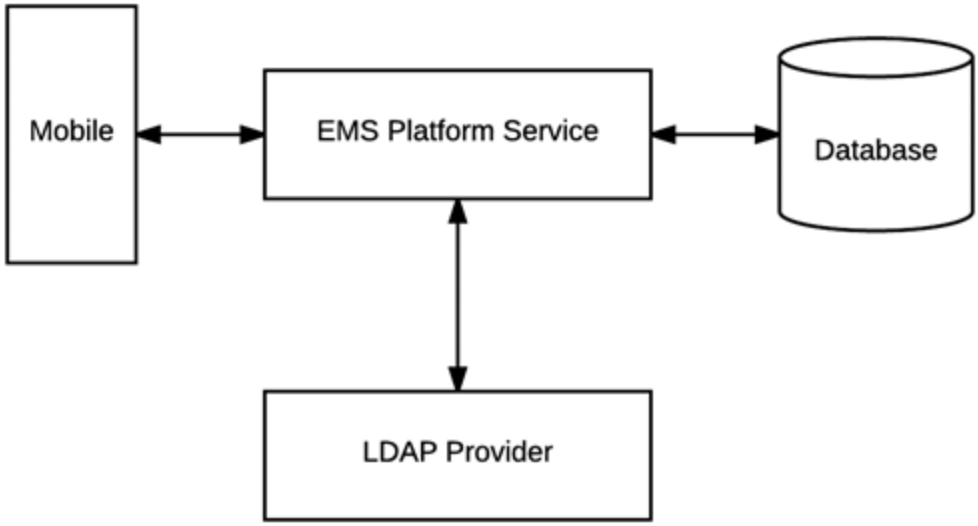
Several built-in authentication methods to pass-in credentials are available including:

- 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 23: 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 24: VPAT for EMS Web App (V44.1)

## EMS ACCESSIBILITY CONFORMANCE REPORT

Based on Voluntary Product Accessibility Template® (VPAT®)1

VPAT Version 2.0 Beta 2

Name of Product: EMS Software Web App V44.1

Date: May 17, 2017

Contact Support

Note: This VPAT is based upon an evaluation of a select number of pages from within the larger application. It is not necessarily exhaustive of all issues.

## STANDARDS/GUIDELINES

This report covers the degree of conformance for the following accessibility standard/guideline:

| STANDARD/GUIDELINE | INCLUDED IN REPORT |
| --- | --- |
| Web Content Accessibility Guidelines 2.0, at<br>http://www.w3.org/TR/2008/REC-WCAG20-20081211/ | Level A - Included<br>Level AA - Included<br>Level AAA - Not Included |
| Section 508 as published in 2017, at<br>http://www.Section508.gov | Included |

## TABLE INFORMATION

For each of the standards, the criteria are listed in the tables below. The first column contains the criteria being evaluated, the second column describes the level of conformance of the product with regard to the criteria, and the third column contains any additional remarks and explanations regarding the product.

- By default, the table information is showing. This information can be hidden by clicking, “Click to show or hide table data”. This allows users to hide information so they see only the sections they need.
- When sections of criteria do not apply, or deemed by the customer as not applicable, the section is noted as such and the rest of that table may be removed for that section.

- When multiple standards are being recorded in this document, the duplicative sections are noted and responded to only one time. The duplicate entry will note the cross reference to the data.

## TERMS

The terms used in the Conformance Level information are defined as follows:

- Supports: The functionality of the product has at least one method that meets the criteria without known defects or meets with equivalent facilitation.
- Supports with Exceptions: Some functionality of the product does not meet the criteria.
- Does Not Support: Majority of functionality of the product does not meet the criteria.
- Not Applicable: The criteria are not relevant to the product.
- Not Evaluated: The product has not been evaluated against the criteria. This can be used only with WCAG 2.0 Level AAA.

## WCAG 2.0 REPORT

Table 1: Conformance Criteria, Level A

Note:  Some issues fall under two criteria. The issue reference will only be listed under one of the applicable criteria.

