

Version 25 | Trapeze Enterprise Asset Management

© 2025 Trapeze Software ULC, its subsidiaries and affiliates (collectively “TSU”). All rights reserved.

Trapeze Software ULC (“TSU”) Proprietary and Confidential: Information contained in this document is proprietary to TSU and its subsidiaries and may be used or disclosed only with written permission from TSU. This guide, or any part thereof, may not be reproduced without the prior written permission of TSU. The recipient acknowledges and agrees that disclosure of this document to recipient, and its use, are subject to the terms and conditions specified in their relevant software license agreement, software maintenance agreement, and/or non-disclosure agreement (“Governing Agreement”) under which this document was disclosed. This document is for internal use only in conjunction with TSU products. This document may not be modified in any way.

All other trademarks, registered trademarks, product names and company names or logos mentioned are the property of their respective owners.

Except as may be provided in the Governing Agreement, TSU and its affiliates, subsidiaries, officers, directors, employees, and agents provide the information contained in this manual on an “as-is” basis and do not make any express or implied warranties or representations with respect to such information including, without limitation, warranties as to non-infringement, reliability, fitness for a particular purpose, usefulness, completeness, accuracy or currentness. TSU shall not in any circumstances be liable to any person for any special, incidental, indirect or consequential damages, including without limitation, damages resulting from use of or reliance on information presented herein, or loss of profits or revenues or costs of replacement goods, even if informed in advance of the possibility of such damages.

TSU reserves the right, to be exercised at its sole discretion and without notice, to change, modify or adapt the contents of this edition in order to accurately reflect any future upgrades to the TSU proprietary software and/or hardware. In the event of such changes, TSU expects, but does not represent or guarantee, that this current edition will continue to remain reasonably accurate insofar as it describes the basic functions of the TSU proprietary software and/or hardware. Furthermore, based on your system settings, certain functionality, such as application screens, may not function exactly as shown or described in this guide.

Technical Support

Trapeze provides several ways to connect with the Customer Care team. Please provide detailed information to the representative. If you are reporting an issue by e-mail, include any error messages, screen shots of your problem, and steps to replicate the issue.

Customer Care is available Monday through Friday, 8:00 a.m. to 8:00 p.m., Eastern Standard Time.

Toll-Free Telephone: 1-877-411-8727

E-mail: cc@trapezegroup.com

FTP Site: <https://ftps.trapezegroup.com/>

Web Site: <https://collaborate.trapezegroup.com>

The website provides access to Trapeze Collaborate which offers resources to implement and operate the software, search knowledge, participate in communities, log/track service requests, sign-up for release alerts, view product health recommendations, and download updates or documentation. For secure access to Collaborate, contact Customer Care through the website or by calling the number above.

Product Compatibility

Refer to the latest [Product Compatibility](#) information on Trapeze Collaborate for requirements including operating system information, databases, Crystal reports, network protocol, HTTP servers and browsers that are supported.

Trapeze EAM™ - Administrator Guide

Version 25.x

February 2026

Contents

1. Overview.....	1
2. Requirements and Environment Planning	2
Database Server	2
Application Server	2
Web Modules Server.....	3
Internet Information Services (IIS).....	4
Reporting Server (Optional).....	6
Interface Server (Optional)	6
Web Modules Client Machine	6
Communications Infrastructure	7
Installer	7
Important Information	7
3. Install Application Server and Database.....	9
Unpackage Installer.....	9
Install Application Server	11
Create Database and Database Objects.....	12
Create MSSQL Server EAM Database.....	12
Create Oracle EAM Database	15
Create Application Service	16
4. Install and Configure Web Modules	18
Installing Web Modules	18
Configurator	19
Main Configurator Options	20
Web Tab.....	20
Authentication Tab.....	24
Database Tab	25
MAXQueue Tab	27
Reporting Tab.....	28
Options Tab	31
Logging Tab.....	33
Asset Index Tab.....	34
Data Services Tab	35

Advanced Tab.....	37
LDAP Tab.....	40
Config Files Tab.....	42
Finalizing Configuration.....	43
5. Install Data Services.....	45
Data Services and API Service Configurator.....	46
Port Exclusions	47
6. Install Reporting.....	49
Reporting Server Installation.....	49
Reporting Server Configuration	50
7. Install MAXQueue and Integration Designer.....	51
8. Configure Post-Installation	52
Configuring Permissions.....	52
Create Admin User via GUI	52
Enabling Access.....	53
9. Customize Web Modules.....	55
Admin Center.....	55
Administration Tasks.....	55
Manage Shortcuts.....	66
Manage Tabs.....	67
Passwords and PIN Numbers.....	71
Forgot Password?.....	71
Change Password.....	73
Change the PIN Number.....	73
Customizing Home Tab.....	74
Editing Modules and Layout of Home Tab	74
Quick Links Module.....	74
Welcome Module	77
User Interface (UI) Options.....	79
Enabling and Disabling UI Control Mode in Web Modules	79
Modifying a UI Control for a Web Modules Page	80
Access a Web Modules Tab via a Properly Formatted URL.....	89
Customize the Logo.....	89
Appendix A. Technical Configuration	90
A.1 Sharing and Migrating Tabs	90
Migrating Tabs from Test to Production.....	90
A.2 Creating URLs to Launch Web Modules Reports.....	92
URL Construction.....	92
Using Web Modules Reporting URLs in the Dashboard Module	94
Using Web Modules Reporting URLs in Web Modules HTML Pages	96

A.3	Formatting a URL to Access a Web Modules Tab	97
	URLs to Access a Web Modules Portal/Page	97
A.4	Mobile and Mapping DNS Settings.....	99
A.5	Running Applications in Console Mode	100
	Data Services	100
A.6	Restarting Web Modules.....	101
A.7	Network Configuration and Anti-virus Recommendations	101
A.8	Configure Single Sign-On (SSO).....	102
	SSO Methods	102
	GUI User Setup for SSO Activation.....	103
	Enable SSO via Configurator	103
	Single Sign-On Browser Configuration	104

1. Overview

The 25.x version of EAM is comprised of the following components: the Application Server, the Web Modules, and MAXQueue. Web Modules is a multi-tiered web-application and MAXQueue is an integration tool that provides interfacing opportunities with numerous vendors.

The system is supported by a database server, application server, and web server. The database server provides data access and storage which is part of the data access layer. The application server acts as part of the business logic layer, which implements the business rules for the product. The web server acts as part of the front-end presentation layer, providing a central web interface for your components.

The addition of specific modules allows your organization to improve performance and efficiency of fleet management. Installed modules may be accessed by everyone in your organization - from mechanics tracking work orders or managers pulling reports, to external customers wishing to view information and enter incidents or complaints.

This guide covers Administrator functions including environment planning, installation, general configuration, customization, and technical configuration topics.

2. Requirements and Environment Planning

The installation process for the EAM system requires the work of a Database Administrator for initial database creation and a System Administrator for installation of the application and configuration. This section provides the necessary details for environment planning, system configuration, and steps to create the initial database. Once the system has been designed and the database has been established, provide the necessary details to the System Administrator who will complete the application installation.

The information presented can be applied to standard configurations. Contact customer support as specified on the copyright page of this document for additional information or questions regarding your specific configuration.

There are three major components to consider when planning the configuration of your system.

- Database Server
- Application Server
- Web Modules

The Application Server and the Web Modules Server can reside on the same machine or separate machines while the Database Server is usually on a separate machine. Depending on your configuration, there may be multiple instances of Application Servers and Web Servers. You will need to run the Installer and create a Deployment for each physical machine in your configuration.

You may be planning for an optional reporting server or interface server for the Reporting and MAXQueue integrations. This section provides information for standard configuration. Please refer to the *Reporting Administrator Guide* or the *MAXQueue Administrator Guide* for additional details.

Database Server

The requirements for a database server depend primarily on the size of the database and the maximum number of concurrent users. Memory on the database server is a major factor affecting performance. It is recommended to allow for future expandability.

Application Server

The requirements for an application server depend on the number of concurrent users, number of active assets, and other variables specific to your organization.

Web Modules Server

The Web Modules Server must have Internet Information Server (IIS) installed since it is a web-based application and requires a web server to function. If your organization uses Crystal Reports, the machine on which this component is installed must have Open Database Connectivity (ODBC) back to the Database Server and Transmission Control Protocol/Internet Protocol (TCP/IP) connectivity to the Application Server. As such, it is strongly recommended that the Web Modules Server exists on the same network segment as both the Database Server and the Application Server.

❗ It is **critical** to upgrade the Application Server **before** upgrading Web Modules Server.

❗ ASP.NET 4.8.0 is a prerequisite for Web Modules Server 25.x.

The machine on which Web Modules will be installed or upgraded must meet the following prerequisites:

- Windows Server 2016, 2019, or 2022.
- Microsoft IIS. If IIS is not installed, consult your systems administrator, as the installation CD for the OS may be required for IIS installation.
- Install the roles and features as indicated:
 - Application Server -
 - .NET Framework 4.8.0
 - Web Server IIS
 - Web Server IIS -

▪ Common HTTP Features	<Select All - except WebDAV which is not required>
▪ Performance	<Select All>
▪ Health and Diagnostics	<Recommended for monitoring and troubleshooting, but not required>
▪ Security	<Select Windows Authentication and Forms Authentication>
▪ Application Development	<Select All - except CGI which is not required>
▪ Management Tools	<Select All - except Management Service which is not required>

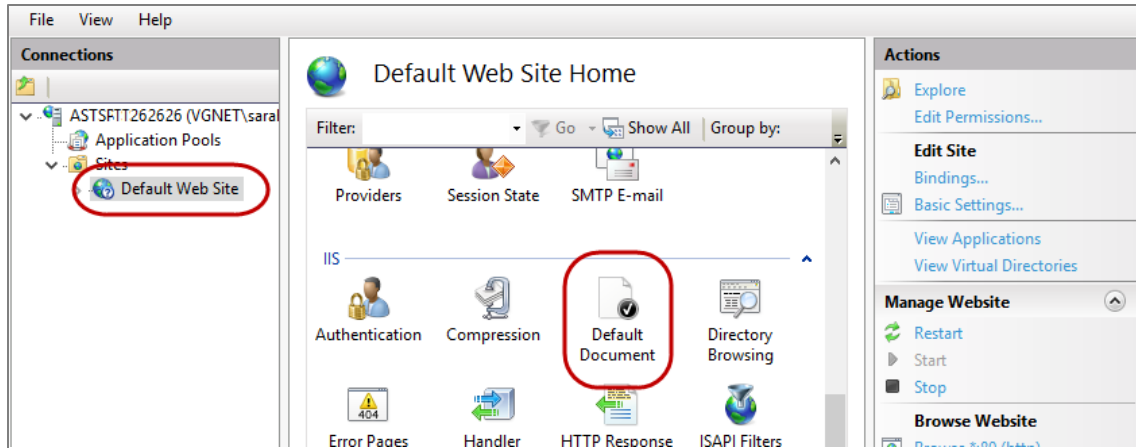
Install the following Windows features:

- .NET Framework Features
- SMTP Server <If you are implementing a local email server for Report Scheduling>
- User Interface and Infrastructure <Recommended for server management, but not required>
- Windows Identity Foundation 3.5
- Windows Process Activation Service
- WoW64 Support
- SQL Server users: The system server should use ODBC Driver 18 for SQL Server when creating your ODBC connections when described in installation documentation.
- Microsoft .NET Framework 4.8.0: EAM uses the Microsoft .NET Framework for interpreting and delivering reports as web content. Ensure that the .NET Framework you install is the Standalone Installer version and not the stripped-down version that comes with MS updates.
- If using Crystal Reports and the Reporting Module, ODBC Connections to all Databases must be created.
- Connectivity to a database. Please refer to the Administrator Guide for each Web Module for exact version requirement.
- Connectivity to an Application Server instance.
- For use with Oracle, a 64-bit Oracle client for the same version of Oracle as your database.

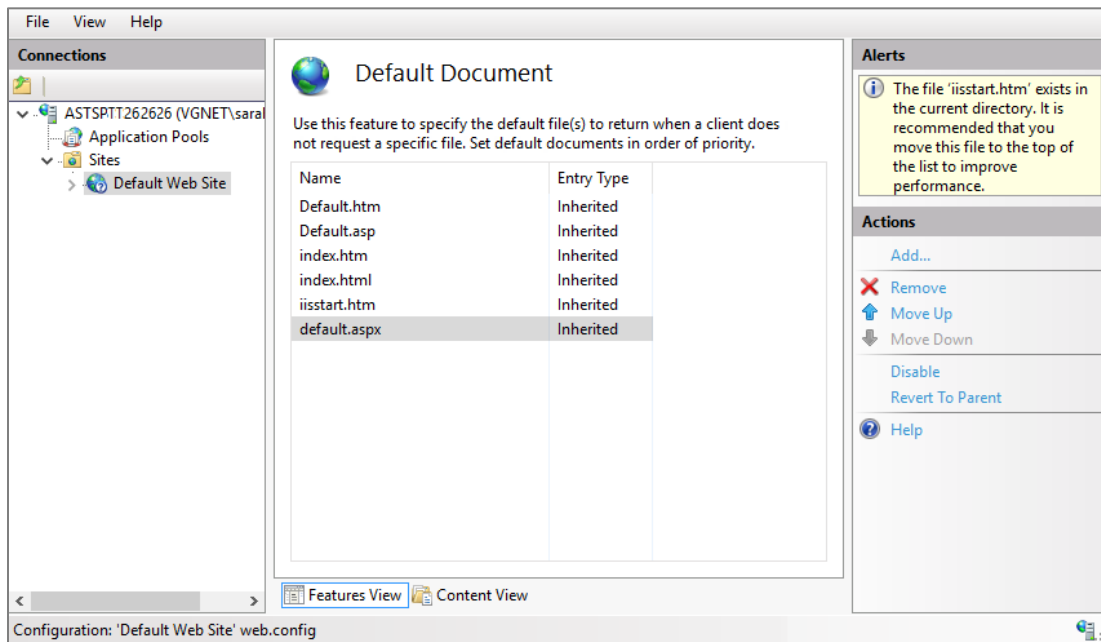
Internet Information Services (IIS)

The following steps are recommended to properly configure IIS.

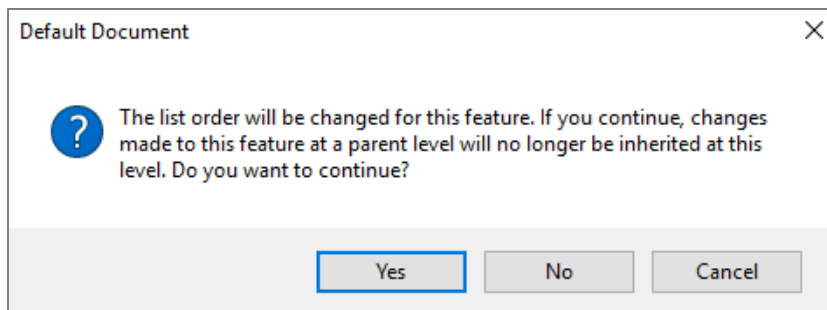
1. Launch IIS console (**Start > Search > inetmgr**) and click to run the program.
2. In the **Connections** pane, select the web application you configured for the web site and double-click on **Default Document** in the **Actions** pane.



The Default Document displays.



3. Select the **Default.aspx** in the **Features** view and use the buttons in the **Action** pane to move it up to the top of the list. If you see the following warning, click **Yes** to continue.



4. In the Connections pane, click Application Pools.

5. Select the application pool for the web application you configured for the Web Modules website and click **Advanced Settings**.

Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NET CLR V...	Managed Pipel...
.NET v4.5	Started	v4.0	Integrated
.NET v4.5 Classic	Started	v4.0	Classic
ASP.NET v4.0	Started	v4.0	Integrated
ASP.NET v4.0 Classic	Started	v4.0	Classic
DefaultAppPool	Started	v4.0	Integrated
DefaultApp_app	Started	v4.0	Integrated

Actions

- Add Application Pool...
- Set Application Pool Defaults...

Application Pool Tasks

- Start
- Stop
- Recycle...

Edit Application Pool

- Basic Settings...
- Recycling...
- Advanced Settings...**
- Rename

Remove

View Applications

Help

Reporting Server (Optional)

For organizations that require significant reporting, an additional server dedicated to Crystal Reports Server is recommended.

Interface Server (Optional)

For organizations that require significant interfaces with other systems, an additional server dedicated to the MAXQueue Integration Module is recommended. Microsoft Message Queuing (MSMQ) is a requirement for this additional server.

Web Modules Client Machine

To access the features available in Web Modules, an end user also needs the following:

- HTTP connectivity to the Web Modules Server.
- A valid system login User ID and Password. Exceptions include the Service Request, Dashboards, and Reporting modules that can be configured to not require a user login.

 When end users connect to Web Modules, they must first enter their User ID and Password. The Web Modules Server establishes a connection to a standard Application instance to validate login information and to read user configuration data.

- With proper hardware and software setup in place, Web Modules supports RFID log-in when single sign-on is enabled.

Communications Infrastructure

The presentation layer will run over wireless and local area networks, wide area networks, Intranets, the Internet, as well as dial-up connections for limited usage.

Installer

The Installer, which can be downloaded from the Customer Support website, will need to be run on any machine that will be installing or upgrading the application, web modules or MAXQueue servers. Each machine that will host these components needs .NET 4.8.0 installed to run the Installer. The database server does not need .NET 4.8.0 installed unless it is also hosting one of these components.