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
| --- | --- | --- |
| 1.1.1 Non-text Content (Level A)<br><br>All non-text content that is presented to the user has a text alternative that serves the equivalent purpose. (See Exceptions.) | Supports with Exceptions | Some images do not have proper alt-text. Icon fonts in the "Services" section do not contain text alternatives. Some icon fonts do not have text alternatives. Decorative SVG images on the home page are not marked as decorative. |
| 1.2.1 Audio-only and Video-only (Pre-recorded) (Level A)<br><br>For prerecorded audio-only and prerecorded video-only media, the following are true:<br><br>» Pre-recorded Audio-only: An alternative for time-based media presents equivalent information for prerecorded audio-only content.<br>» Pre-recorded Video-only: Either an alternative for time-based media or an audio track presents equivalent information for pre-recorded video-only content. | Supports | Pre-recorded audio-only and pre-recorded video only media are not present. |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| 1.2.2 Captions (Pre-recorded) (Level A)<br><br>Captions are provided for all pre-recorded audio content in synchronized media, except when the media is a media alternative for text and is clearly labeled as such. | Supports | Pre-recorded audio in synchronized media is not present. |
| 1.2.3 Audio Description or Media Alternative (Pre-recorded) (Level A)<br><br>An alternative for time-based media or audio description of the pre-recorded video content is provided for synchronized media. (See Exceptions.) | Supports | Pre-recorded video content for synchronized media is not present. |
| 1.3.1 Info and Relationships (Level A)<br><br>Information, structure, and relationships conveyed through presentation can be programmatically determined or are available in text. | Supports with Exceptions | Programmatically determined structure is not provided for some of the content. There are some empty list items. The main navigation nested list does not properly define the nested structure. Some pages do not have headings defined in the correct place. Some tables do not have their column headers |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| | | properly defined, or they are using ARIA grids and do not have all ARIA roles assigned correctly. Some form elements are not explicitly labeled. |
| 1.3.2 Meaningful Sequence (Level A)<br><br>When the sequence in which content is presented affects its meaning, a correct reading sequence can be programmatically determined. | Supports with Exceptions | Some of the content does not have a reading sequence that is programmatically determined. When the main navigation is collapsed, it is still readable by screen reader users. There are a couple of other instances in the main content of the pages where content hidden from all users is still readable by screen reader users. |
| 1.3.3 Sensory Characteristics (Level A)<br><br>Instructions provided for understanding and operating content do not rely solely on sensory characteristics of components, such as shape, size, visual location, orientation, or sound.<br><br>Note: For requirements related to color, refer to Guideline 1.4.1. | Supports | Instructions for content do not rely on sensory characteristics. |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| 1.4.1 Use of Color (Level A)<br><br>Color is not used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element. | Supports with Exceptions | Color alone is used to convey some information. Some links are identified through color alone. The availability of attendees and rooms in the schedule search is conveyed exclusively through color. |
| 1.4.2 Audio Control (Level A)<br><br>If any audio on a Web page plays automatically for more than 3 seconds, either a mechanism is available to pause or stop the audio, or a mechanism is available to control audio volume independently from the overall system volume level. | Supports | Audio content is not present. |
| 2.1.1 Keyboard (Level A)<br><br>All functionality of the content is operable through a keyboard interface without requiring specific timings for individual keystrokes. | Supports with Exceptions | Numerous user interface elements cannot be operated with the keyboard. |
| 2.1.2 No Keyboard Trap<br><br>(Level A) | Supports | No keyboard trap is detected during navigation. |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
| --- | --- | --- |
| If keyboard focus can be moved to a component of the page using a keyboard interface, then focus can be moved away from that component using only a keyboard interface, and, if it requires more than unmodified arrow or tab keys or other standard exit methods, the user is advised of the method for moving focus away. | | |
| 2.2.1 Timing Adjustable (Level A)<br><br>For each time limit that is set by the content, at least one of the following is true:<br><br>» Turn off: The user is allowed to turn off the time limit before encountering it; or<br>» Adjust: The user is allowed to adjust the time limit before encountering it over a wide range that is at least ten times the length of the default setting; or | Supports | Users can extend or turn off timeouts for tasks. |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
| --- | --- | --- |
| » Extend: The user is warned before time expires and given at least 20 seconds to extend the time limit with a simple action (for example, "press the space bar"), and the user is allowed to extend the time limit at least ten times | | |
| 2.2.2 Pause, Stop, Hide (Level A)<br><br>For moving, blinking, scrolling, or auto-updating information, all of the following are true:<br><br>» Moving, blinking, scrolling: For any moving, blinking or scrolling information that (1) starts automatically, (2) lasts more than five seconds, and (3) is presented in parallel with other content, there is a mechanism for the user to pause, stop, or hide it unless the movement, blinking, or scrolling is part of an activity where it is essential; and | Supports | No moving content is present on the pages. |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
| --- | --- | --- |
| » Auto-updating: For any auto-updating information that (1) starts automatically and (2) is presented in parallel with other content, there is a mechanism for the user to pause, stop, or hide it or to control the frequency of the update unless the auto-updating is part of an activity where it is essential | | |
| 2.3.1 Three Flashes or Below Threshold (Level A)<br><br>Web pages do not contain anything that flashes more than three times in any one second period, or the flash is below the general flash and red flash thresholds. | Supports | No flashing or blinking content is present on the pages. |
| 2.4.1 Bypass Blocks (Level A)<br><br>A mechanism is available to bypass blocks of content that are repeated on multiple Web pages. | Does not Support | A mechanism to bypass blocks of content is not available. Some ARIA landmarks are also defined incorrectly. |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| 2.4.2 Page Titled (Level A)<br><br>Web pages have titles that describe topic or purpose. | Supports with Exceptions | Some pages do not have informative titles. The reservation confirmation screen is lacking a descriptive title. |
| 2.4.3 Focus Order (Level A)<br><br>If a Web page can be navigated sequentially and the navigation sequences affect meaning or operation, focusable components receive focus in an order that preserves meaning and operability. | Supports with Exceptions | Focus order is illogical and does not follow the navigation sequence of pages in some cases. Some content when it is supposed to be hidden from all users can still be reached with the keyboard. The main navigation is one example. Also, when modal dialogs close, the focus is not set back to a logical spot within the page. |
| 2.4.4 Link Purpose (In Context) (Level A)<br><br>The purpose of each link can be determined from the link text alone or from the link text together with its programmatically determined link context. | Supports with Exceptions | Some links do not have link text or surrounding text that convey their purpose. Many of the links have text, but the text repeats other link text on the page and the differences between the links cannot be perceived. |
| 3.1.1 Language of Page<br><br>(Level A) | Does Not Support | Human language is not defined on each page. |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| The default human language of each Web page can be programmatically determined. | | |
| 3.2.1 On Focus (Level A)<br><br>When any component receives focus, it does not initiate a change of context. | Supports | A change of context is not initiated when elements on the page receive focus. |
| 3.2.2 On Input (Level A)<br><br>Changing the setting of any user interface component does not automatically cause a change of context. | Supports | Changing the settings of controls does not change context. |
| 3.3.1 Error Identification (Level A)<br><br>If an input error is automatically detected, the item that is in error is identified and the error is described to the user in text. | Supports with Exceptions | Some error messages are not semantically related to their form element. |
| 3.3.2 Labels or Instructions (Level A) | Supports with Exceptions | Some user input controls do not have labels or instructions. The date and time inputs do not convey their formatting requirements. |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| Labels or instructions are provided when content requires user input. | | |
| 4.1.1 Parsing (Level A)<br><br>In content implemented using markup languages, elements have complete start and end tags, elements are nested according to their specifications, elements do not contain duplicate attributes, and any IDs are unique (see exceptions).<br><br>Note: Start and end tags that are missing a critical character in their formation, such as a closing angle bracket or a mismatched attribute value quotation mark are not complete. | Supports with Exceptions | Some elements do not have correct structure. |
| 4.1.2 Name, Role, Value<br><br>(Level A)<br><br>For all user interface components (including but not limited to: form elements, links and components generated by scripts), the name and role can be programmatically determined; states, properties, and values that can | Supports with Exceptions | Some user interface controls provide names, states, roles, and values. Controls that expand and collapse sections do not convey their current state. Dynamic changes to the page are not perceived by screen reader users. Complex UI components such as tab panels are not implemented correctly. Some form labels are not defined correctly. |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| be set by the user can be programmatically set; and notification of changes to these items is available to user agents, including assistive technologies. | | |