Important Information

- Special characters are not supported in all Web Module fields and unanticipated results may occur. Special characters include any character not found on a standard keyboard.
- User defined required fields that do not appear in Web Module forms will return validation messages.
- Popup blockers must be disabled for Web Modules to work properly.
- Opening links into new Windows or Browser tabs will cause Web Modules instability.
- Bookmarking Web Module pages inside of workflows is not supported.
- Using a DPI other than standard 100% could cause an issue with the headers in Enterprise Portal and the layout of fields in the GUI. It is recommended to not adjust DPI without doing testing to ensure the views in your workflows are not impacted.
- If your organization enforces location/department security, the user's assigned user groups must have location/department security authorization for security to be applied to the user.
- Date and time for each user is displayed in their local time zone for daily use, and for processes like jobbing on and off tasks. Information stored on the database is based on the time zone of the database server.
- License files used by 3rd party libraries in the App Server, Web Modules, Data Services, and MAXQueue are stored in the respective folder for that item, such as:
 - <deployment>/Licenses/AppServer

- <deployment>/Licenses/WebModules
 - <deployment>/Licenses/DataServices
 - <deployment>/Licenses/MaxQueue
- ❗ Any person who uses EAM agrees that information provided to the software will be stored and used by the system and may be shared with other users of the system, the software publisher, and the organization to whom the software is licensed. This includes, but is not limited to, the contents of any uploaded files, information about the user's geographic location, GPS/GIS information contained in images and photographs, and any personal contact information entered into the system.
- ❗ Do not use the browser's **Back** button.
- ❗ Do not use the browser's **Refresh** button (or the F5 shortcut). Gadget-based portals include a refresh functionality as defined in the module.

3. Install Application Server and Database

The installation of the Enterprise Asset Management system requires the work of a Database Administrator for initial database creation before installing the application. Get the database location and necessary details from your Database Administrator to complete this process.

Installation Steps:

The following provides high-level steps for installation.

1. Unpackage Installer
2. Install Application Server
3. Create Database and Database Objects
4. Create Application Service
5. Install Client Application - GUI
6. Install Web Module Server
7. Install Data Services
8. Install Reporting (Optional)
9. Install MAXQueue and Integration Designer (Optional)
10. Configure Installation

Requirements:

- The name or IP address of the application server
- The port of the application instance
- The database server name
- The name of the database to which you are connecting (applies to MSSQL and Oracle)

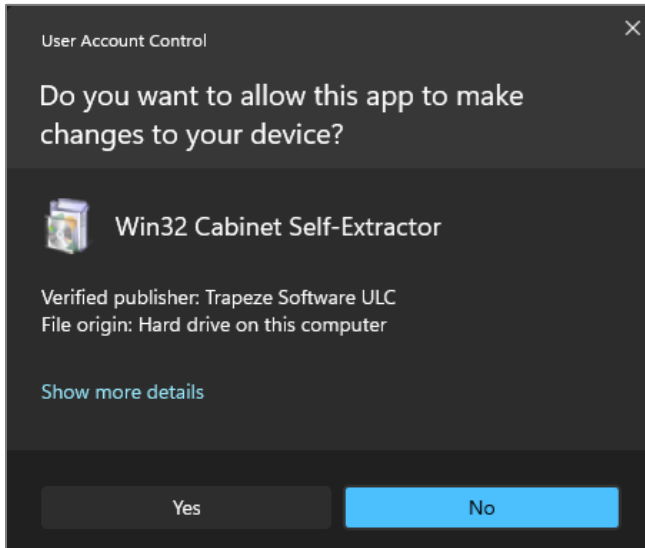
Database user IDs and passwords for DBA, App, and View users which are typically EMSDBA, EMSAPP, and EMSVIEW.

Unpackage Installer

1. Locate and run the Base Installer. The Installer will need to be run on each machine that will host an application, and .NET 4.8.0 will need to be installed on each machine to run the installer.

 The Installer can be downloaded from the Customer Support website. When unzipping the file, it may need to be unblocked. To unblock this file, right-click the file, click **Properties**, and click **Unblock**.

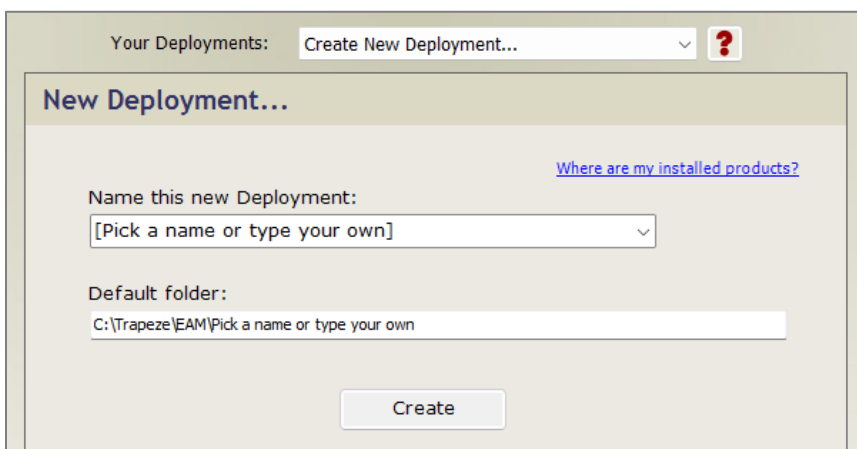
2. Right-click **EAMSetup.exe** and then select **Run as administrator**. User Account Control may present an administrative dialog box. Click **Yes**.



The Installer will extract.

3. Select **Create New Deployment** from the Your Deployments drop-down list.
4. Name the deployment and select the default folder where each item will be installed. It is recommended that the default path is used; however, the default path can be changed if desired.

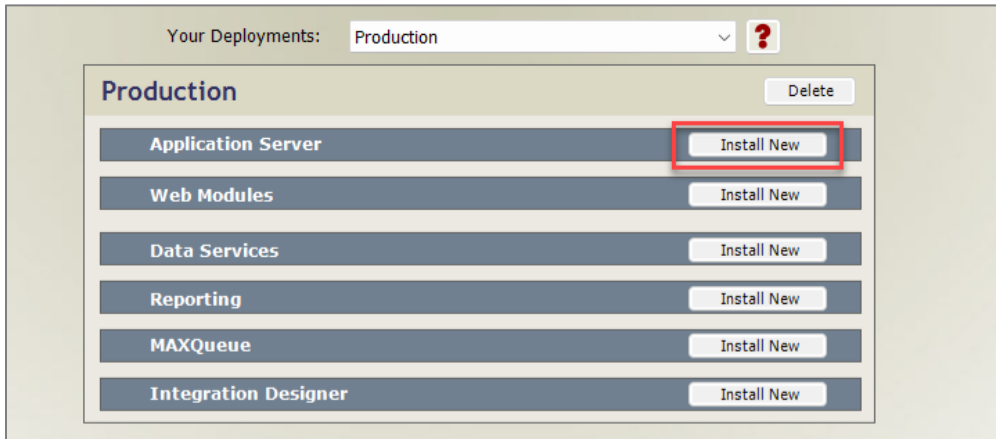
 Do not use version numbers in the deployment names.



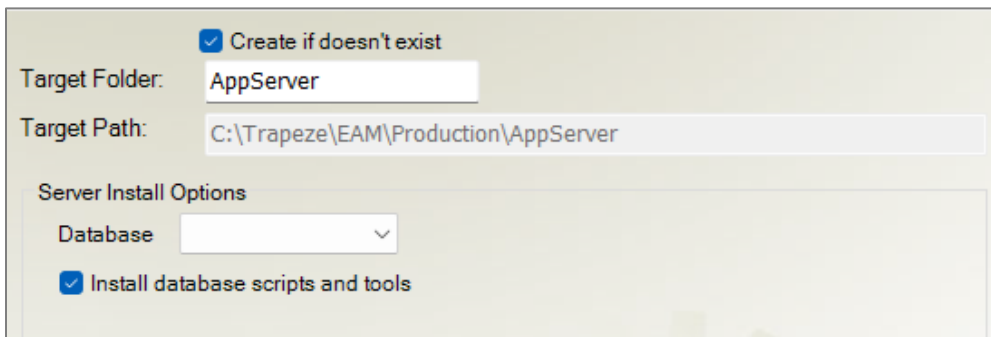
5. Click **Create**.

Install Application Server

1. From the Installer main page, click **Install New** next to the Application Server option.



2. Select the database from the dropdown on the Application Server Installer pop-in.



3. Click **Install Now**.
4. When the installation of the Application Server is finished, it will appear on the installer main page under the Application Server option.

The Application Server is now installed, and the database and database objects can be created.

Create Database and Database Objects

High-level Steps:

1. MSSQL Server or Oracle Client and Server must be installed.
2. EAM Application Server must be installed.
3. EAM Database must be created by using "proto.sql". ODBC cannot be created until this is done.
4. ODBC connections must be created.
5. Database scripts must be run to install EAM Schema into the Database. This includes tables, views, and database objects, and then pre-loads tables with base configuration data.

Create MSSQL Server EAM Database

Requirements:

- Supported version of MSSQL Server must be installed. Refer to the System Requirements and Compatibility Guide.
- Selected character set must support SQL_Latin1_General_CP1_CI_AS.
- Verify server authentication. The service or server must be restarted after the SQL Server and Windows Authentication setting is changed. Open SQL Management Studio. Right-click on your server and select **Properties**. Select **Security** from the menu on the left. Under Server authentication, change selection to **SQL Server and Windows Authentication**.
- EAM Application Server software must be installed.

Creating the MSSQL Server EAM Database:

1. Create EAM Database
 - i. Create an empty database in MSSQL for the EAM instance.
 - ✔ While using SQL Server Management Studio for the first run of proto.sql to create the first database, it is vital to "Run as Administrator." You must also be connected using either the System Administrator (SA) account or as an account with equivalent privileges.

- a. Open the proto.sql script in SQL Server Management Studio. It is located here:

C:\Trapeze\EAM\<Deployment Name>\AppServer\dbobjects\DBInit\110

- b. Edit the script according to your requirements and database configuration:

- **Database Name** – Update the six instances where the database is referred to as “proto” to “[Deployment Name]”. For example:

4	CREATE DATABASE	proto	4	CREATE DATABASE	M22
5	ON PRIMARY		5	ON PRIMARY	
85	GO		85	GO	
86	ALTER DATABASE	proto	86	ALTER DATABASE	M22
87	GO		87	GO	
88	ALTER DATABASE	proto	88	ALTER DATABASE	M22
89	GO		89	GO	
90	ALTER DATABASE	proto	90	ALTER DATABASE	M22
91	GO		91	GO	
92	ALTER DATABASE	proto	92	ALTER DATABASE	M22
99	GO		99	GO	
100	USE	proto	100	USE	M22
101	GO		101	GO	

- **Filename** – Update the file paths to reflect where you want these database files stored on disk. Be sure to keep the name of the files unchanged. For example:

7	NAME	= 'EMSMAN',	7	NAME	= 'EMSMAN',
8	FILENAME	= 'f:\proto\fa\emsmain.mdf',	8	FILENAME	= 'C:\Databases\MSSQL\M22\emsmain.mdf',
9	SIZE	= 20MB,	9	SIZE	= 20MB,
10	MAXSIZE	= 100MB,	10	MAXSIZE	= 100MB,
11	FILEGROWTH	= 1MB	11	FILEGROWTH	= 1MB
13	FILEGROUP EMSDATA1		13	FILEGROUP EMSDATA1	
14	(		14	(	
15	NAME	= 'EMSDATA1',	15	NAME	= 'EMSDATA1',
16	FILENAME	= 'f:\proto\fa\emsd1.ndf',	16	FILENAME	= 'C:\Databases\MSSQL\M22\emsd1.ndf',
17	SIZE	= 50MB,	17	SIZE	= 50MB,
18	MAXSIZE	= 100MB,	18	MAXSIZE	= 100MB,
19	FILEGROWTH	= 5MB	19	FILEGROWTH	= 5MB
23	NAME	= 'EMSDATA2',	23	NAME	= 'EMSDATA2',
24	FILENAME	= 'f:\proto\fa\emsd2.ndf',	24	FILENAME	= 'C:\Databases\MSSQL\M22\emsd2.ndf',
25	SIZE	= 50MB,	25	SIZE	= 50MB,
26	MAXSIZE	= 100MB,	26	MAXSIZE	= 100MB,
27	FILEGROWTH	= 5MB	27	FILEGROWTH	= 5MB

- **Size** - Edit the values based on your sizing requirements including maximum size and file growth.

✔ Use Find Replace functionality with whole word matching.

- c. Run the script by clicking **Execute**.
- d. Review the proto.log for errors. Contact technical support if there are errors.

2. Create ODBC Connections.

- i. Verify that the ODBC driver is installed on the App server for your version of Microsoft SQL Server.
 - ii. Launch Windows 64-bit ODBC Data Source Administrator.
 - iii. In the ODBC Data Source Administrator dialog box that appears, click the **System DSN** tab, and then click **Add**.
 - iv. In the Create New Data Source dialog box that appears, choose **ODBC Driver 18 for SQL Server** and then click **Finish**.
 - v. In the **Name** field, type the Database Name (DB Name).
 - vi. In the **Server** field, type the computer name of the database server and then click **Next**.
 - vii. Select **With SQL Server authentication using a login ID and password entered by the user**.
 - viii. In the **Login ID** field, type **emsdba**.
 - ix. In the **Password** field, type **emsdba**, and then click **Next**.
 - x. Click **Next** again on the following screen.
 - xi. Change **Connection Encryption** from **Mandatory** to **Optional**, then click **Back**.
 - xii. Choose the default database by selecting **Change the default database to**, and then select <DB Name> from the list.
 - xiii. Click **Next**, then click **Finish**.
 - xiv. Click **Test Data Source**.
 - xv. After the **Tests Completed Successfully** message appears, click **OK**.
3. Run scripts to create the database schema, objects, and load initial configuration data.
 - i. Open a command prompt to the following location:


```
C:\Trapeze\EAM\<Deployment Name>\AppServer\ldbobjects\
```
 - ii. From the command line, in that folder, input the following commands after replacing the listed variables:

<ODBC> is the name of the ODBC connection you made for the database.

 - **newdb emsdba/emsdba@<ODBC>**

- `newId emsdba/emsdba@<ODBC>`
- `uiLoad emsdba/emsdba@<ODBC>`

Create Oracle EAM Database

Requirements

- Supported version of Oracle client and server must be installed. Refer to the System Requirements and Compatibility Guide.
- EAM Application Server software must be installed.

Steps

1. Create EAM Database
 - i. Create an empty database in Oracle for the EAM instance.



Note: The database must be configured with the **WE8MSWIN1252** character set. Verify this before moving forward.

ii. Run scripts to create database users for the EAM database.

a. Open a command prompt to the following location:

C:\Trapeze\EAM\<Deployment Name>\AppServer\dbobjects\DBInit\ora10i

<Deployment Name> is the name given to your deployment when creating it.

b. From the command line, in that folder, input the following command after replacing the listed variables:

<Path> is the folder where the DB is located. This path cannot include any spaces.

<Password> is the password for the sys database user which is set when creating the database.

<TNS> is the name of the TNS entry for your database in the tnsnames.ora file used by your Oracle listener service.

- **fa <Path> "sys/<Password>@<TNS> as sysdba"**

iii. Run scripts to create the database schema, objects, and load initial configuration data.

a. Open a command prompt to the following location:

C:\Trapeze\EAM\<Deployment Name>\AppServer\dbobjects

b. From the command line, in that folder, input the following commands after replacing the listed variables:

<TNS> is the name of the TNS entry for your database in the tnsnames.ora file used by your Oracle listener service.

- **sqlplus emsdba/emsdba@<TNS> @newdb.sql**

- **exit**

- **sqlplus emsdba/emsdba@<TNS> @newld.sql**

- **uiloadd emsdba/emsdba@<TNS>**

Create Application Service

The application service can be created after the application and database servers have been set up. Running the system as a service is recommended, but it can also be run in console mode.

! Alert: If you will be running the system in console mode, it has been found that newer versions of Windows Server OS have changed default settings for consoles that result in higher CPU usage. It is recommended that you review the settings to ensure reasonable CPU usage.

The following steps describe how to create the application service.

1. Create a shortcut to fa_srv.exe on the desktop. This file is found in the application folder of the package you installed.
2. Right-click the shortcut on the desktop, select **Properties**, and then click the **Shortcut** tab.
3. Type in the target location on the Shortcut tab. It is recommended that the system name is used as a prefix for the service name and variable names so that they all display in the same area. An example is provided below, along with the individual information to enter.

Example: -install EAM.AppSrv.Production.3001 -p 3001 -d EAMPROD

- -install <EAM App Service name>
 - -p <Port Number>
 - -d when using MSSQL, enter <ODBC>
when using Oracle, enter <TNS>
4. Run the shortcut. You may need to right-click and select **Run as Administrator** to run the shortcut.
 5. From the Control Panel, double-click **Services**. Select the service that was created, and then click **Start**.
 6. Go to Properties > General Tab and set the Startup Type to **Automatic**.
 7. Review the log file to make sure the app initialized.

4. Install and Configure Web Modules

The Web Modules Server must have Internet Information Server (IIS) installed and permissions configured. If your organization uses Crystal Reports, the machine on which it is installed must have Open Database Connectivity (ODBC) back to the Database Server and Transmission Control Protocol/Internet Protocol (TCP/IP) connectivity to the Application Server.

Installing Web Modules

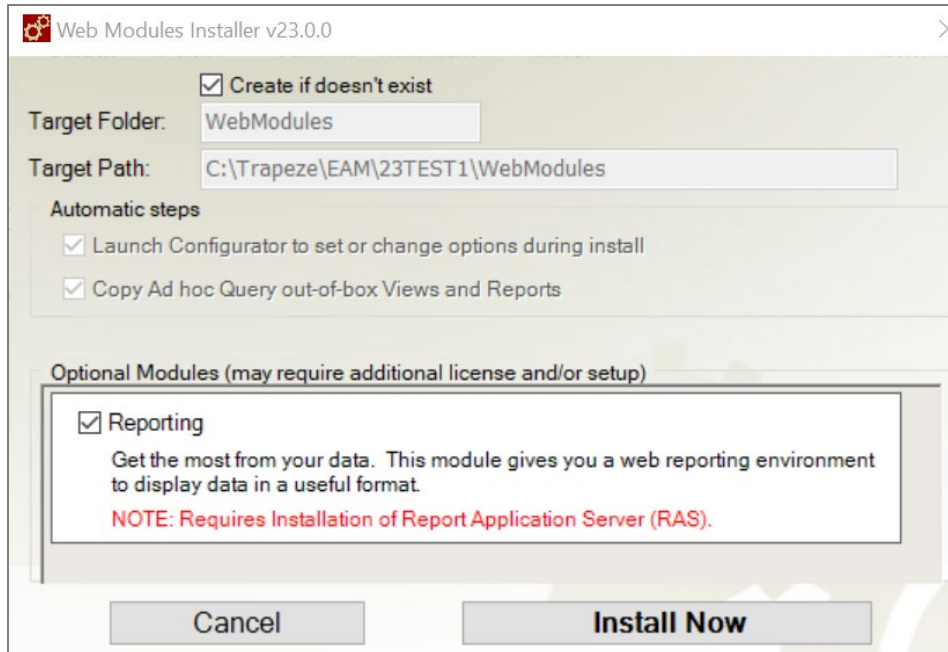
1. From the Installer, choose a deployment from the **Your Deployments** drop-down list. It is recommended that the web modules are installed on the same server as the application.