## TABLE 2. CONFORMANCE CRITERIA, LEVEL AA

Note: Some issues fall under two criteria. The issue reference will only be listed under one of the applicable criteria.

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| 1.2.4 Captions (Live) (Level AA)<br><br>Captions are provided for all live audio content in synchronized media. | Supports | Live audio content is not present. |
| 1.2.5 Audio Description (Prerecorded) (Level AA)<br><br>Audio description is provided for all pre-recorded video content in synchronized media. | Supports | Pre-recorded video content for synchronized media is not present. |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| 1.4.3 Contrast (Minimum) (Level AA)<br><br>The visual presentation of text and images of text has a contrast ratio of at least 4.5:1. | Supports with Exceptions | Some content does not have a color contrast ratio of at least 4.5:1. |
| 1.4.4 Resize text (Level AA)<br><br>Text can be resized without assistive technology up to 200 percent without loss of content or functionality (see Exceptions). | Supports with Exceptions | Some text cannot be resized up to 200% without overlapping other content in some cases. |
| 1.4.5 Images of Text (Level AA)<br><br>If the technologies being used can achieve the visual presentation, text is used to convey information rather than images of text. | Supports | Text is not conveyed as images of text. |
| 2.4.5 Multiple Ways (Level AA)<br><br>More than one way is available to locate a Web page within a set of Web pages. | Supports | All Web pages have multiple ways of navigation. |
| 2.4.6 Headings and Labels (Level AA)<br><br>Headings and labels describe topic or purpose. | Supports | Headings and labels on all pages describe the topic or purpose. |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| 2.4.7 Focus Visible (Level AA)<br><br>Any keyboard operable user interface has a mode of operation where the keyboard focus indicator is visible. | Supports with Exceptions | Some elements obtain partial visible focus or no focus at all when users navigate to them. |
| 3.1.2 Language of Parts (Level AA)<br><br>The human language of each passage or phrase in the content can be programmatically determined. | Supports | There are no changes in language within the page. |
| 3.2.3 Consistent Navigation (Level AA)<br><br>Navigational mechanisms that are repeated on multiple Web pages within a set of Web pages occur in the same relative order each time they are repeated, unless a change is initiated by the user. | Supports | All Web pages have consistent navigation mechanisms. |
| 3.2.4 Consistent Identification (Level AA)<br><br>Components that have the same functionality within a set of Web pages are identified consistently. | Supports | All components with the same functionality are identified consistently. |
| 3.3.3 Error Suggestion (Level AA) | Supports | User input controls have suggestions to correct |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| If an input error is automatically detected and suggestions for correction are known, then the suggestions are provided to the user. | | errors. |
| 3.3.4 Error Prevention (Legal, Financial, Data) (Level AA)<br><br>For Web pages that cause legal commitments or financial transactions for the user to occur, that modify or delete user-controllable data in data storage systems, or that submit user test responses, at least one of the following is true:<br><br>» Reversible: Submissions are reversible.<br>» Checked: Data entered by the user is checked for input errors and the user is provided an opportunity to correct them.<br>» Confirmed: A mechanism is available for reviewing, confirming, and correcting information before finalizing the submission. | Supports | No legal commitments or financial transaction are present on the page. |

# TABLE 3. CONFORMANCE CRITERIA, LEVEL AAA

Note: WCAG 2 Level AAA conformance criteria were not evaluated.