If installing the Web Modules on a separate server for the application server, do the following:

- i. Select Create New Deployment.
 - ii. Name the deployment the same as the application server deployment.
 - iii. Enter the correct drive letter in the Default Folder section.
 - iv. Click Create. This creates the deployment folder in the directory path entered in the Default Folder section.
2. In the Web Modules section, click **Install New**.



3. Leave the target folder as the default WebModules.
4. Select any optional modules that your organization will be using.
5. Click **Install Now**.



The Installer will automatically launch the Configurator.

6. Configure the Web Modules using the Configurator.

 After the installation has finished, you will be prompted to review the reporting-views-errors.log. If you are running an instance without telematics, the log file will always contain errors. Ignore these errors as they are considered acceptable.

Configurator

The Configurator tool is designed to assist customers in configuring the web product. It should be used to perform all edits to the web.config file. It properly sets the base web.config file settings required for the proper version of application software that you are using and allows the site administrator to quickly review and set any required configuration settings. The Configurator analyzes your system and writes the proper value to the web.config file based on the IIS version, values entered by the system administrator, and other key factors.

While installing or reinstalling the web product, the Configurator will be launched once all files are copied. After clicking **Install Now** or **Upgrade Now** from the main Installer, the Configurator for the current web instance will display. It will read any existing settings you had if this is an upgrade. If the Configurator is closed or does not launch automatically, it can be launched in the following ways:

- Web Modules: Directly using **Configurator.exe** found in <installation directory><instance name>\WebModules\Web\bin

- Reporting Module: Directly using **Configurator.exe** found in <installation directory>\<instance name>\ReportingModules\Web\bin
- Through the installer when installing base Web Modules or Reporting Module and checking the "Launch Configurator" option
- Using the **Config** button on the installer

The Configurator consists of many tabs that allow setting values for different areas. In the upper right corner, you will see the IIS version that was determined to be on the current machine. It also displays the best guess of the operating system (OS). If this is a new installation, the default settings will be loaded for your IIS version as determined by your OS:

- Windows 2022 = IIS 10
- Windows 2019 = IIS 10
- Windows 2016 = IIS 10
- Windows 2010 = IIS 8.5 / IIS 10

Please note that many installations require adjusting advanced settings within IIS, many of which are not supported by Configurator. However, it is possible to install a working instance without using the IIS management tools directly by using the **Web** tab as explained in the [Web Tab](#) section below.

Main Configurator Options

Two main application buttons display at the bottom of the Configurator:

Exit: When you click **Exit**, you will be reminded to save any changes you may have made to the settings. Click **OK** to exit the Configurator.

Save and Restart Web Application: After setting or confirming all the tab option values, you must save the web.config file before these changes will take effect.

✔ You must save the web.config on an upgrade or new install of your Web version at least once before the Web instance will function.

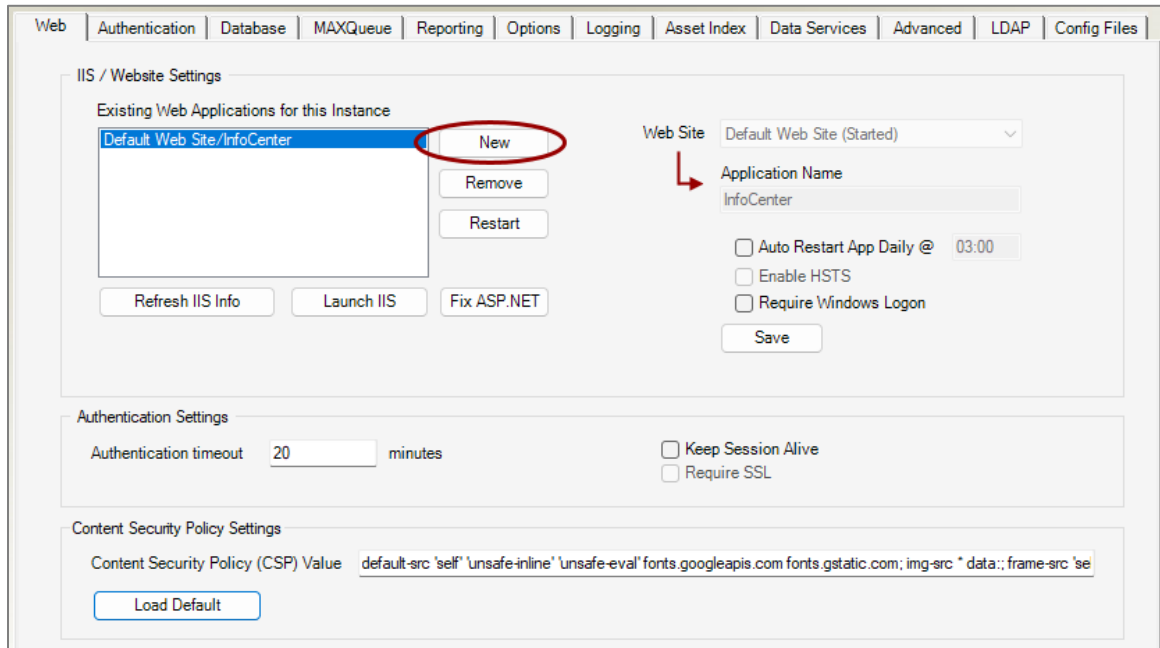
❗ Saving this file will restart the Web application pool as the web.config file will be altered.

Web Tab

If new install, you must create at least one web application for the instance. More than one web application is needed if you want one web application for Single Sign-On/Windows authenticated users and a separate web application for anonymous users.

Creating a New Web Application

1. Click **New**.



2. Choose a **Web Site**. This will determine how users connect to Web Modules.

The Web Site you choose will determine which TCP/IP port is used, among other things. Typically, this should be the Default Web Site running on Port 80.

- ✓ If you wish to manage or view the available web sites, use IIS management tools (you can click **Launch IIS** to get there easily). It is safe to use IIS to make changes while Configurator is running. If you make changes, just click the **Refresh IIS Info** button in the configurator when you are finished, and it will update the list of web sites and applications.

The Web Site determines the first part of the URL to access Web Modules. For example: `http://hostname:port/`.

- ✓ “:port” is only required if it is not port 80. A typical URL will look like:
`http://webserver.company.com/appname.`

3. Choose an **Application Name**. This is the name of the application (virtual directory) under which this installed instance of web modules will run.

- The application name determines the latter part of the URL to access Web Modules. For example, if you choose “Web Modules” for the application name, the Web Modules URL will look like: `http://hostname:port/Web Modules`.



A special case exists for SSL/HTTPS: Secure Sockets Layer which requires additional setup within IIS. Contact your system administrator for details.

4. Choose the time for **Auto Restart App Daily**. This is the time at which the daily application restart occurs. This option is disabled by default. Turning it on is only advised for high usage web apps with minimal downtime.
5. **Enable HSTS**: This allows the usage of HTTP Strict Transport Security available in IIS 10.0 v1709. HTTP Strict Transport Security (HSTS) is a security measure to ensure that users do not use regular HTTP when HTTPS is available on a site.



This setting is web site wide, meaning this affects ALL web applications under a site within IIS. Please keep this in mind if you wish to enable.

- It is advised if you have cases where users cannot use HTTPS due to certificate issues or other concerns, you set up another site to function without HSTS.
 - If you ever need to modify specific details, do so within IIS Manager. The Web Configurator simply sets defaults and only controls if HSTS is enabled or not.
 - The defaults for the Strict-Transport-Security header are max-age set to 31536000 (one year), includeSubDomains is true, and redirectHttpToHttps is true.
 - This setting controls if HSTS is enabled and its redirectHttpToHttps is enabled as it works independently of the enabled attribute.
6. **Require Windows Logon**: This is disabled by default. If **Require Windows Logon** is checked, then anonymous access will be disabled, and users accessing the website will be prompted for windows/domain credentials.
 - Reasons to check this option:
 - Added security in the event that you expect all of the application users to have windows domain accounts.
 - If you want to use Single Sign-On, you MUST check this box.
 7. Click the **Save** button within the IIS / Website Settings section to create the new web application or to save changes to the existing web application.
 - ✓ The **Save** button within the IIS / Website Settings section will not save the other configuration options. Use **Save and Restart Web Application** to save other configuration options. It is strongly recommended that you configure and save the IIS/Website Settings before moving on to the other settings.
 8. To change the options for an existing web application, click on the application in the list, change the options as desired, and click **Save** (or **Cancel** to abort).

✔ You may notice a slight delay while IIS is making the changes in the background.

9. Setup the web.config authentication settings for Web Modules by continuing to the **Authentication Settings** area on the Configurator Web tab.

Authentication Settings



The screenshot shows the 'Authentication Settings' window. It contains a label 'Authentication timeout' followed by a text input field with the value '20' and the unit 'minutes'. To the right, there are two checkboxes: 'Keep Session Alive' and 'Require SSL', both of which are currently unchecked.

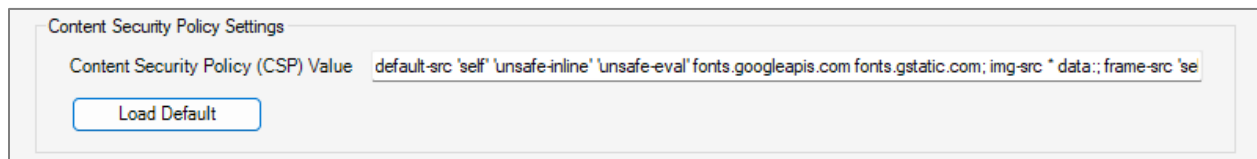
Authentication timeout: This is the amount of time in minutes a user can stay connected without using the portals before they are disconnected.

Keep Session Alive: Checking this box allows users to remain connected indefinitely.

Require SSL: This will allow an EAM admin or IT admin to set the IIS server to require any communication to web server once authenticated to be done through a secured HTTPS connection. Using HTTPS and SSL is recommended and should be considered a requirement for any production instance that is exposed externally.

- Disabled by default to ensure that it does not break any website that has mixed bindings. Please review your site to determine if you can enforce HTTPS for all users and turn this setting on. It is strongly advised to enforce HTTPS using the "Enable HSTS" setting on the web tab alongside this setting.
- This setting is only available if the IIS site has a configured HTTPS binding and an associated SSL certificate to that binding.

Content Security Policy Settings

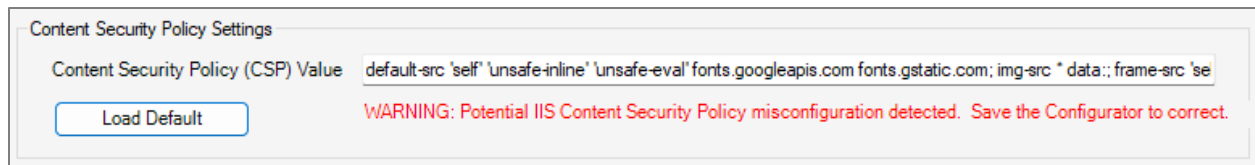


The screenshot shows the 'Content Security Policy Settings' window. It features a label 'Content Security Policy (CSP) Value' followed by a text input field containing the default CSP value: `default-src 'self' 'unsafe-inline' 'unsafe-eval' fonts.googleapis.com fonts.gstatic.com; img-src * data:; frame-src 'se`. Below the input field is a button labeled 'Load Default'.

Content Security Policies (CSP) allow an admin to control where content like images and scripts on a website can be loaded from and is a simple way to protect users by locking down the external resources that can be used.

By default, EAM will not enforce any CSP, but the Configurator will allow admins to specify a CSP that matches their requirements. A default CSP is provided that ensures standard EAM functionality continues to operate correctly and can be loaded via a button in the Configurator.

A misconfigured CSP can prevent EAM from working as intended.



This warning occurs when a *potential* misconfiguration is detected. This can occur for the following reasons:

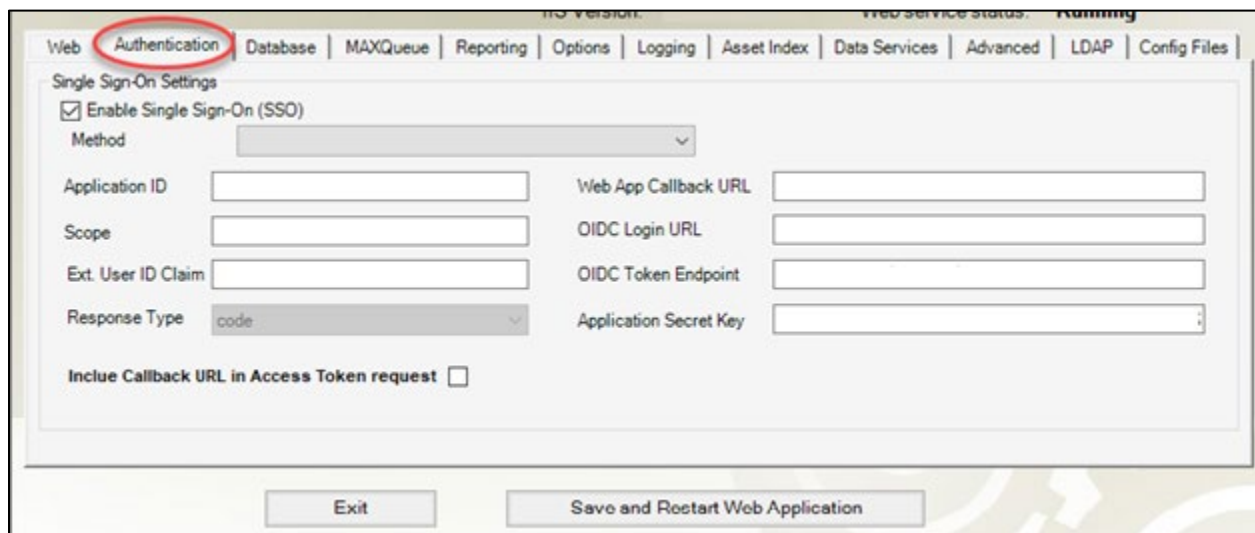
- CSP header is manually configured in IIS on the child application (for example, InfoCenter)
- CSP header is manually configured in IIS on the parent web site (for example, Default Web Site)

If the Configurator is used to configure the CSP, this scenario will not occur. Furthermore, when saving your settings in the Configurator, it will correct any misconfiguration that exists.

Authentication Tab

The Authentication Tab allows you to enable single sign-on (SSO) functionality and select the method you will be using for SSO.

It is possible to support a mixed environment if you have two or more web applications for this instance: configure one of the applications to **Require Windows Logon**, and another application to not require Windows logon. Trusted Single Sign-On users will use the URL for the application with Require Windows logon checked. Other users can use the other application. In the event that the user does not provide valid Windows credentials and is not automatically signed into Web Modules, the user's credentials can be used as an alternative.



Single Sign-On Settings

Enable Single Sign-On (SSO): Check this box to setup the environment for Single Sign-On.



You must also set IIS to disable anonymous access to use SSO. This can be done automatically by checking **Require Windows Logon** for one or more web applications in the list and then **Save**.

Method: Web modules supports SSO logins using the following methods. Please refer to the [Single Sign-On \(SSO\)](#) section for configuration details for each method and additional SSO information.

- Active Directory Federation Services (ADFS)
- Integrated Windows Authentication
- Lightweight Directory Access Protocol (LDAP)
- Microsoft Entra ID
- OpenID Connect

Database Tab

The Database tab contains settings that relate to the database and applications with which the web instance will connect.

The screenshot shows the 'FASuite Database' configuration window. The 'Database' tab is selected and circled in red. The window is divided into two main sections: 'FASuite Database' and 'FASuite Applications'.

FASuite Database Section:

- Database Type:** A dropdown menu.
- Database Server (IP / hostname):** A text input field.
- Database Name:** A text input field.
- Database Port:** A text input field with a 'Restore Default' button next to it.
- DBA Username:** A text input field containing 'emsdba'.
- DBA Password:** A password input field with masked characters (dots).
- App Username:** A text input field containing 'emsapp'.
- App Password:** A password input field with masked characters (dots).
- View (readonly) Username:** A text input field containing 'emsview'.
- View Password:** A password input field with masked characters (dots).
- Test Database Connections:** A button at the bottom right of the section.

FASuite Applications Section:

- Application Host Name or IP Address:** A text input field.
- Port Number:** A text input field with an 'Add' button next to it.
- Application Servers (at least one required; must connect to same database):** A list box containing one entry with a blue header.
- Test:** A button next to the list box.
- Test All:** A button below the 'Test' button.
- Remove:** A button at the bottom right of the section.

1. Choose or confirm your **Database Type, Server, Name, and Port**.
 - i. Database Type – MSSQL or Oracle
 - ii. Database Port – The port will load from FACommon.Configuration. Click the **Restore Default** button to load the default port for the selected database type.
2. Set or confirm the database connectivity information for the database that you plan to connect with the Web Modules.

DBA Username	emsdba	Password	
App Username	emsapp	Password	
View (readonly) Username	emsview	Password	
Test Database Connections			

All values are required. When using the configurator to set database passwords, passwords may contain more than 15 characters.

- **DBA Username** and **Password** are typically the EMSDBA user unless you have changed this value in your database.
 - **App Username** and **Password** are typically the EMSAPP user unless you have changed this value in your database. *Not required for MSSQL.
 - **View (read only) Username** and **Password** are typically the EMSVIEW user unless you have changed this value in your database.
3. Click the **Test Database Connection** button to test each user/password combination to ensure they are good connections to the database.
 - ✔ The test database connection button may take a minute or more depending on your environment.
 4. The **Database Connection Test** dialog informs you that the tests passed. Click **Close** to continue configuring the Database tab.
 5. Continue to the **Applications** area on the Database tab. You must enter at least one application server connection, but you can enter many if you wish to spread the load.

- i. Highlight the Application Server connection string in the list to the right and click **Remove** to remove that application from the connections list.

The application server no longer displays.

- ii. On the left side, enter the Application host name or IP address and port number and click the **Add** button.

The value is added to the list of application servers on the right.

- iii. Use the two test buttons in the FASuite Applications section to test either the selected application server or all the servers listed. Be sure the application is running before testing the connection.
 - Select an application connection string from the connections list box and click the **Test** button to test that application connection.

OR

 - Click the **Test All** button to test each connection string.

The connection results are returned.

6. Click **OK** when the Connection Successful dialog displays.

MAXQueue Tab

Operating System: **Windows 10.0 (64-bit)**
IIS Version: **10.0** Web service status: **Running**

Web | Authentication | Database | **MAXQueue** | Reporting | Options | Logging | Asset Index | Data Services | Advanced | LDAP | Config Files

MAXQueue Settings

MAXQueue Database User: Password:

Management Port:

☐ Enable Event Logging

Exit Save and Restart Web Application

If you make use of MAXQueue for any reason, please set these values.

- **MAXQueue database user and password:** These are the username and password used when MAXQueue connects to the database. By default, they should be UN: maxqueue PW: maxqueue.
- **Management Port:** This is a port used by software that is still in development. Its value should remain what it is by default.
- **Enable Event Logging:** Check this to enable logging of MAXQueue events as they pass through the enabled services. The log files can grow large, so this typically is only enabled when troubleshooting an issue.

Reporting Tab

The Reporting tab contains three sections: **Reporting**, **Crystal Reports Settings**, and **Scheduler Settings**. If your organization is only using Ad Hoc Query module, you only need to be concerned with the Reporting section. Those using Crystal Reporting, must complete BOTH the Reporting and Crystal Reports Settings sections on this tab.

The screenshot shows the 'Reporting' configuration window. The 'Reporting' tab is highlighted with a red circle. The 'Root Path to reports' field is set to 'C:\'. Below it, a note states: 'The root path contains Ad Hoc Query reports as well as Crystal reports, and is required even if you are not using Crystal Reports. You must grant the IIS worker process read and write permissions to this folder.' The 'Report Server' field is set to 'localhost'. The 'Reporting Request Timeout' is set to 110 seconds, with a note: '(Overrides the default machine.config value)'. The 'Report expiration window' is set to 30 seconds, with a note: 'Recommended value: 30 seconds. Higher value means that expired report connections will be left open longer. Lower values mean connections to the RAS will be closed sooner. Caution: using less than 15 seconds may cause open reports to be forcefully closed.' The 'Connection Information' section includes fields for 'ODBC Name' (QAM25_LOCAL), 'Database User' (emsvie), and 'Password' (masked). Buttons for 'Reporting Logo' and 'Replace Connection Info' are located on the right side.

Reporting Section

The Reporting section must be completed if your organization is using Ad Hoc Query or Crystal Reports.

- **Root Path to reports:** Root Path to reports must be entered to a shared reports folder if using external reporting. The directory to the shared reports folder **MUST** match the URL entered when setting up the External reports instance.

The **Root Path to reports** is the path to the reporting folder where the Query files are stored and the Crystal report files are located. This field should not be left blank. Create the folder if it does not exist and grant the appropriate web users permission to the folder (including write access to the Query sub folder, since that is where Ad Hoc Query reports are saved). This folder must have permissions for RAS to get to it and IIS user. Refer to the *Reporting Administrator Guide, Setting Up a Remote Crystal Report Application Server to Work with Web Modules (optional)* for more information on configuring RAS to access the reports.

- **Reporting Logo** – Click to configure logo that will display on reports.
- **Replace Connection Info** - The Report Connection Replacer Tool allows you to update the ODBC/TNS connection information for all reports in the reporting directory when changes are made in the Configurator. This tool aims to prevent the need for updates to the report connection on the first report run and reduces the likelihood of reports timing out. Click this button and a form with a tree-view displaying all the reports inside the report path will be displayed.



Note: The tool supports a silent mode which can be activated with the parameter “-s” allowing it to run without displaying the interface.

Crystal Reports Settings Section

Only complete the Crystal Reports Settings section if you are using Crystal Reporting.

- **Reporting Type:** Select the appropriate button depending on if you use a traditional or external reporting environment.
 - **Traditional Reporting:** Traditional reporting is using the reporting internally in the Web Modules.

Field	Example Entry
Report Server	• http://10.21.100.55 • 10.1.100.50 • https://10.21.100.55 • FleetProd

- **External Reporting:** External reporting is when you use an external server for reporting outside of the Web Modules. External Reporting Environment Fields:

Field	Example Entry
Report Server	Name of the machine housing the Crystal RAS.
Client Name or IP address	• http://68.21.155.37 • 68.21.155.37 • https://68.21.155.37 • FleetProd
Server name or IP address	• http://68.21.155.37 • 68.21.155.37 • https://68.21.155.37 • FleetProd
Instance name	FleetReporting

The following scenarios explain when to use which type of reporting.

Environment	Description
Traditional Reporting	Select Use Traditional Reporting Environment and enter the Report Server connection information for the location where the RAS server is located.
External Reporting Server with users within the firewall	Select Use External Reporting Environment and enter the Client name or IP address and the Instance Name. If users are behind the firewall, then you can access the report server directly without any translation to the IP address or server name.

Environment	Description
External Reporting Server with users outside the firewall	Select Use External Reporting Environment and enter Client name or IP address and Instance Name. You also need to enter the Server name or IP address for the external reporting instance. Behind the scenes, the page needs to communicate to the report server directly. The software allows the configuration of the client IP or server name so it can be used outside the firewall.

- **Report Server:** Server where Crystal RAS will be located.
- **ODBC Name:** The ODBC name to be used when running Crystal reports. Typically, this is an ODBC using the special Data Direct ODBC drivers for Crystal Reports.
- **Database User and password:** The database user and password to be used for running reports. We recommend using the view user EMSVIEW.
- **Reporting Request Timeout (seconds):** If you have reports that are longer running, you may wish to increase the default timeout for running a report. This is only recommended to be changed if you have these long-running reports, and we suggest you keep it as close to the default 110 as possible to ensure connections are closed in a timely manner when not in use.
- **Report expiration window:** This controls the number of seconds for the system to wait before closing a connection to the RAS that is no longer associated with an open report.

Options Tab

The **Options** tab provides a few options and file upload settings that can be set to make the user experience more enjoyable.

Web | Authentication | Database | MAXQueue | Reporting | **Options** | Logging | Asset Index | Data Services | Advanced | LDAP | Config Files

Features and Options

- ☐ Enable user-friendly error messages (Should always be enabled on a production server)
- ☐ Enable Reset Password ("Forgot Password" link on login page)
- ☐ Use pcProx cards on web login
- ☐ Disable Mapping integration

Website Page Title: Enterprise Asset Management

File Upload Settings

- ☒ Enable File Uploads (Enterprise Portal and Shop Activity modules)
- Maximum upload size: 12 MB
- Request timeout: 90 seconds
- Upload folder path: C:\Trapeze\EAM\Uploads

Web user(s) must have Read and Write access to folder

Features and Options

- **Enable user-friendly error messages:** This should always be checked in a normal working environment. It may be necessary to uncheck this when troubleshooting issues, but in most cases, we recommend leaving this checked.
- **Enable Reset Password:** Provides a **Forgot Password** link on the login page. This option requires the following to function correctly:
 - MAXQueue Notifications module must be configured correctly and enabled
 - Notifications module
 - Notifications - rule service enabled and the email server adapter configured
 - Data Event AWMMessageInsert enabled
 - A valid matching user ID in the USR_MAIN table. This matching user ID cannot be disabled, but an expired password is allowed to user this reset process.
 - The matching user ID record in the USR_MAIN table must have a valid email entered. Emails from the Operator table are not able to use this reset process.
- **Use pcProx cards on web login**
- **Disable Mapping integration:** Check this box to disable Mapping integration. It is enabled by default.
- **Website Page Title:** Define the title of the website page.

File Upload Settings

- **Enable File Uploads (Enterprise Portal and Shop Activity Modules):** These are enabled by default. Carefully consider whether you want to allow file uploads in Enterprise Portal/Shop Activity modules.
- **Maximum Upload Size and Request Timeout:** The upload size and request timeout values should not be set below the default values or errors may occur when uploads are attempted.
- **Upload Folder Path:** The upload folder path should be configured with correct web user permissions (the web application user needs permission to write to this folder).

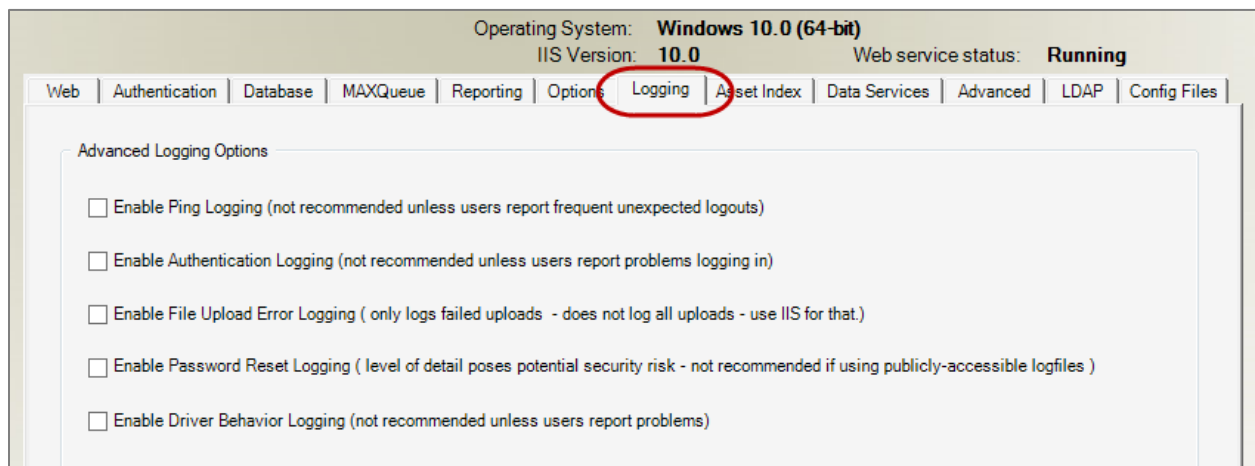
SMTP Settings

- **SMTP Server / SMTP Port**
- **Enable TLS:** If disabled, EAM will not attempt to secure the connection to the SMTP server using TLS. If enabled, EAM will require that the specified SMTP server have the TLS capability enabled and proper TLS certificates installed.
- **Override email address**
- **Authentication type:**
 - Anonymous – Use to connect to SMTP servers that do not require EAM to authenticate itself.
 - Basic Authentication – Use when the SMTP server requires valid credentials from EAM to send emails.
 - Microsoft Graph – Use to hook into Microsoft’s Cloud Office 365 and Azure platforms for sending emails. Requires additional setup and configuration.
- **Stop Scheduler**
- **Start Scheduler**
- **Remove Service**

Logging Tab

The tab has setup for logging options. Typically, you will use these options for troubleshooting with support.

Except for the Portal Identification option, the options on this tab are specifically for use with help from a customer support representative. Unless otherwise directed, please leave the default values in place for these advanced settings.



- **Enable Ping Logging** – Records the URL used and if exceptions are thrown from Data Service ping to allow easier debugging of ping process.
- **Enable Authentication Logging**
- **Enable File Upload Error Logging**
- **Enable Password Reset Logging**

When optional logging is turned on, the log will record the following:

- Any attempt to reset a password.
- A user and email address was found (in USR_MAIN) but the login failed. For example: User entered a bad password.
- The Users screen failed to load. This would be a rare application crash situation.
- The password reset failed to update the USR_MAIN record. This would mean a valid UserID was found, but the system failed to save the new password.
- The notification failed to get written to MSG_MAIN table. In this case, the system will attempt to revert the password to its original value.
- The notification failed to get written AND the password revert attempt failed.

The log will not record the following:

- Password reset succeeded
- UserID was not found in the database when trying to reset the password
- User was found in the database but there is no email address on the USR_MAIN table

Asset Index Tab

Operating System: **Windows 10.0 (64-bit)**
 IIS Version: **10.0** Web service status: **Running**

Web | Authentication | Database | MAXQueue | Reporting | Options | Logging | **Asset Index** | Data Services | Advanced | LDAP | Config Files

☒ **Enable Asset Index**
 Recommended; Asset Index is required for Search, Asset Chooser, Asset Portal, and Asset Condition Assessment

Asset Index Options

Rebuild index every minutes
 Recommended value: 10
 Higher value means that index is rebuilt less frequently and is less in sync with database.
 Lower values mean opposite. Index will not be rebuilt more than once per minute.
 Caution: using less than 10 minutes might thrash the database and web servers; monitor carefully.

Maximum search results shown in Asset Chooser
 Recommended value: 100
 More than a few hundred rows may result in poor browser experience and higher network traffic.

☐ **Include COMPONENT Assets**
 More assets => larger index and slower to sync. Additional Portal options may be required to see components.

☐ **Allow leading wildcard in searches**
 Not recommended. Results in inefficient use of index and slower search times.

☐ **Enable trace logging**
 Results in many log entries. Use only while troubleshooting.

The Asset Index tab provides options for configuring the Asset Index builder which is used for the Asset Chooser, Asset Condition Assessment, Asset Portal, and Search functionality within the application. It is recommended that you do not change these settings unless instructed by your Customer Support representative.

Data Services Tab

Web | Database | Authentication | MAXQueue | Reporting | Options | Logging | Asset Index | **Data Services** | Advanced | LDAP | Config Files

Data Services Integration Options

Service API

Protocol SSL Certificate

Host Port number

☒ **Enable API Cache**
☐ **Enable HSTS**

Swagger
Required when running Data Services in a TLS Offloaded environment.

Host

☐ **Exclude port in token URL**

Visually snap position to nearest marker if within distance units.

Data Services, which is used for getting map data, map tiles, MobileFocus, and other data via REST APIs, can serve requests outside of localhost.

By default, the service will run on `http://localhost:9000` and is available for use only by the application. By using the hostname or IP address of the machine, the service can be exposed for use from other servers or clients. If choosing to use a host other than localhost, be aware that there is no authentication or authorization built into this service, and any user or process that can access the host and port will be able to request data from the service.

Service API

Your system must have a valid (trusted) certificate and the appropriate port open on the firewall for these services to run.

SSL Certificate

The two SSL Certificate fields are drop-down menus that contain the options of all the certificates stores on the local machine personal certificate store.

Certificates can be stored on either your local certificate store, or in the WebHosting store. Because certificates in different stores can have the same common name, the drop-down list here displays either **Personal:** or **WebHosting:** followed by the name of the certificate.

Creating a Binding

Choose between HTTP and HTTPS for the protocol used to communicate with the API services. If you select HTTPS, you can select a certificate to create an SSL binding. If you install web and data services under the same deployment, they do not share the configuration. It is recommended that you select a certificate (not **None**) for the SSL certificate because data services should have that certificate bound. The scenarios involved when setting up this information are listed below.

Scenario	Result
HTTPS protocol is selected Certificate is selected.	An SSL binding for that port and certificate is created. If a binding exists for the previous value in this field, it will be deleted.
HTTPS protocol is selected No certificate is selected.	If there is a certificate bound to the previously configured port, this will be unbound. No certificate is bound to the newly configured port.
HTTP protocol is selected	The certificate field is disabled and set to None . If a binding exists for the previous value in this field, it will be deleted. No additional bindings are created.

Build next page links using https for SSL offloading environments for API responses

When enabled, API's NextPageLink will be constructed using HTTPS protocol regardless of what actual protocol is selected.

Enable API Cache

This option enables cache for API.

Enable HSTS

HTTP Strict Transport Security (HSTS) can be enabled for API by checking “Enable HSTS” checkbox on Data Services tab in configurator.

Swagger

This section allows configuring the public domain name to be used when the swagger web application needs to sign a user in to fetch results for an endpoint..

Host

- Leave this blank to have swagger use the configured Services URL (existing behavior).
- Set this to the public domain name to access the API. It will be used by Swagger when reaching back out to the API.

Exclude port in token URL

- Enable this when you have your environment setup to use a subdomain to map to the target port instead of explicitly specifying the port in the URL. (For example, api.mytransit.com vs www.mytransit.com:9000)

Advanced Tab

The screenshot shows the 'Advanced' configuration tab in the Trapeze EAM Administrator Guide. The 'Advanced' tab is highlighted with a red circle. The form contains the following sections:

- Portal Settings:** Includes fields for 'Portal Name' and 'External Logoff URL'. A note states: 'Portal Name determines the tabs this instance will show.'
- Enterprise Integration Options:** Includes a field for 'Encryption key'.
- Advanced Troubleshooting Options:** Includes two checkboxes:
 - ☐ Show session time remaining (in seconds) in top right corner. Not recommended for production servers.
 - ☐ Enable ASPX debugging (NEVER enable this on a production server!)
- Advanced Database Options:** Includes a dropdown for 'Database Connection Pooling Options' with the value '<DEFAULT>'. A note below states: '(Only change this if you know what you are doing.)'
- Encryption:** Includes a field for 'Deployment Encryption Key' with a masked value, a 'Show Key' checkbox, a 'Generate Key' button, and a checkbox for 'Enable secure messaging encryption (please refer to Configurator Guide before enabling)'.

Portal Settings

The Portal Identification section only applies if you are using or plan to use **multiple** installed instances of Web Modules that point to the **same** database (for load balancing, for example).

Portal Name: Each installed instance must have exactly one Portal Name. When installing multiple instances, a choice must be made for each additional instance: will it **share** the same tabs and modules as the other instances, or will it use **different** tabs and modules from the other instances?

- Instance with Shared Tabs and Modules:** To share the same tabs and modules with another instance, use the **same Portal Name** for each instance (the default value is "FASuite Web"). This is the most common method, and should be used in a load-balancing setup.
- Instance with Different Tabs and Modules:** To define an instance that has a different set of tabs and modules, use a **different Portal Name** from any other instance. This setup may be useful to an organization with distinctly different sets of users. For example: one instance for shop users (mechanics, supervisors, storekeepers, production managers), an instance for dashboards, PMM, and high-level reports (executives), and an instance for creating service requests and reservations (customers). In this example, each set of users would be given a different URL to access only the parts of the system

they need and may provide other benefits (upgrading the shop server without taking the customer server offline).