# TABLE 4. WCAG CONFORMANCE REQUIREMENTS

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| 1. Conformance Level<br><br>One of the following levels of conformance is met in full.<br><br>» Level A: For Level A conformance (the minimum level of conformance), the Web page satisfies all the Level A Success Criteria, or a conforming alternate version is provided.<br>» Level AA: For Level AA conformance, the Web page satisfies all the Level A and Level AA Success Criteria, or a Level AA conforming alternate version is provided.<br>» Level AAA: For Level AAA conformance, the Web page satisfies all the Level A, Level AA and | Supports with Exceptions | Some of the Level A and Level AA conformance requirements are met. Level AAA was not evaluated |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| Level AAA Success Criteria, or a Level AAA conforming alternate version is provided. | | |
| 2. Full pages<br><br>Conformance (and conformance level) is for full Web page(s) only, and cannot be achieved if part of a Web page is excluded. | Supports with Exceptions | The full page was audited for issues, however, within each page there was only partial conformance to the guidelines. |
| 3. Complete processes<br><br>When a Web page is one of a series of Web pages presenting a process (i.e., a sequence of steps that need to be completed to accomplish an activity), all Web pages in the process conform at the specified level or better. (Conformance is not possible at a particular level if any page in the process does not conform at that level or better.) | Supports with Exceptions | The entire process of reserving a room and viewing a schedule was evaluated, but the pages in the process only partially conformed to the guidelines. |
| 4. Only Accessibility- | Supports with Excep- | The pages audited were tested using a com- |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| Supported Ways of Using Technologies<br><br>Only accessibility-supported ways of using technologies are relied upon to satisfy the success criteria. Any information or functionality that is provided in a way that is not accessibility supported is also available in a way that is accessibility supported. | tions | bination of assistive technologies: the latest versions of JAWS and NVDA in both latest versions of IE and Firefox. Additionally, keyboard-only support was tested in IE, Firefox and Chrome. Where the application meets a conformance requirement, accessibility-supported ways of using technologies was supported. Where conformance requirements were not met, assistive technologies were used in the testing, but coding errors created barriers to assistive technology users. |
| 5. Non-Interference<br><br>If technologies are used in a way that is not accessibility supported, or if they are used in a non-conforming way, then they do not block the ability of users to access the rest of the page. In addition, the Web page as a whole continues to meet the conformance requirements under each of the following conditions:<br><br>1. When any technology that is not relied upon is turned on in a | Supports | The parts of the pages that assistive technology users cannot access due to coding errors do not prevent assistive technology users from accessing other parts of the pages that do meet conformance requirements. |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| user agent,<br>2. When any technology that is not relied upon is turned off in a user agent, and<br>3. When any technology that is not relied upon is not supported by a user agent | | |

# 2017 SECTION 508 REPORT

## FUNCTIONAL PERFORMANCE CRITERIA

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| 302.1 Without Vision | Supports with Exceptions | Some images, active elements (links and buttons), and form controls lack accessible names necessary for assistive technologies |
| 302.2 With Limited Vision | Supports with Exceptions | Some color contrast problems exist. Some content cannot be enlarged to 200%. |
| 302.3 Without Perception of Color | Supports with Exceptions | Some links are identified with color alone. |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| 302.4 Without Hearing | Supports | No audio content is present |
| 302.5 With Limited Hearing | Supports | No audio content is present |
| 302.6 Without Speech | Supports | No speech is required for operating the application |
| 302.7 With Limited Manipulation | Supports with Exceptions | Some interactions require using a mouse |
| 302.8 With Limited Reach and Strength | Supports with Exceptions | Some interactions require using a mouse |
| 302.9 With Limited Language, Cognitive, and Learning Abilities | Supports with Exceptions | Some interactions will create challenges for users with some cognitive or learning impairments |

# HARDWARE

Note:  This is not a hardware product.

# SOFTWARE

Notes:

- Examples of "Platform software" are desktop operating systems; embedded operating systems, including mobile systems; Web browsers; plug-ins to Web browsers that render a particular media or format; and sets of components that allow other applications to execute, such as applications which support macros or scripting.
- Examples of "Software Tools" are defined as Software for which the primary function is the development of other software. Software tools usually come in the form of an Integrated Development Environment (IDE) and are a suite of related products and utilities. Examples of IDEs include Microsoft® Visual Studio®, Apple® Xcode®, and Eclipse Foundation Eclipse®.

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| 501 Scope - Incorporation of WCAG 2.0 AA | See WCAG 2.0 section | |
| 502 Interoperability with Assistive Technology | | This section only applies to "platform software." |
| 502.2.1 User Control of Accessibility Features | Not Applicable | This application is not "platform software." |
| 502.2.2 No Disruption of Accessibility Features | Supports | The application does not disrupt accessibility features. |
| 502.3 Accessibility Services | | This section only applies to "platform software" and |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| | | "software tools." |
| 502.3.1 Object Information | Not Applicable | This application is not "platform software" and is not a "software tool." |
| 502.3.2 Modification of Object Information | Not Applicable | This application is not "platform software" and is not a "software tool". |
| 502.3.3 Row, Column, and Headers | Not Applicable | This application is not "platform software" and is not a "software tool." |
| 502.3.4 Values | Not Applicable | This application is not "platform software" and is not a "software tool." |
| 502.3.5 Modification of Values | Not Applicable | This application is not "platform software" and is not a "software tool." |
| 502.3.6 Label Relationships | Not Applicable | This application is not "platform software" and is not a "software tool." |
| 502.3.7 Hierarchical Relationships | Not Applicable | This application is not "platform software" and is not a "software tool." |
| 502.3.8 Text | Not Applicable | This application is not "platform software" and is not a "software tool." |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| 502.3.9 Modification of Text | Not Applicable | This application is not "platform software" and is not a "software tool." |
| 502.3.10 List of Actions | Not Applicable | This application is not "platform software" and is not a "software tool." |
| 502.3.11 Actions on Objects | Not Applicable | This application is not "platform software" and is not a "software tool." |
| 502.3.12 Focus Cursor | Not Applicable | This application is not "platform software" and is not a "software tool." |
| 502.3.13 Modification of Focus Cursor | Not Applicable | This application is not "platform software" and is not a "software tool." |
| 502.3.14 Event Notification | Not Applicable | This application is not "platform software" and is not a "software tool." |
| 502.4 Platform Accessibility Features | Not Applicable | This application is not "platform software" and is not a "software tool." |
| 503 Applications | | |
| 503.2 User Preferences | Supports | The application allows user preferences from platform settings for color, contrast, font type, font size, |

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| | | and focus cursor. |
| 503.3 Alternative User Interfaces | Not Applicable | No alternative user interfaces are provided. |
| 503.4 User Controls for Captions and Audio Description | | |
| 503.4.1 Caption Controls | Not Applicable | No video content is present. |
| 503.4.2 Audio Description Controls | Not Applicable | No video content is present. |
| 504 Authoring Tools | | This section only applies to applications where users can author content. |
| 504.2 Content Creation or Editing | Not Applicable | This is not an authoring tool. |
| 504.2.1 Preservation of Information Provided for Accessibility in Format Conversion | Not Applicable | This is not an authoring tool. |
| 504.2.2 PDF Export | Not Applicable | This is not an authoring tool. |
| 504.3 Prompts | Not Applicable | This is not an authoring tool. |
| 504.4 Templates | Not Applicable | This is not an authoring tool. |

# SUPPORT DOCUMENTATION AND SERVICES

| CRITERIA | CONFORMANCE LEVEL | REMARKS AND EXPLANATIONS |
|---|---|---|
| 601.1 Scope | | |
| 602 Support Documentation | | |
| 602.2 Accessibility and Compatibility Features | Not Applicable | No documentation was evaluated. |
| 602.3 Electronic Support Documentation | Not Applicable | No documentation was evaluated. |
| 602.4 Alternate Formats for Non-Electronic Support Documentation | Not Applicable | No alternate formats were evaluated. |
| 603 Support Services | | ICT support services including, but not limited to, help desks, call centers, training services, and automated self-service technical support, shall conform to 603. |
| 603.2 Information on Accessibility and Compatibility Features | Not Applicable | No support services were evaluated. |
| 603.3 Accommodation of Communication Needs | Not Applicable | No support services were evaluated. |

# CONTACT 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 25: 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

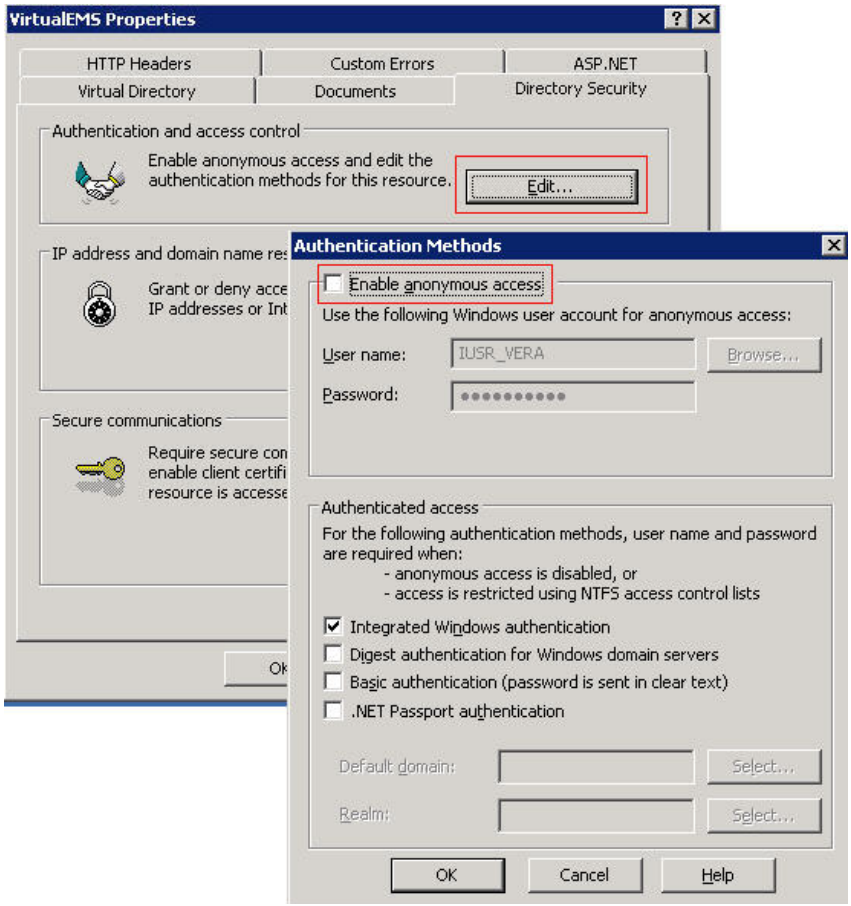
When a domain user who is logged on to a networked PC accesses an EMS Everyday User application, such as EMS Web App, EMS Mobile App, or EMS for Outlook, their Active Directory credentials (Domain\User ID) are compared against corresponding Domain\User ID information recorded in the **Network ID** and\or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