- If this is a new install, no extra steps are required.
- If this is an upgrade, additional steps are needed.

Upgrades:

In previous versions of Web Modules, tabs and modules settings were defined in a file named **PortalCfg.xml**. If this is an upgrade from version 6.3.x or lower, the existing **PortalCfg.xml** will be automatically loaded into the database where it will be managed from now on. This automatic load generally goes smoothly but if it does not you may see a **Server is unavailable** message in the web browser. If that happens, check **InfoCenter.log** in the LogDir for more information. If there is a configuration issue, the log file should describe the steps necessary to fix it. Some of the possible issues and solutions are:

- Could not automatically rename PortalCfg.xml to PortalCfg.xml.loaded – to resolve the issue, rename the file manually, and verify that there is no file named “PortalCfg.xml” in the web folder. Restart the web application.
- Configuration already loaded for Portal Name – this occurs in a configuration where two or more instances are sharing tabs and modules and have the same **Portal Name** value. The first time any one of the shared instances is accessed, it will load that instance’s copy of PortalCfg.xml into the database and rename it to PortalCfg.xml.loaded. Before accessing any additional shared instance (instance with the same Portal Name), it is necessary to manually rename that instance’s PortalCfg.xml file to PortalCfg.xml.loaded. After doing this, restart the web application.
- Configuration already loaded for Portal Name – this can also occur if the goal is to configure two instances with different tabs and modules, and for some reason the **Portal Name** was not set to a unique value for each instance. To correct this, use Configurator to set the Portal Name to a unique value for each instance with different tabs and modules. After clicking **Save**, the web application will automatically be restarted.
- Migrating tabs and modules defined in a test instance to a production instance.

External Logoff URL: Enter an external URL into this field when you want the user to be redirected to another page after a timeout or when they log off.

Enterprise Integration Options

Encryption Key - Used when integrating external enterprise products into web modules.

Advanced Troubleshooting options

Session timer – Not recommended to enable for production environment.

ASPX debugging – Do not enable for production environment.

Advanced database options

Database Connection Pooling Options – Only change the pooling and data access settings if you know what you are doing.

Encryption

Deployment Encryption Key - Enter a secure messaging encryption key to enable encryption between the application and clients that connect to it. Restart any core application instances after applying this setting.

Generate Key – Click this button if you would prefer the system to generate a key for you.

Enable secure messaging encryption - This is only advised if you need the extra layer of security, and your web application server is physically a separate machine from where your core application.

LDAP Tab

This tab controls how the system communicates with a configured LDAP server including connection details and credentials, authentication settings and user data import settings.

Operating System: **Windows 10.0 (64-bit)**
IIS Version: **10.0** Web service status: **Running**

Web | Authentication | Database | MAXQueue | Reporting | Options | Logging | Asset Index | Data Services | Advanced | **LDAP** | Config Files

Authentication Settings

Authentication mode: **All Users** (dropdown)
Mapped groups only: ☒

External Server

Host:
Port:
User:
Password:
Filter:
Recursive: ☒
Use SSL: ☐
Test Connection Test Filter

User Synchronization

Settings

Enable user data import: ☒
Import data on login: ☒
Create user record on login: ☒
UserID to create / import user data:

Field Mapping

User ID:
Name:
Phone:
Email:
User groups:
Leave mapping blank for fields to ignore when importing data.

Authentication Settings

A drop-down list allows you to select the authentication mode for LDAP configuration. The following values can be selected:

- **All Users** – Every login to the system must be authenticated through the LDAP directory. This only applies to Web Modules and Data Services (mobile).
- **Mixed** – Only users who have the “Requires External Authentication” flag set on their user record will be required to authenticate through the LDAP server. Otherwise, the native system authentication will be used.
- **Mapped groups only** – In order to authenticate users against the configured LDAP server, they will need to belong to at least one user group in the system that has the LDAP server. Otherwise, native system authentication will be used.

External Server

This section controls how the system will connect to the LDAP server. It includes the following fields:

- **Host** - IP address or server name of directory to connect to.
- **Port** - The port to be used when connecting to the directory service.

- **User** - The "view-only" user to be used to pull user information from the directory service.
- **Password** - The "view-only" password to be used to pull user information from the directory service.
- **Filter** - The LDAP filter used to filter the directory service down to users and groups in the system.
- **Recursive** - Indicates that sub-folders in the directory service should be pulled as well, or if only the filtered folder should be pulled.
- **Use SSL** - Indicates if the LDAP connection should use certificates for secure communication. This is turned off by default, because it requires additional environment configuration.
- **Test Connection** - Attempts to connect to the configured LDAP directory using the server, port, user and password provided. Displays a message to the user indicating success or failure.
- **Test Filter** - Attempts to connect to the configured LDAP directory and runs a query using the provided filter. Displays a message to the user indicating success or failure and the number of user records found in the filter.

User Synchronization

The settings in this section support importing user data from a configured LDAP server. For this functionality to work, the External Server section must also be completed to allow for connection to the LDAP server.

Settings

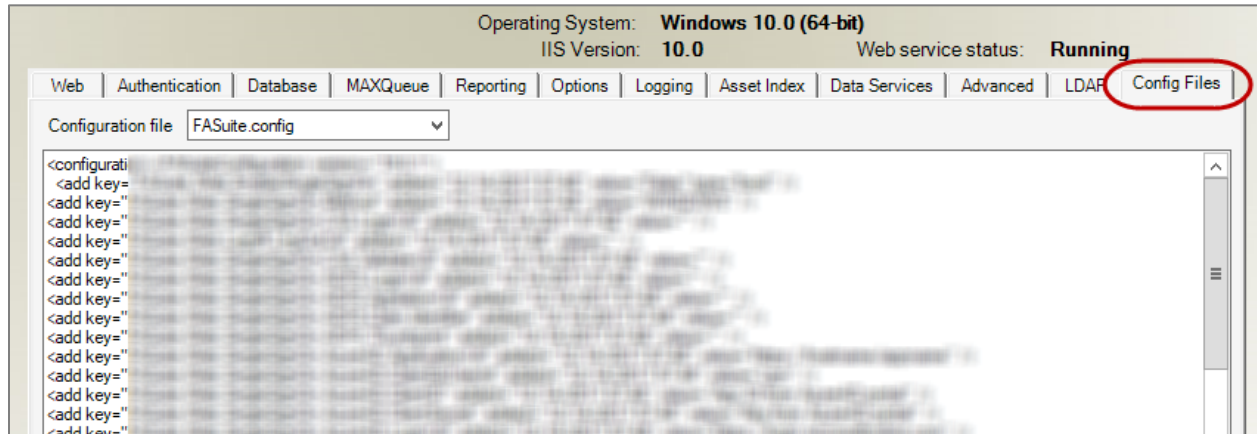
- **Enable user data import** - Enables the ability to import user data from the LDAP server. When this is disabled, users will not import data on login and the UI in the User Management admin page in web modules will be hidden.
- **Import data on login** - Controls if user data should be imported into the system when the user logs into the system.
- **Create user record on login** - Controls if the system user record should be created if it does not already exist when the user logs in.

Field Mapping

These settings control how user attributes from the connected directory are mapped to the system user fields. If the field is left blank, that data will not be imported from the LDAP server.

Config Files Tab

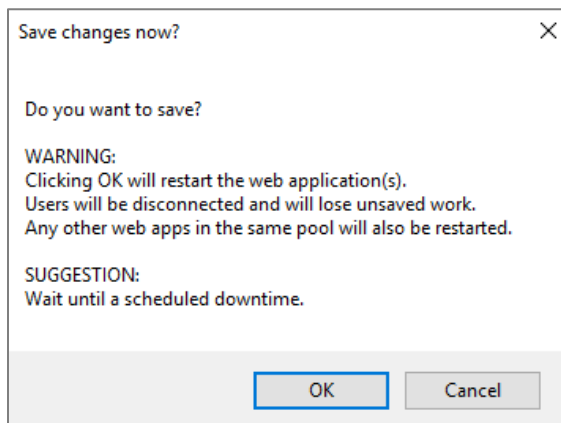
This tab contains a drop-down list that allows you to select which file to review. While the raw SAVED XML files are displayed, all editing of the files should be done through the other tabs of this Configurator tool.



Finalizing Configuration

To save all updates performed:

1. From any tab, click **Save and Restart Web Application** when you are finished using the Configurator. A warning dialog may display to warn that if you save, you will log off all connected users.



2. Click **OK**.
3. Click **OK** on the Settings Successfully Saved dialog.
4. Click **EXIT** to exit Configurator.

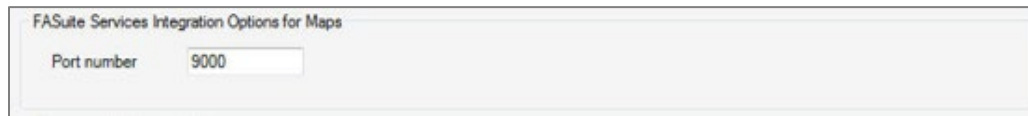


If you are performing an installation or upgrade, exiting the Configurator will resume the install or upgrade process.

- ✔ You can launch the Configurator at any time from the **web/bin** folder in your installed Target directory which can be accessed by clicking the folder name in the main Installer window.

Advanced Tab

The FASuite Services Integration Options for Maps section allows you to change the default port number used by the mapping service. The default setting for this option is 9000 which can be changed.



The screenshot shows a configuration window titled "FASuite Services Integration Options for Maps". Inside the window, there is a label "Port number" followed by a text input field containing the value "9000".

5. Install Data Services

Data Services is an integration service that is required as part of the core installation. It supports MobileFocus devices and provides access to geocoding, geodata, and tiles for mapping functionality throughout the system along with any API processes.

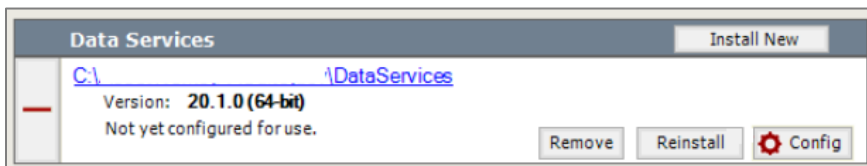
Prior to installing Data Services, ensure the following requirements have been met:

- Requires 64-bit Windows
- Must be installed in the same deployment as the Web Modules.
- Must be installed on the same machine as the Web Modules.
- Only one instance of the API service should be installed per deployment.

 If Data Services is running as server or console, it must be shut down prior to upgrading.

From the Installer, do the following:

1. Choose a deployment from the **Your Deployments** drop-down list.
2. Click **Install New** in the Data Services section.



3. The configuration file for the Data Services is located at deployment/DataServices/EAM.services.exe.config
 - i. The folder and file are created by the Web Modules Configurator when the Save button is clicked.
 - ii. If you do not see it in the specified location, contact Customer Support to verify the version being installed.
4. Edit the service properties to startup automatically and set auto-recover options to restart at first, second, and subsequent failures. Set restart service after two minutes.
5. Start the service that was installed.
 - i. In the case where there are multiple services on the machine, you can identify the desired service by the folder name in the service description.
 - ii. If the service was already installed and running, the installer will attempt to stop it, upgrade it, and restart it. Verify that this worked.

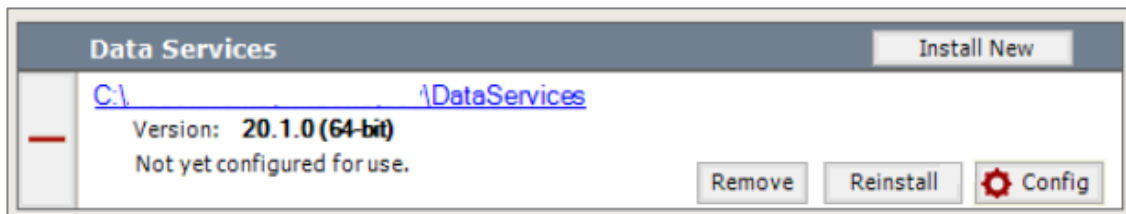


6. Launch Configurator via **Config** button after installing the API service.
7. Configure the Web Modules using the Configurator.
8. After configuring the API service, click **Save** in the Configurator and then restart the API service.

Data Services and API Service Configurator

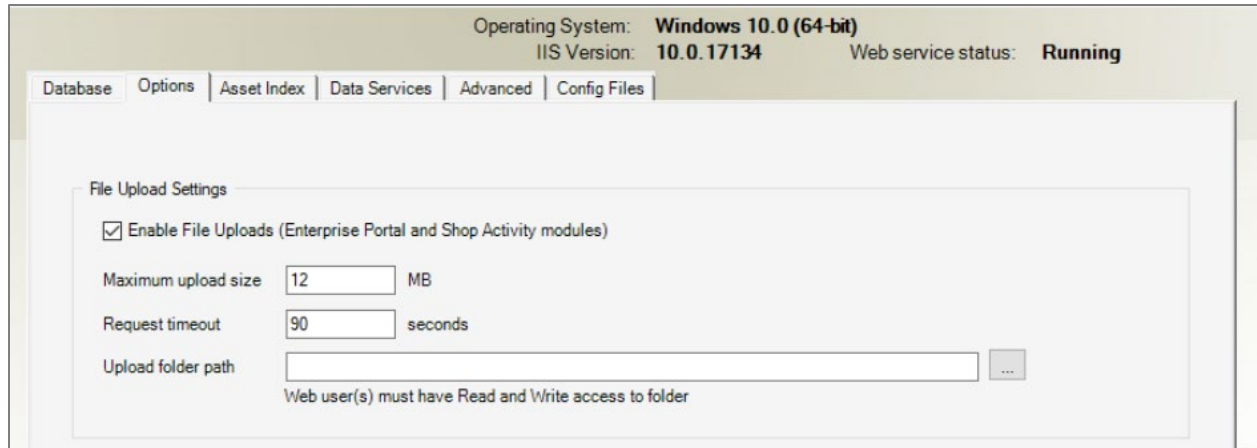
When you install the API service, you must configure it separately from the main Web Modules configurator.

The Data Services Configurator will launch after clicking the Config button when installing the API service. To access it when not doing an install or upgrade, launch the Configurator.exe from the DataServices folder of the deployment.



The Data Services Configurator has the following tabs. Please click the link for each tab to go to the full description of the tab:

- [Database](#)
- [Options](#) (File Upload Settings only)
- [Asset Index](#)
- [Data Services](#)
- [Advanced](#)
- [Config Files](#)



After configuring the API service, click **Save** and restart the API service.

Important Information:

- Only one instance of the API service should be installed per deployment.
- If any configuration changes have been made to Web Modules such as database connection, application server connection, API host or port, or for any settings that are shared between the API and Web Modules, then you must also make the same changes to the API service.
 - Go to the folder where the API Service runs and launch Configurator.exe to make the changes.

Port Exclusions

It is recommended to perform port exclusions for the specific ports to be used by EAM.

Components to consider for port exclusion:

- Core Application port (for each instance)
- Data Services Identity Service port
- Data Services Primary Service port
- MAXQueue port
- Reporting Application Server port

To manually configure port exclusions:

1. Run Powershell as an admin for machine.
2. Confirm what software is running on what port using the following command:
 - `netstat -ab`

3. Confirm the tcp dynamic port range for machine using the following command:
 - `netsh int ipv4 show dynamicport tcp`
4. Ensure product or their related windows service is turned off on machine for the port exclusions you will add.
5. Execute the following command replacing <theport> with each port you wish to exclude:
 - `netsh int ipv4 add excludedportrange protocol=tcp startport=<theport> numberofports=1 store=persistent`
6. Confirm exclusions using the following command:
 - `netsh int ipv4 show excludedportrange protocol=tcp`
7. Confirm that the local address 0.0.0.0 is added to the iplisten list on machine using the following command:
 - `netsh http show iplisten`

If it is not in list, then add using the following command:

 - `netsh http add iplisten 0.0.0.0`
8. Turn products back on and confirm they are functioning as intended.

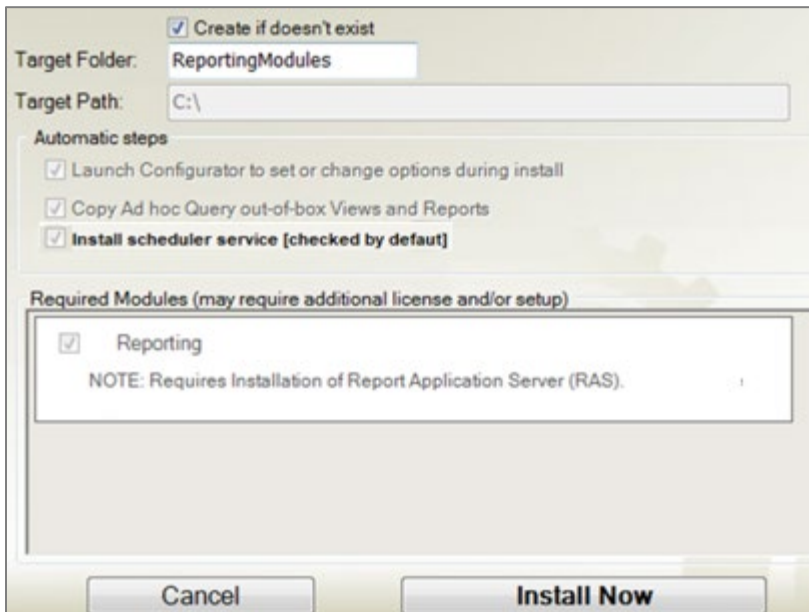
6. Install Reporting

From the Installer, do the following:

1. Choose a deployment from the **Your Deployments** drop-down list.
2. Click **Install New** in the Reporting section.



3. Verify the settings.



4. Click Install Now.

Reporting Server Installation

From the reporting file directory, do the following:

1. Right-click ~\[Crystal RAS Directory]\DATA_UNITS\RAS\setup.exe and select **Run as administrator**. If prompted with a User Account Control window, select **Yes**.
2. Confirm your desired language and press **OK**. Click **Next**.
3. Click **Next** on the Check Prerequisites screen after adding any missing prerequisites.
4. Select the option to accept the license agreement. Click **Next**.
5. Enter the product key. Click **Next**.