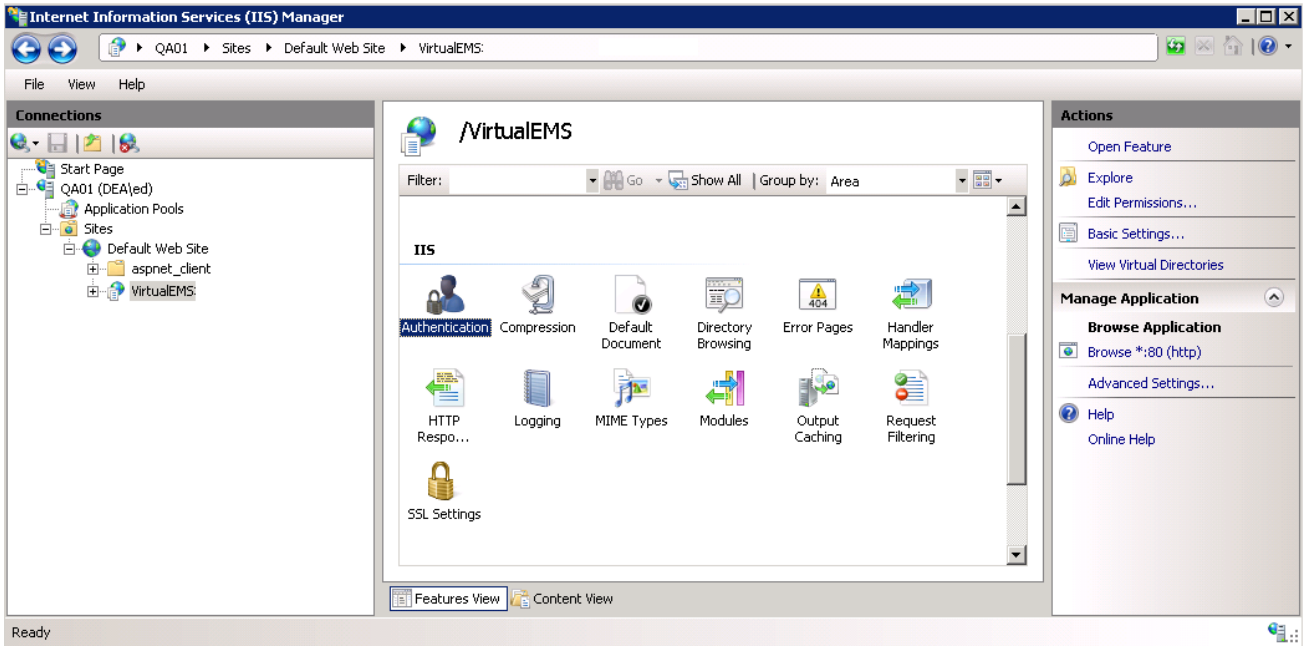
3. Right-click your EMS application's site and choose **Properties**. The Properties screen will open.
4. Go to the **Directory Security** tab and click the **Edit** button under the Authentication and access control section. The Authentication Methods screen will open.
5. Uncheck the **Enable anonymous access** option. The **Integrated Windows authentication** option should be the only option checked.



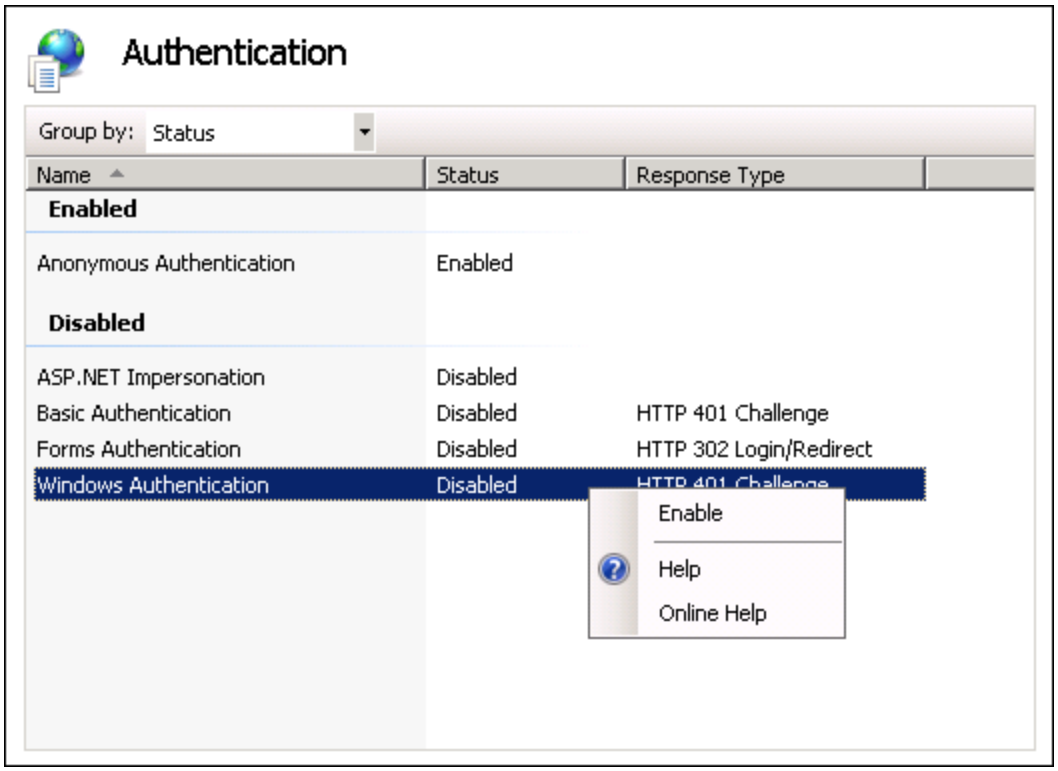
6. Click **OK** to exit the Authentication Methods screen. Click **OK** again to exit the Properties screen. You have completed the necessary IIS configuration steps for IIS 6.0.

# 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 26: 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

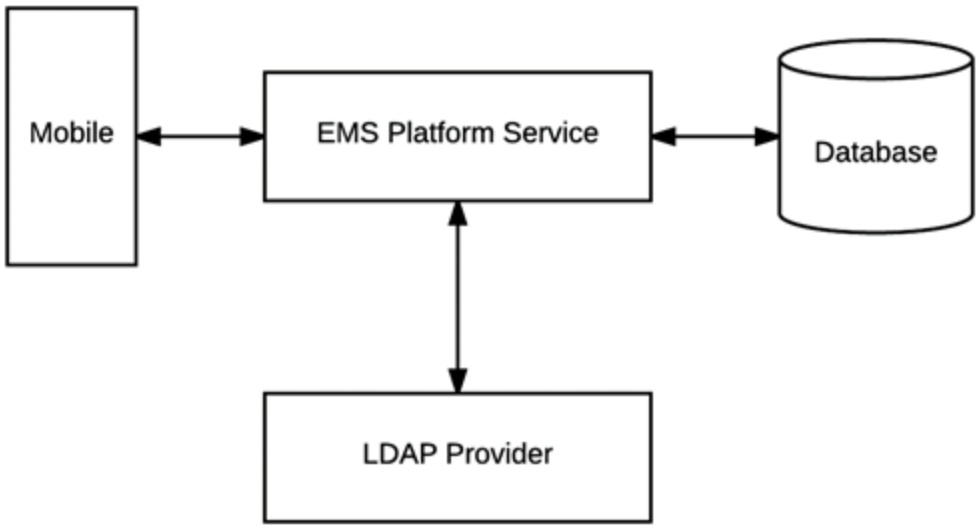
**Warning for Existing EMS Customers:** Before activating any Integrated

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 27: 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,

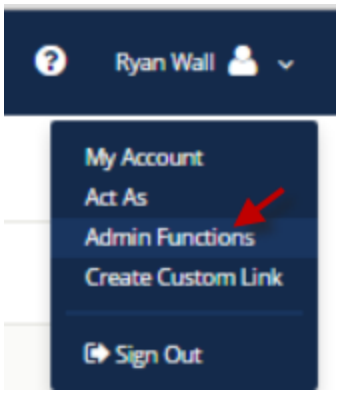
department, etc.) as a Directory Service object containing a property (i.e., member) that contains the users that belong to your various groups.

» 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.

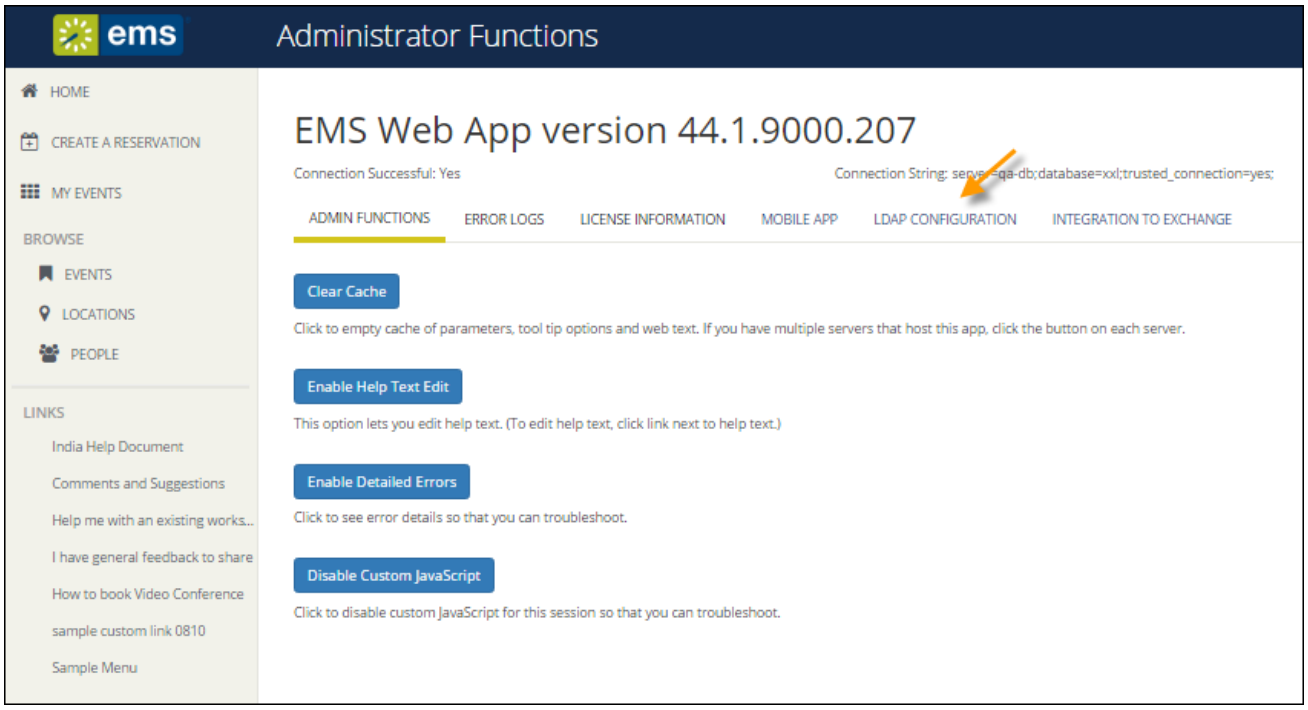
# CONFIGURE EMS WEB APP TO USE LDAP AUTHENTICATION

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**).