6. Select any desired additional language packages. Click **Next**.
7. Click **Next** without changes to install the default features.
8. Click **Next** again to start the installation.
9. When prompted, select **Finish**.

Reporting Server Configuration

1. Locate and run **Central Configuration Manager** found in Start > All Programs > SAP Business Intelligence > SAP Crystal Reports Server 2016, OEM Edition > Central Configuration Manager.
2. Stop the service SAP Crystal Reports Server 2016, OEM Edition.
3. Right-click the service and select **Properties**.
4. Select the **Parameters** tab:
 - i. Update the radio selection under Max Number of Records to **Unlimited**
 - ii. Toggle Option Type to **Server**.
5. Optional: Change the Maximum Simultaneous Report Jobs option to **Unlimited Jobs**.
6. Change the Report Directory value to Drive>:<DeploymentName>\Reporting.or Reporting Share Name if configuring stand-alone server.
 The Reporting Share Name must exactly match the reporting path in the Configurator.
7. Under the Properties tab, the default **Log On As** user will be set as System Account. Optional: Uncheck System Account and set the **Log On As** user to a network administrator specified service account with correct permissions.
8. Restart the Report Application Server.
9. Configure the Reporting Application Server using the Configurator.

7. Install MAXQueue and Integration Designer

MAXQueue is a middleware integration tool providing real time and scheduled interfacing opportunities with numerous vendors. MAXQueue utilizes staging tables, messaging, email, and many other technologies to transmit and receive data between systems. Certain requirements must be configured before MAXQueue can be installed into your environment.



Please refer to the *MAXQueue Administrator Guide* for requirements, installation, and configuration details.

8. Configure Post-Installation

Configuring Permissions

The following permissions must be assigned to allow users to have proper access to the Web Modules.

1. The IUSR account and IIS_IUSRS group needs read access to the following directory with the same permissions applied to all its child folders:
 - <INSTALL_DIRECTORY>\web
2. The IIS_IUSRS group also needs write and modify access to the following directories and folders:
 - <DeploymentName>\WebModules\Temp
 - Temporary files folder – Always required.
 - <DEPLOYMENT_FOLDER>\Logs – Always required. Logs are located one level above the <INSTALL_DIRECTORY>
 - <INSTALL_DIRECTORY>\Web\Search – Required if using Lucene.
 - <INSTALL_DIRECTORY>\Web\Dashboard\Images – Required if using Dashboard module and/or PMM module.
 - <UPLOAD_DIRECTORY> – Required if using File uploads. File UPLOAD_DIRECTORY is specified on the Options tab of Configurator.
 - <REPORT_DIRECTORY> – Required if using Ad Hoc Query and/or Crystal Reports (Reporting/Scheduling). The REPORTING_DIRECTORY is defined in the Reporting tab of Configurator.
 - <INSTALL_DIRECTORY>\WebModules\DataFiles



This folder is only needed if you have an ICU integrated with FuelFocus. You may need to manually create this folder if it does not currently exist.

Create Admin User via GUI

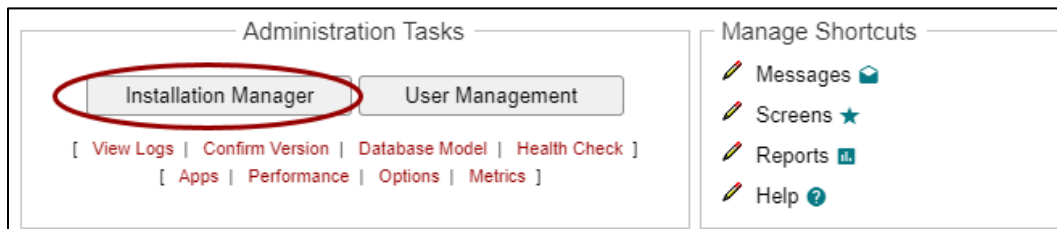
An admin user must be created via the GUI before logging into EAM to continue with the installation configuration.

1. Create a shortcut for the EAMGui.exe file.
2. Right click on the EAMGui.exe file and select the Properties button.

3. In the Shortcut tab, select the Target field and append the path there with the TCP/IP address or the computer name of the system application server and the port number you defined for the application in the following format:
 - i. <target path> <Address>:<Port>
 - ii. C:\Trapeze\EAM\Prod\AppServer\EAMGui localhost:1999
4. Log in to GUI with default credentials:
 - i. User ID: USERSETUP
 - ii. Password: usersetup
5. Create a new user with administrative rights.
6. Continue to web modules and login with the new admin user.

Enabling Access

1. Navigate to your Web Modules instance and log in with the new admin user.
2. Click the **Admin** shortcut button at the top left of the page. Select **Admin Center** from the drop-down list.
3. Click **Installation Manager** in the Administration Tasks box.



The Web Modules Installation and License Management page displays.

4. In the **Primary Product Key** field, enter the license key. Click the **Restore Defaults** button to populate the Quick Links and Welcome sections with the default links and message. Then click the **Update Modules** button to complete the installation process.

Installation and License Management

Primary Product Key

Customer ID:

Installed Modules

Licensed	Up-to-date	Module	Override Key	Expires	Conversion Number	Expected Conversion
☒	☒	Accounting Portal		Never	12	12
☒	☒	Allocation and Assignment		Never	0	0
☒	☒	Asset Configuration Management		Never	0	0
☒	☒	Asset Performance Assessment		Never	0	0
☒	☒	Billing		Never	0	0
☒	☒	Capital Planning		Never	0	0
☒	☒	Customer Access		Never	0	0
☒	☒	Enterprise Portal		Never	0	0
☒	☒	Equipment Planning		Never	1	1
☒	☒	Equipment Portal		Never	0	0
☒	☒	FluidFocus		Never	20	20
☒	☒	FuelFocus		Never	20	20

Back

Update Modules

Restore Defaults

A Successful update message displays.

- Click the **Back** button to return to the **Main Admin** tab.

Log out of the application, exit the browser, open a new browser, and log back in prior to accessing the specific modules for configuration.

9. Customize Web Modules

To perform configurations through the **Admin** tab, you must be logged in as a member of a user group that has system administrator rights.

Admin Center

Initial configuration can be done through the Admin Center in the application. Click the **Admin** shortcut at the top left of a Web Modules page and select **Admin Center**.

The screenshot displays the Admin Center interface. At the top, there is a navigation bar with icons for Messages, Screens, Reports, and Admin. Below this is a secondary navigation bar with tabs: Home, Work Management, Technician, Asset Configuration Management, and Supervisor. A 'Quick Links +' button and a 'Component Library' link are also visible. The main content area is divided into two primary sections: 'Administration Tasks' and 'Manage Tabs'.

Administration Tasks includes buttons for 'Installation Manager' and 'User Management'. Below these are links for 'View Logs', 'Confirm Version', 'Database Model', 'Health Check', 'Apps', 'Performance', 'Options', and 'Metrics'.

Manage Tabs features an 'Add New Tab' button and an 'Export Tabs' button. It contains two lists: 'Tabs' (Home 2.0, Work Management, Technician, Supervisor, Asset Configuration Management, Service Request, Network Restrictions, Storekeeper, Storeroom, Reporting) and 'User Groups' (AX-LOC RIGHTS, AX-LOC2 RIGHTS, LM-SYSADMIN, LOADER, NOTADMIN, SYSADMIN, TEST, TEST1234, USERSETUP). A 'Default Tab' dropdown menu is located at the bottom right of the Manage Tabs section, with an 'Apply' button next to it.

Administration Tasks

The Administration Tasks area of this page includes buttons to access the Installation Manager and User Management pages as well as links to View Logs, Confirm Version, Database Model, Health Check, ActiveX, and Metrics.

Installation Manager

Clicking the Installation Manager allows you to enter Installation and License Management information as well as view and update installed modules.

Installation and License Management

Primary Product Key

Customer ID: QA

Installed Modules

Licensed	Up-to-date	Module	Override Key	Expires	Conversion Number	Expected Conversion
☒	☒	Accounting Portal		Never	12	12
☒	☒	Allocation and Assignment		Never	0	0
☒	☒	Asset Configuration Management		Never	0	0
☒	☒	Asset Performance Assessment		Never	0	0
☒	☒	Billing		Never	0	0
☒	☒	Capital Planning		Never	0	0
☒	☒	Customer Access		Never	0	0
☒	☒	Enterprise Portal		Never	0	0
☒	☒	Equipment Planning		Never	1	1
☒	☒	Equipment Portal		Never	0	0
☒	☒	FluidFocus		Never	20	20

User Management

Clicking the User Management button takes you to the User Management page which provides system administrators an overview of the users in their system and allows them to perform certain functions. Metrics relating to users, user logging, user authentication and user data import are displayed on the page.

User Management

Total Active Users 37

Total Logins Today 8

Total Users logging 0

Total Mobile Users 34

Users with no employee 5

Authentication Mode Native

Data Import Enabled N

Log All Users Y

Log Anonymous Activity N

Stop Logging All Users

Log Anonymous Activity

Users

Search...

	User ID	Name	Phone Number	Email Address	Session Location
☐	AX-LOC1	AX-LOC1			AX-LOC1 - AX-LOC1 LOCATION RIGHTS ACCESS
☐	AX-LOC2	AX-LOC2			AX-LOC2 - AX-LOC2 LOCATION RIGHTS ACCESS

Showing 37 records

Current Filter

Is Active: YES

Define Filter

Clear Filter

You can also do the following from User Management:

- Turn logging on/off for all users.
- Turn logging on/off for anonymous activity.
- Turn logging on/off for one or more users at the same time.
- Import users from a connected LDAP server (ability to create and update user data is supported).
- View users in the system.
- Filter users via a search box.
- Interact with data in the user table, such as clicking a UserID to open the EP screen or click an email address to send an email to a user.

User Logging

Web Modules checks whether it is in logging mode every 20 seconds. Therefore, once logging is enabled for a user, you should wait 20 seconds before proceeding with testing.



If there are multiple instances of Web Modules running, the flag for whether the call log is turned on is stored in the database. Therefore, all Web Modules instances will log the information.

- Click the **Log all users** button to log all users.
- Click the **Log anonymous activity** button to log activities when no user is logged in. (An anonymous user can use certain modules without logging into Web Modules.)

Once logging is started, a file is generated in the following log:

- Logs\<yyyymm>\<yyyymmdd>\WebModules\<Instance>\ directory called **sqlcalls_<username>.log**
 - **<yyyymm>**: Year and month of the logs
 - **<yyyymmdd>**: Year, month, and day of the logs
 - **<Instance>**: Specific web instance the logs were generated from

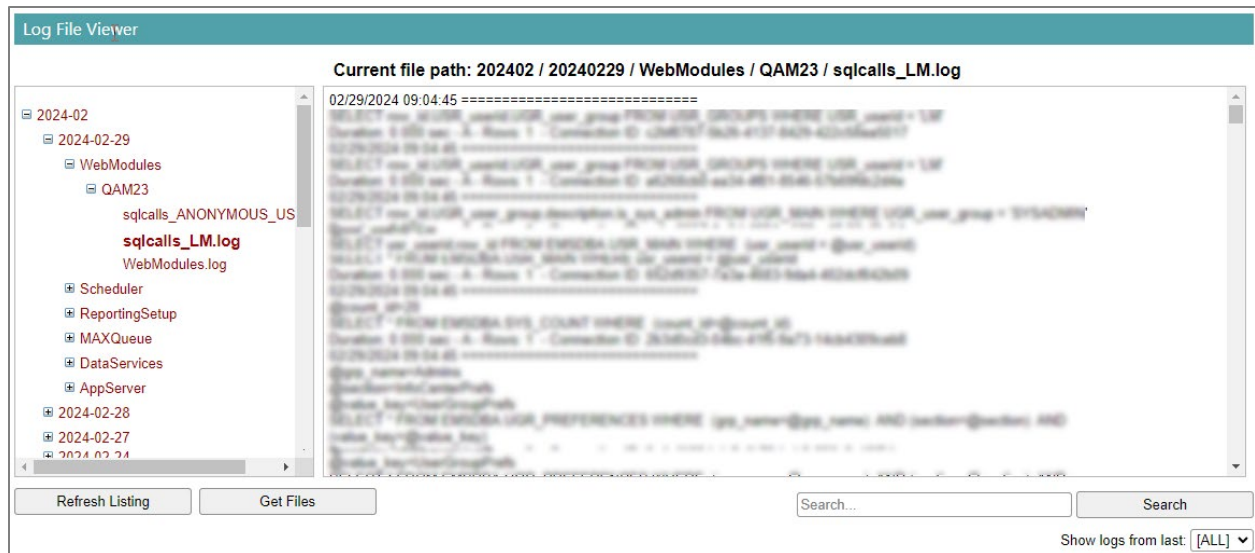
View Logs

Logging functionality is available through the **Admin Center**. There are two ways to view the log files:

- Click the **View Logs** link on the Admin page

- Click the **Admin** shortcut and select **View Logs**:

In the Log File Viewer page that opens, select a log by clicking the (+) in the menu on the left to drill down to the desired log. Click on the desired log to display it in the viewing pane.



The log files are physically stored in the Logs directory that is at the same level as the main Web Modules directory. To view the log file, follow the default path: **<Install Path>\Logs**. **Where Install Path is the folder you chose during the upgrade/install.**



Clicking the blue hyperlink from the Installer instance will open the Install Path folder for easy access to the Logs. This includes Application, Web, Reporting, MAXQueue and other logs created by the system.

- Refresh Listing:** Updates the logs to update any changes since the page was launched or opened, or since the last refresh.
- Get Files:** This option allows you to select a log or set of logs that can be downloaded and zipped together in a file folder. When selected, choose what directories you wish to download by checking the appropriate checkbox and then click the Download button.
- After selecting a log file to view, use the **Search** field in the bottom-right part of the screen to highlight specific entries in the log file.

Confirm Version

Confirm Version provides contents and details of the bin directory.

Contents and details of the bin directory				Version 23.0.0
Title	Version	Description	Time Stamp	File Size (Bytes)
Ajax.NET Professional for Microsoft.NET 2.0	23.5.10.1	.NET Library that provides AJAX related methods to simplify the communication between server and client.	02/29/2024 08:56	151,552
AllocationAssignment	23.0.0.16214	Facilitates allocation and assignment of equipment and resources.	02/29/2024 09:00	235,520
AMBBusinessFacades	23.0.0.16094		02/29/2024 08:56	2,651,648
AMBBusinessObjects	23.0.0.34259		02/29/2024 08:59	7,473,152
AntiXss Library for .NET 4.0	4.3.0.0	Encoding classes for safe-listing encoding of HTML, XML and other output types.	02/29/2024 08:59	62,608
Antlr3.Runtime	3.5.0.2		02/29/2024 08:56	103,424
ApplicationUtilization	1.0.0.0		02/29/2024 08:57	23,040
AssetConfigurationManagement	23.0.0.16219	Create, manage and analyze asset configurations	02/29/2024 09:00	62,976
AssetListByType	23.0.0.16125		02/29/2024 08:57	10,752
AssetPerformanceAssessment	23.0.0.16217	Assess Asset Conditions	02/29/2024 09:00	89,088

Database Model

Database Model allows you to view Database Table information through the **Admin Center**.

1. In the Administration Tasks area, click the **Database Model** link.

FASuite Database Tables	
Click on a table name to view its details and relationships	
Table name	Description
AA_MAIN	ALLOCATION & ASSIGNMENTS
AA_NOTES	ALLOCATION & ASSIGNMENTS NOTES
AAINV_AALIST	ALLOCATION & ASSIGNMENTS ASSET INVENTORY LIST
AAINV_CRITERIA	ALLOCATION & ASSIGNMENTS ASSET INVENTORY CRITERIA
AAINV_MAIN	ALLOCATION & ASSIGNMENTS ASSET INVENTORY
AAREQ_MAIN	ALLOCATION & ASSIGNMENT REQUESTS
AAREQ_NOTES	ALLOCATION & ASSIGNMENTS REQUESTS NOTES
AASTAT_MAIN	ALLOCATION & ASSIGNMENTS STATUS
ACATMAP_MAIN	ASSET CATEGORY MAPPING
ACATMAP_VALUES	ASSET CATEGORY MAPPING VALUES
ACAT_MAIN	ASSET CATEGORIES: PRIMARY INFORMATION
ACC_MAIN	ACCESS KEYS
ACCIDTYP_MAIN	ACCIDENT TYPE

2. Click a Table name to view the **Table details and relationships** dialog.

Table details and relationships

ACAT_MAIN

ASSET CATEGORIES: PRIMARY INFORMATION

Expand All Collapse All

Primary keys

Name	Data type	Size
ACAT_category_no	CHAR	30

Columns

Name	Data type	Size	Allow NULL?	Default Value
ACAT_category_no	CHAR	30	False	NONE (0)
ACAT_category_no_new	CHAR	30	True	NONE (0)
ACAT_invalidated	CHAR	1	True	CHARNO (103)
auto_numbering_eq	CHAR	20	True	NONE (0)
cmp_tree_update_off	CHAR	1	True	CHARNO (103)
DB_ACC	SMALLINT		True	NONE (0)
description	CHAR	60	True	NONE (0)
id_structure_eq	CHAR	40	True	NONE (0)

- Click on a row to toggle information about it.

Health Check

To assist in troubleshooting web configuration issues, a Health Check page is available. Administrators can go to the Health Check page by clicking the **Admin** shortcut and selecting **Health Check**.

In addition, any user may browse to the Web instance they wish to troubleshoot and type in the following URL:

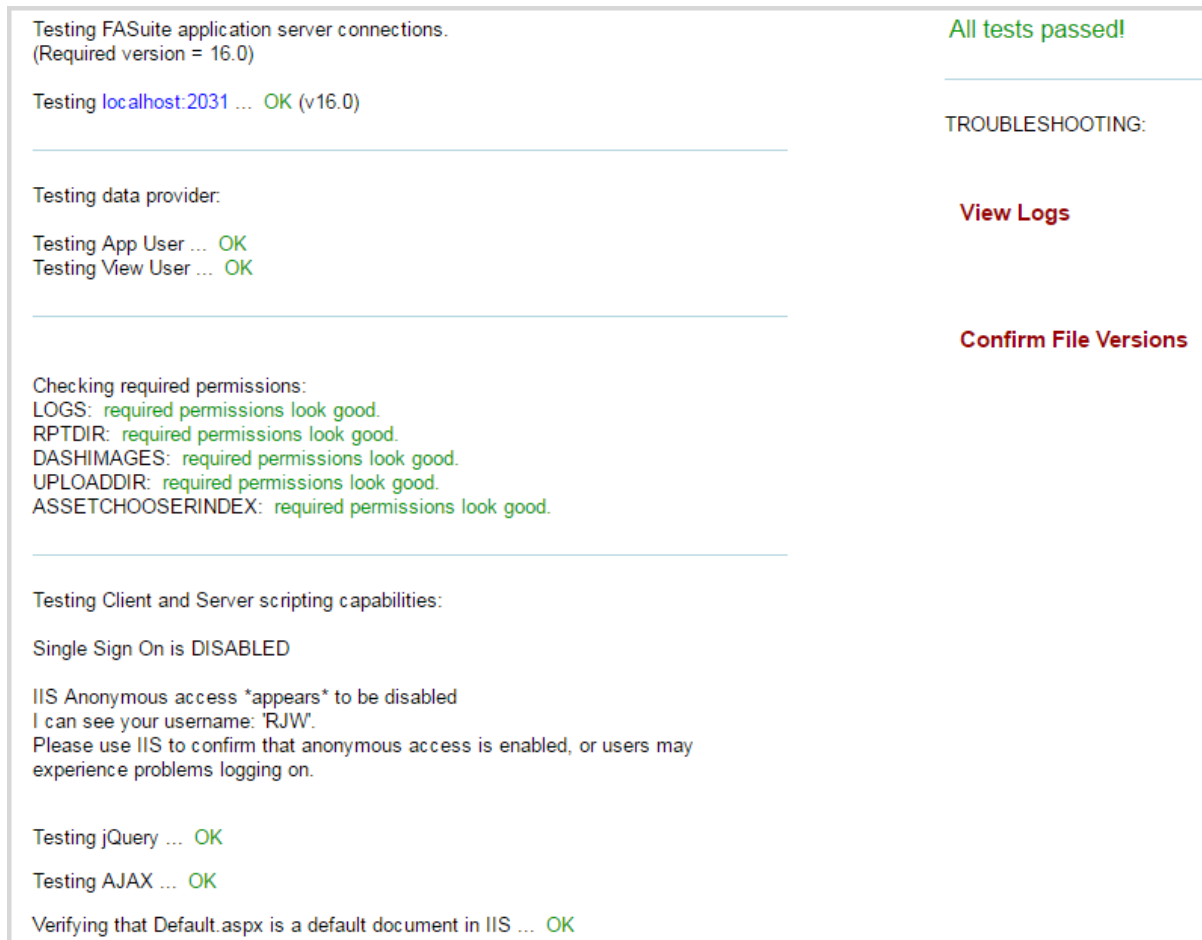
`http://<instance URL>/<instance Name>/utils/healthcheck.aspx`

Where **<instance URL>** is the main Web URL. This cannot be localhost. It must be either a server name or an IP address. The **<instance Name>** is the name of the web application to which you are pointing.



If upgrading from an older version, you may need to refresh MAXQueue permissions to properly run the health check. Ensure that the 'emsapp' user has proper permissions.

The following screenshot shows a sample Health Check page:



The Health Check page analyzes and displays information as follows:

Message and Links - In the upper right corner, a message and links display.

- A message summarizes the results of all tests. If all tests were successful, the text is GREEN and reads, “All tests passed!” If there are any failed tests, a message in RED indicates the issue that needs correction.
- Link to view the Web logs – Follow this link to view any error log files.
- Link to confirm file versions – Follow this link to view the version information for all web dll files.

App Connection Verification – Validates that the version number is correct to pair with Web. This test displays results for each application connection string defined in the configuration.

Data Provider Verification - Verifies direct DB connections as defined in the configuration.

- Database type is displayed (MSSQL or Oracle)

- Each user type is tested - dba, app, and view users

Required Permission Verification - Verifies required permissions for LOGS, DASHIMAGES, UPLOADDIR and ASSETCHOOSERINDEX.

Client and Server Scripting Capabilities Verification

- Must have access to the logging, web, and reporting directories with appropriate permissions
- Indicates if Single Sign-On is enabled or not
- Confirms the IIS Authentication method
- Tests jQuery
- Tests AJAX
- Verifies that default.aspx web page is defined as a default document in IIS.

If all of the above information passes the tests, then Web Modules should run successfully.

Health Check Troubleshooting

A simplified version of this health check is performed every time the web application starts. If a critical area fails, the application server will go into a “Server down” state, and users trying to access the website will see a **Server is unavailable** message. If this happens, check the **LogDir/InfoCenter.log** (Health Check section) for the reason that the web app was disabled.

Possible reasons web app can be disabled:

- Database connection failure
- Invalid permissions on required folders
- Incorrect ASP.NET / framework version
- Incorrect version for one or more Application servers

When the web app is disabled, it is usually still possible to access the web pages in the **tools/** and **utils/** folders (including log file viewer, health check, and **tools/faversion.aspx**). However, if there is a sever issue (like loss of database connectivity) this will not occur.

If the server is unavailable, and you do not see any entries in the LogDir folder, verify that the IIS user (or ASPNET user, depending on your configuration) has write permissions to the LogDir folder.

Apps

The Apps section allows you to install apps to work with EAM. The following are apps that are available to be installed.

Installers

Please note that Station Connect is only designed for Windows OS only.

[Station Connect App Install](#)

StationConnect

Click the **Station Connect App Install** link to download the StationConnect.Installer.exe.



Please refer to *Station Connect* documentation for specific details regarding installation and use of the Station Connect app.

Performance

Clicking Performance in the Administration Tasks section takes you to a page that allows you to set a refresh rate for each type of session, view statistics, and export this data.

Refresh every

ApplicationSession

DataAccess

FASession

ServerControls

Statistics

Total Samples	2
Current Samples	2

Export Current to CSV

Options

The Options page allows you to set certain portal-wide options.

Portal-wide Options	
Reporting Options	
Use Asset Chooser instead of Choice-list	☒
Show logged in User ID on report	☐
Require access rights for all ad hoc reports	☐ Ad Hoc Access Rights
User group allowed to create new Ad Hoc reports	[All users (default)] ▼
Web Modules UI Preferences	
Environment color	☒ Use system default coloring
Sets the background color of the application header. Used to identify non-production environments (e.x. stage, test).	

Reporting Options

Use Asset Chooser instead of Choice-list: Check this option to use the Asset Chooser when selecting assets when running reports.

Show logged in User ID on report: Check this option to display the logged in user at the footer of reports.

Require access rights for all ad hoc reports: Provides an additional layer of access rights. Administrators can specify what Users and User Groups may be allowed to view reports. This is beneficial when two types of users both have access to the same screen, but one of them should not be able to see the other's reports. For example, a supervisor may create a cross-team performance report that they do not want everyone with access to that screen to be able to view.

User group allowed to create new Ad Hoc reports: Allows you to specify which user groups are allowed to create new Ad Hoc reports.

Web Modules UI Preferences

Environment color: Configure the color of the tab bar. This option can be used when needing to identify non-production environments.

Log in page image: Select or upload and configure an image for the log in page. This image appears as a background on the log in page.

Log in page logo: Select or upload and configure a logo for the log in page. This logo appears at the top of the log in page.

Navigation panel logo: Select or upload and configure a logo for the navigation page. This logo appears on the navigation panel.

Application logo: Select or upload and configure a logo for the application. This logo appears at the top, left of the application.

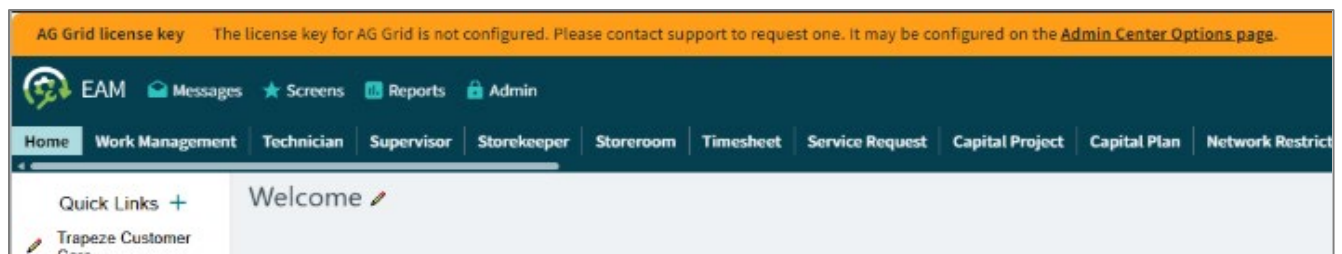
Center application logo (optional): Select or upload and configure a logo for the center of the application. This logo is optional and would appear at the top, center of the application if enabled.

Web Control Customizations

Clear user table customizations system-wide: Enable if you would like to clear table customizations that have been created by users.

Clear portal default table customizations system-wide: Enable if you would like to clear the default table customizations system-wide.

AG Grid table license key: Allows configuration of a table library license key which is part of the Service Request Center portal. The AG Grid license is required and a banner will appear at the top of the page if the AG Grid license key is missing. The banner message will only disappear once the AG Grid License Key field is completed.



Mobile Options

Allow saved login on device: Check this option to allow the user to open the mobile application and automatically be logged in. This option uses the last user that was logged into the application for auto-login.

Use External Identifier as Username: Check this option to enable users to log into the web application using their external ID (such as their email address).



Note: If Single Sign-on (SSO) is not configured at the server level through the configurator, this setting will not apply to MobileFocus. If SSO is enabled at the server level, users logging in will see an optional link on the mobile device to enter their external ID and use SSO.

Auto-logout timer (minutes): Define a time in minutes for when mobile will log out.

Map Options

Default map bounds: Pan and zoom the map to the desired view, and then click **Use this view** to set the center latitude, longitude, and zoom level.

You can also set the Default center point and bounds using the **Latitude** and **Longitude** fields, and the **Default zoom** level.

Enable GE CityIQ IoT Sensors Integration: Check this box to enable GE CityIQ IoT Sensors Integration. This option also allows you to set the **Authentication URL**, **Events URL**, **Media URL**, **Metadata URL**, **Username**, **Password**, and **Service Subscription** for the integration.

Metrics

Metrics allows you to view Web Usage Metrics including **Screen statistics**, **Browser statistics**, and **User statistics**.

1. In the Administration Tasks area, click the **Metrics** link.

Web Usage Activity			
Screen statistics (most used first)			
Rank	Screen ID	Screen Title	Hit count
1	7608	Login.aspx	3492
2	7229	WorkManagementPortal.aspx	2638
3	7466	FAScreenToolbar.aspx	2387
4	7099	ReportList.aspx	1322
5	7224	FAScreenHistoryPopIn.aspx	1288
6	7194	FAScreenChoiceListPopIn.aspx	1104
7	7185	WorkOrderPostings.aspx	867
8	7003	technicianportal.aspx	629
9	7143	ReportViewer.aspx	627
10	7010	workordermain.aspx	478
11	7158	InfoCenterAdmin.aspx	440
Show all			

2. Click **Show all** to show all results in the list.
3. Click a **Screen ID**, **Browser**, or **User ID** link to open additional screens and view more statistics about that selection.

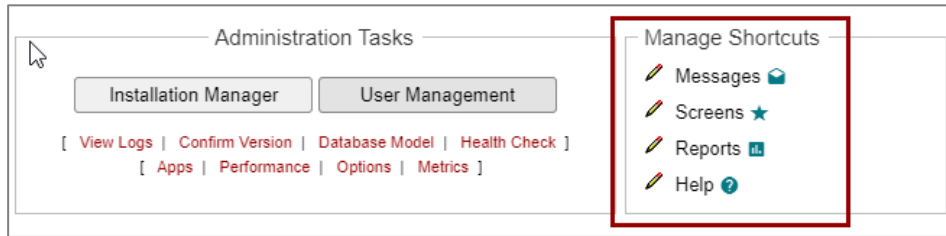
Manage Shortcuts

Web Modules offers shortcuts to the Enterprise Portal, Reports, Instant Messenger and Notifications. These shortcuts allow specified user groups to access Enterprise Portal, Reports, Instant Messenger and Notifications from anywhere in Web Modules. When the logged in user has access rights to a shortcut, it appears as an icon in the upper left corner of all Web Modules pages as shown in the screenshot below.

To configure the user groups that have Shortcut access:

1. Click the **Admin** button and select **Admin Center**.

- Click the edit pencil icon for the desired shortcut in the **Manage Shortcuts** area of the Main Administrator Page.



- Select the desired **User Groups** and click **Apply Changes**.

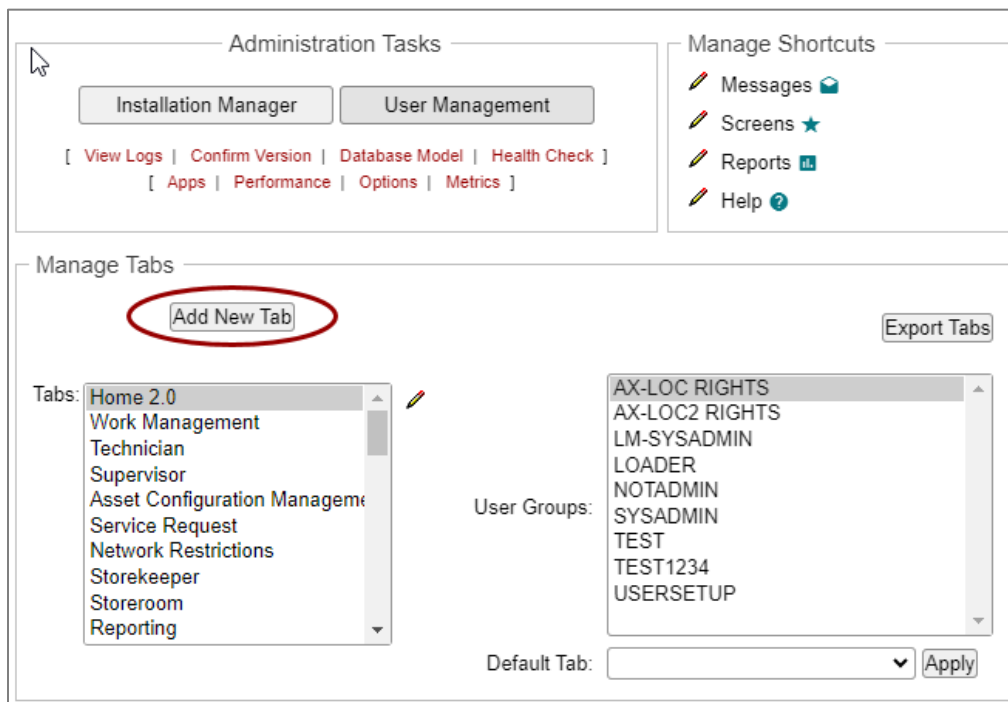
The shortcuts will display in the upper corners of the Web Modules pages.

Manage Tabs

Adding a Tab

Modules are added to a Web Modules instance via tabs. Once you have installed the Web Modules base and accompanying modules, basic configuration of the modules is determined based on your organization's requirements.

- In the **Manage Tabs** section, click the **Add New Tab** button.



The Tab Configuration and Access Rights page displays.

2. In the **Tab Name** field, enter the name you would like to designate for the tab.
3. Set the **Authorized Roles** to restrict who may access the **Work Mgmt** tab by checking the desired groups. These groups are based on your user groups, so set access accordingly.

 By checking the **All Users** option, Web Modules will not require a valid logon for an end user to access the tab. Certain web modules may be configured to support such anonymous access to their functions.

4. Check the **Show to mobile users?** option if you would like the tab to be available to mobile users. In the **Mobile Tab Name** field, enter the tab name you would like displayed for mobile users.
5. In the Add Module section, enter the following:
 - **Module Type:** Select the module you wish to associate the tab with from the dropdown choice list.
 - **Module Name:** Enter the module name you wish to display on the page for this section of the Web page.
6. Click Add to Organize Modules Below.

*The module name displays under **Content Pane** in the **Organize Modules** section as shown in the screenshot below.*

You may choose to move the module to the left or right panes for formatting needs, and more than one module may be stacked on top of each other in each pane. The Dashboards Module is an example of a module that may be stacked on another module to provide an immediate snapshot of key performance indicators within that module. Most modules, however, are designed to exist on tabs alone.

 Some modules, such as Service Request, will cause unexpected results due to features within each page when using a shared tab between two (or more) modules. If using multiple modules on one tab, test all workflow functionality before configuring for general use.

8. Click **Save** to save the changes and add the tab.

Deleting a Tab

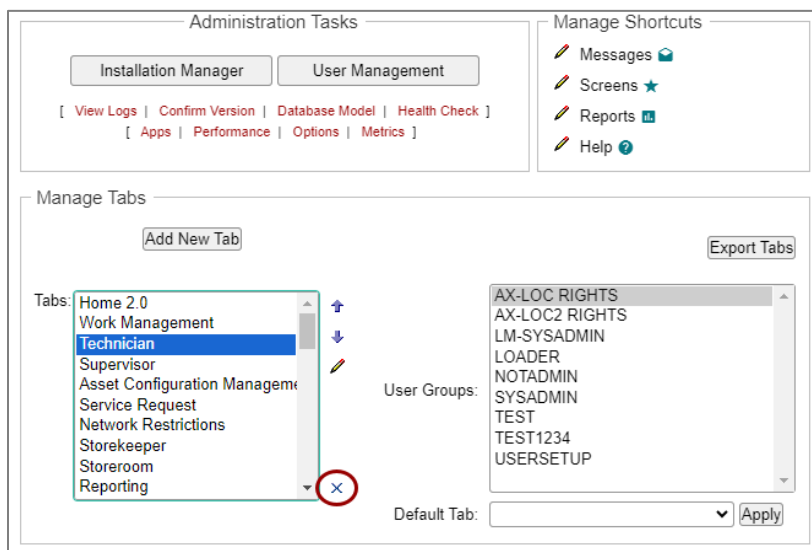
To delete a tab from Web Modules, log in to Web Modules. Click the **Admin** button and then select the **Admin Center** link.