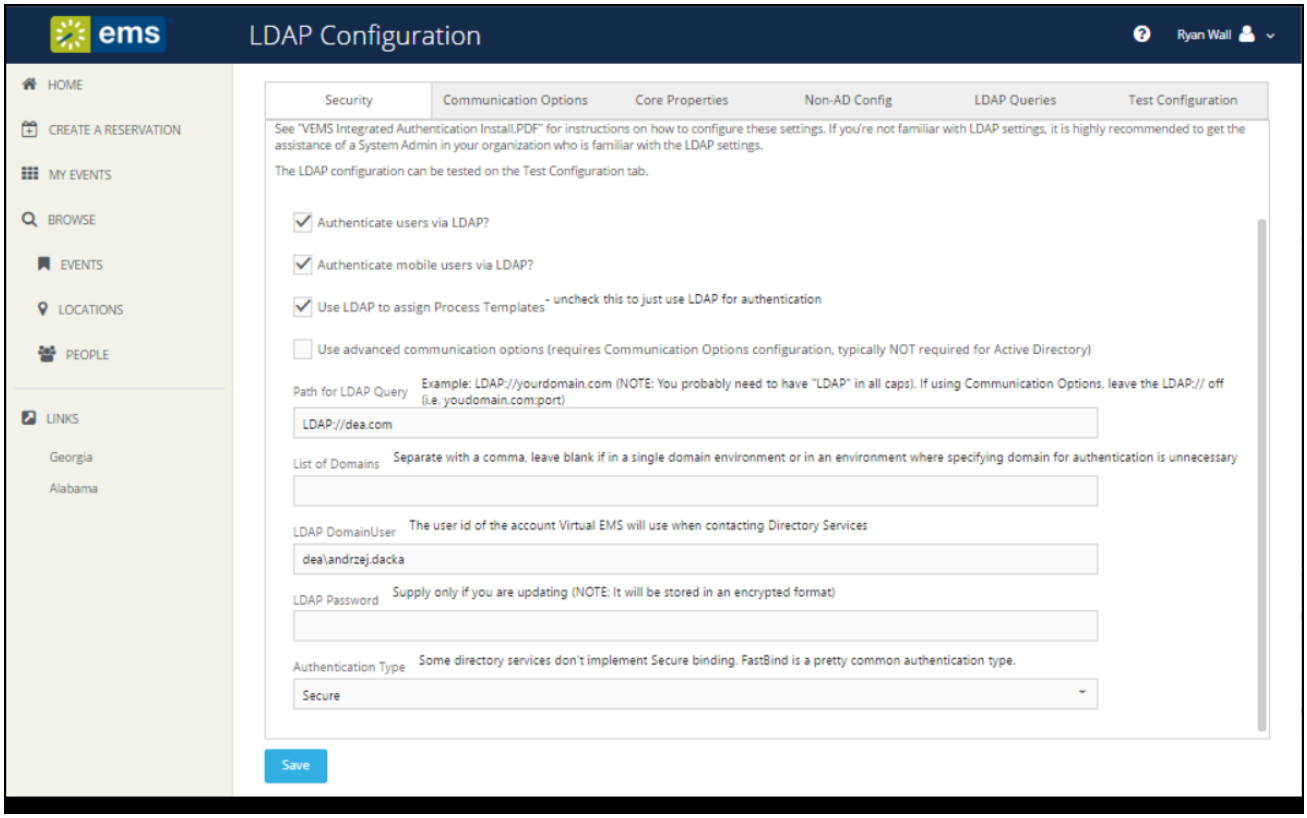
   See Also: Configure Security Templates
2. From the User Options, select **Admin Functions**.



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




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




# 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

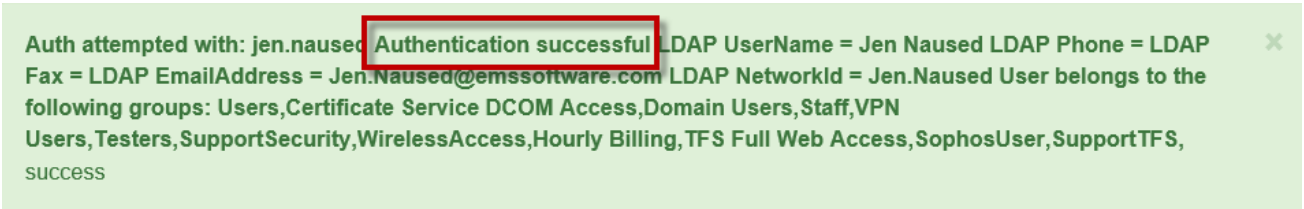
1. Click **Save**.

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).



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 28: 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<br>Session<br>Form<br>Cookie<br>Query String |
| Authentication | Portal Authentication Variable | User variable to be compared against the EMS Everyday User External Reference/Network ID field |

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

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

## REDIRECT USER LOG IN TO YOUR SSO PROVIDER

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

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

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

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

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

# SPECIFY A DIFFERENT DEFAULT HOME PAGE FOR GUEST USERS

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

# CHAPTER 29: 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]/ 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 30: Authentication Options for EMS Web App and Virtual EMS (VEMS)

Authentication is controlled by three factors.  They all must be configured correctly for the authentication to work:

1. **Login Credentials:** This is the location where external LDAP/Windows/Portal credentials need to be entered in our software for each user.
2. **Enabled by:** This is either a parameter or checkbox that needs to be enabled for the authentication to work.
3. **Configuration Page:** This is where configuration and options are set for the authentication.

## INTEGRATED WINDOWS AUTHENTICATION

- Login Credentials: Network ID / External Reference in web user account settings (Either of these work)
- Enabled by: Within IIS on the VEMS site, "Authentication" options, Windows Authentication enabled, Anonymous Authentication disabled
- Configuration Page: IIS "Authentication" options

# LDAP

- Login Credentials: Network ID / External Reference in web user account settings (This is specified by the "Field Used to Authenticate Web User" on the VEMS/EMS Web App Parameters tab).
- Enabled by: ldapconfiguration.aspx page, "Authenticate users via LDAP?" check-box (must be logged in with Web Admin security role and have Integrated Authentication in license).
- Configuration Page: ldapconfiguration.aspx page (there are multiple tabs).
- Other Notes: EMS LDAP License is required for this to work. The web server will need access to directory server for this to work.

# PORTAL

- Login Credentials: Network ID / External Reference in web user account settings (this is specified by the "Field Used to Authenticate Web User" on the VEMS/EMS Web App parameters tab).
- Enabled by: Always enabled; select the appropriate entry from the "Portal Authentication Method" on the VEMS/EMS Web App Parameters page
- Configuration Page: There are multiple different setup items in the VEMS/EMS Web App parameters under the "Authentication" area