You are taken to the page where tabs, user groups and module definitions may be modified. In the Manage Tabs section, highlight the tab name you would like to delete and click on the **X** to the right.

Deleting a Module from a Tab

In some instances, you may have more than one module installed within a tab (for example Dashboards Module stacked with the Supervisor Portal). To delete the stacked module, follow the steps below.

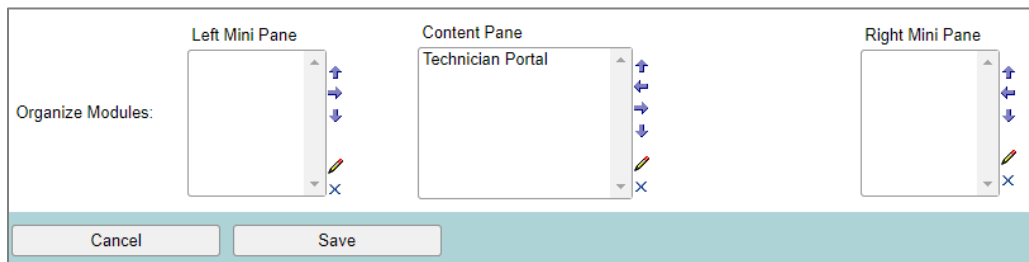
1. Click the **Admin** button and then click the **Admin Center** link.
2. Select the tab that needs to be modified and click the **Delete** icon.



Granting Edit Rights for Tabs

To give module editing rights to other user roles:

1. In the Admin Center, select the tab you want to edit, and click the edit pencil.
2. In the Organize Modules section at the bottom of the page, click the module name in the **Content Pane** to select it.



3. Click the **Edit** icon to the right.

The Module Settings page displays.

 A screenshot of the 'Module Settings' page. The title is 'Module Settings'. Below it, there are several fields and checkboxes:

- Module Name:** A text field containing 'Technician Portal'.
- Cache Timeout (seconds):** A text field containing '0'.
- Roles that can edit content:** A section with two columns of checkboxes:
 - Left column: ☐ All Users, ☐ LM-SYSADMIN, ☐ LOADER.
 - Right column: ☐ NOTADMIN, ☐ TEST1234, ☐ USERSETUP.
- Show to mobile users?:** ☐
- Show to module title?:** ☒

 At the bottom of the form, there are two buttons: 'Cancel' and 'Save'.

4. To restrict who may edit settings and content in the new module, check the appropriate user groups checkboxes in the **Roles that can edit content** area. If the module has an associated edit page, the roles checked in this area will have access to edit the module.
5. To save the changes, click **Save**, or to leave without saving changes, click **Cancel**.
6. You are taken back to the Tab Configuration and Access Rights Page. Scroll to the bottom of this page and click **Save** to save changes to the tab and its modules to Web Modules.

You are returned to the Admin Center and the new tab will display along the top of the application and under the Manage tabs section.

Setting a Default Tab

Use the Administration Tasks page to set a default tab for a user group to see when they first open the Web Modules.

To set a default tab:

1. In the Admin Center, select the user group that needs a default tab in the User Groups pane.
2. In the **Default Tab** drop-down below, choose the new default tab.
3. Click **Apply**.

Passwords and PIN Numbers

The following are the minimal password complexity requirements which are automatically set for new installs:

- Password may not be the same as User ID
- Minimum of 8 characters
- Combination of letters and numbers required
- One special character required
- User passwords must be changed every 60 days
- Minimum number of days between password changes is one
- Number of password changes required before reuse 6

If upgrading, an optional script can be run to enforce these minimal password complexity requirements.

The system will notify the user that their password is expiring beginning 14 days before it expires (default). The number of days can be configured by going to the Security – Setup – Options screen, Passwords tab in the Enterprise Portal.

Forgot Password?

If Enable Reset Password was set in the Configurator, a **Forgot Password?** link displays under the **Login** button.

For this process to work, the following items must be true:

- A valid matching user ID in the USR_MAIN table. This matching user ID cannot be disabled, but an expired password is allowed to user this reset process.
- The matching user ID record in the USR_MAIN table must have a valid email entered. Emails from the Operator table are not able to use this reset process.
- MAXQueue Notification Module must be configured correctly and enabled, along with the AWMMessageInsert Data Event.

To reset your password:

1. On the home page, click **Forgot Password?**.

The Reset Password pop-in displays.

2. Enter your User ID and click **Reset Password**.

If an email address exists for your User ID, a unique password is generated and an email is sent.

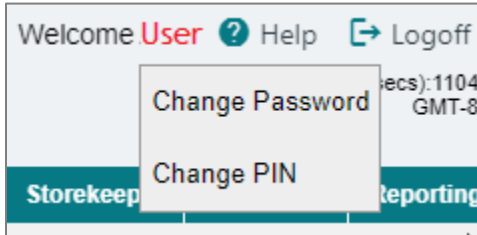
3. Enter your user ID and the temporary password supplied in the email to log in. On the next log in, you will be prompted to change your password.

Change Password

Use the following procedure to change your password through the Web Modules.

To change your password:

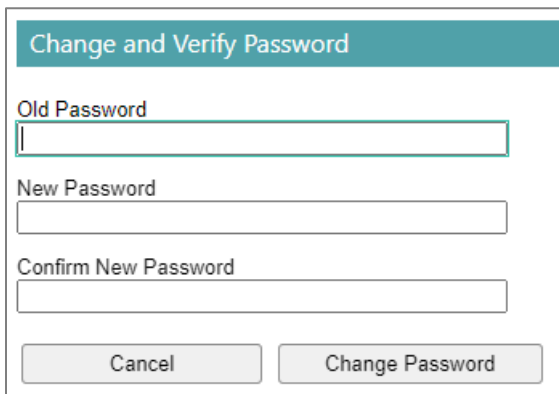
1. In the top-right corner of the Web Modules, click your ID where it displays **Welcome** [ID].



The password options display.

2. Click **Change Password**.

The Change and Verify Password pop-in displays.



3. Enter your current password (in the **Old Password** field), and the new password in the **New Password** and **Confirm New Password** fields.
4. Click **Change Password** to save or **Cancel** to cancel out and leave the password the same as it is.

Change the PIN Number

Use the following procedure to change your PIN number through the Web Modules.

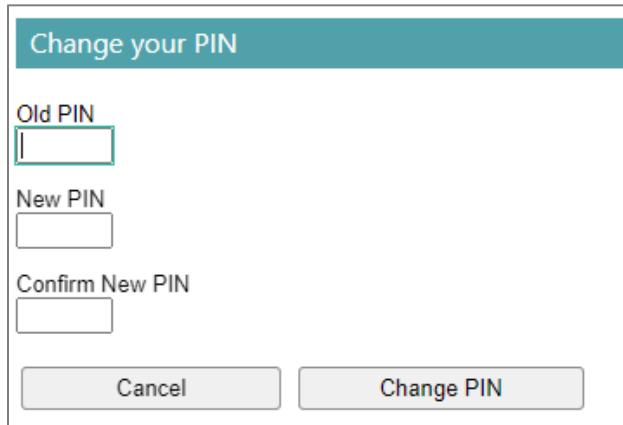
To change your PIN:

1. In the top-right corner of the Web Modules, click your ID where it displays **Welcome** [ID].

The password and PIN options display.

2. Click **Change PIN**.

The Change your PIN pop-in displays.

A screenshot of a 'Change your PIN' pop-in form. The form has a teal header with the title 'Change your PIN'. Below the header, there are three input fields: 'Old PIN', 'New PIN', and 'Confirm New PIN'. Each field is a simple rectangular box. At the bottom of the form, there are two buttons: 'Cancel' on the left and 'Change PIN' on the right. The 'Change PIN' button is highlighted with a teal border.

3. Enter your current PIN (in the **Old PIN** field), and the new password in the **New PIN** and **Confirm New PIN** fields.
4. Click **Change PIN** to save or **Cancel** to cancel out and leave the PIN the same as it is.

Customizing Home Tab

Editing Modules and Layout of Home Tab

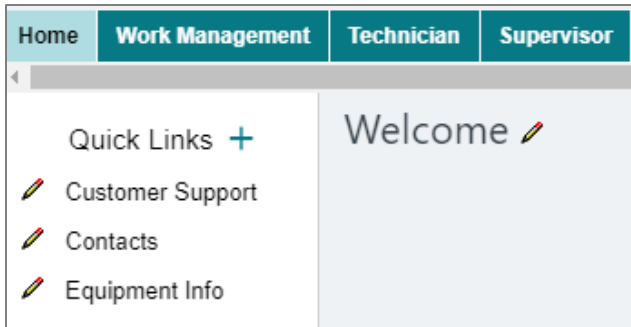
To modify the layout of the Home Tab or add a module such as the Announcements or Events modules, go to the Admin Center.

1. From the **Manage Tabs** section of the **Admin Center**, select the Home tab from the Tab list.
2. Click the **Pencil Icon** next to the Tabs list.
3. Scroll down to the **Add Module** section. Select the module you would like to add and click **Add to “Organize Modules” Below**.
4. Configure the appearance of the module in the **Organize Modules** section.
5. Click **Save**.

Quick Links Module

To add a link:

1. Click the **Plus** icon next to the Quick Links title.



The Link Details page displays.

- Complete the fields for the type of link you want to add. The types available are URL, Screen, and Crystal Report.

Link Detail

- **Title:** Enter the title of the link to display.
- **Description:** Enter a description if desired.
- **View Order:** Enter a numerical value to indicate the order you would like the link to appear in the Quick Links list.
- **Created by** and **Created on:** When creating a link, the system records the creation information.

Link Target

- URL

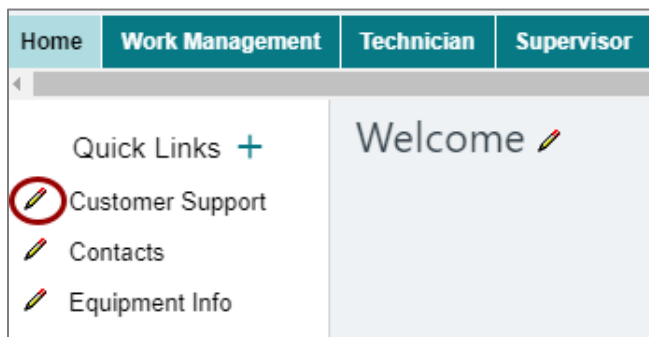
- **URL:** Enter the URL in this field. This field is hidden if the **EP URL** checkbox is checked.
 - **Open in new window:** Check this box if you would like a new browser to open when the link is clicked.
 - Screen
 - **Screen ID:** Enter the screen ID number for the screen. This field is hidden unless **EP URL** is checked.
 - **Filter Pairs:** Enter the basic filter information for the screen. This filters the screen automatically when it loads, rather than having to enter filter information when the screen opens. This field is hidden unless EP URL is checked.
-  **Note:** Note filter value pairs must be in the following format:
(window:control = value) separated by a “^”.
- For example, the following filter information filters on the window 188:2, and 188:3, and filters for the control information of RALOC2, the year 2013. 188:2=RALOC2^188:3=2013
- Crystal Report
 - **Report Name:** Select the report from the drop-down menu.

3. Click **Save**.

The Home Page displays your newly added Quick Link.

To modify or delete an existing link:

1. Click the **Edit Pencil** icon next to the link on the Home page.



The Link Details Page displays where you may edit information accordingly.

Link Detail

Title

Customer Support

Description

View Order

0

Created By

Created On

01/17/2024 09:49

Link Target

Type

URL

URL

Open in new window

☒

Cancel

Save

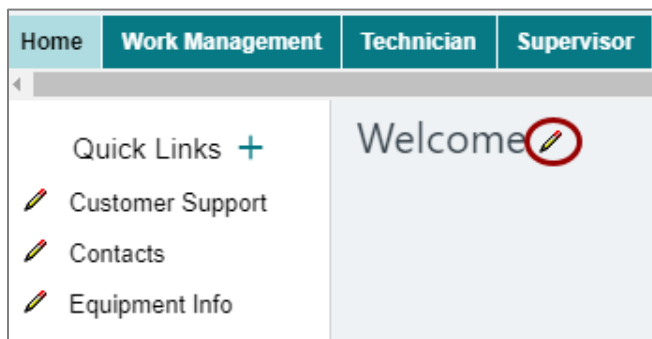
Delete

2. Edit the information accordingly and click **Save**.
3. Delete the link by clicking **Delete**.

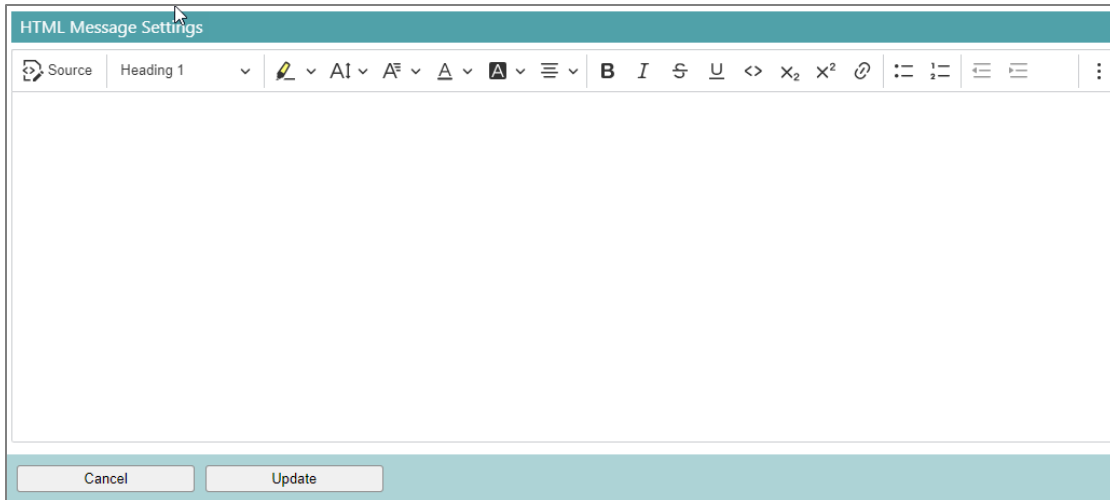
Welcome Module

To customize the welcome message:

1. Click the **Edit icon** next to the Welcome title.



The HTML Settings page displays.



2. Enter plain text or HTML in the Desktop Content area to customize the Welcome message displayed on the Home page. Click **Source** in the upper left corner if you plan to enter HTML content directly. Enter plain text or HTML in the Mobile Content area if your company has mobile users.
3. Customize the appearance using the HTML Message Setting toolbar.
4. Click **Update** to update your Welcome message or click **Cancel** to cancel the action.

To add an image to the Welcome area:

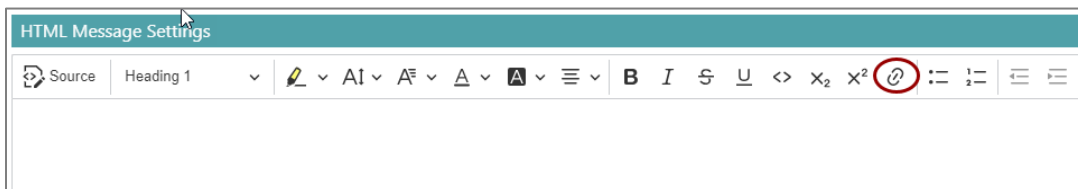
1. Place the image in the directory within *WebModules\Web\Images* folder.



Note: Create a custom directory to keep all user added images centralized and prevent them from being overwritten in future upgrades. For example, the location would look like the following:

http:\\<server>\<instance>\WebModules\Web\images\<customdirectory>\myimage.png

2. From the HTML Message Settings toolbar, click the down arrow in the image section.



3. Place the link to the image uploaded previously to your images folder in the **URL** field.
4. Click **Ok**.

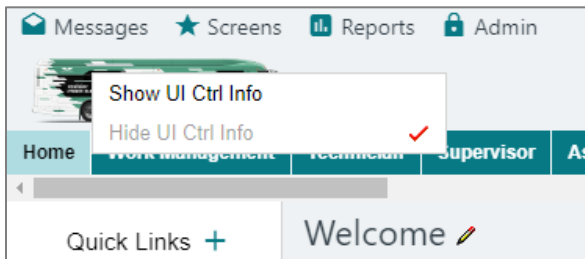
User Interface (UI) Options

Enabling and Disabling UI Control Mode in Web Modules

In Web Modules, most controls are assigned to UI controls for tailoring and language support.

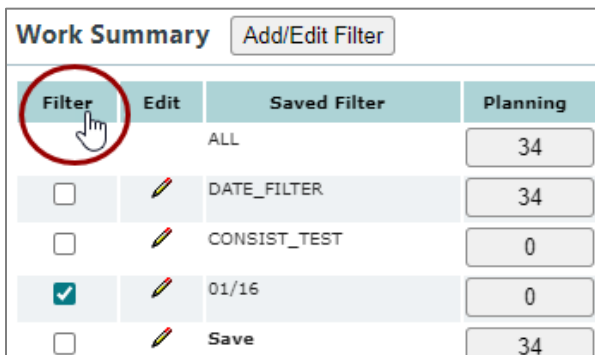
To use UI controls:

1. To turn on the UI controls, right-click on the logo in the upper-left corner.
2. Click **Show UI Ctrl Info**.

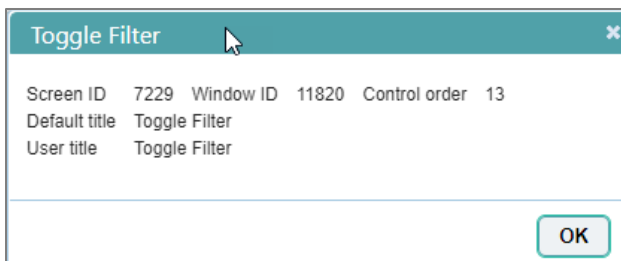


The UI Ctrl mode is enabled.

3. Hold the **Shift** button and click on a label (for example, Filter below). This method is used to see information for both web modules and Enterprise Portal screen fields and labels.



A dialog box displays the Screen ID, Window ID, Control Order, Default Title, and User Title.



4. Click **OK**.
5. To turn off the UI controls, right click on the logo.
6. Click on Hide UI Ctrl Info.
7. Click **OK**.
8. Refresh your browser which will take you back to the home page.

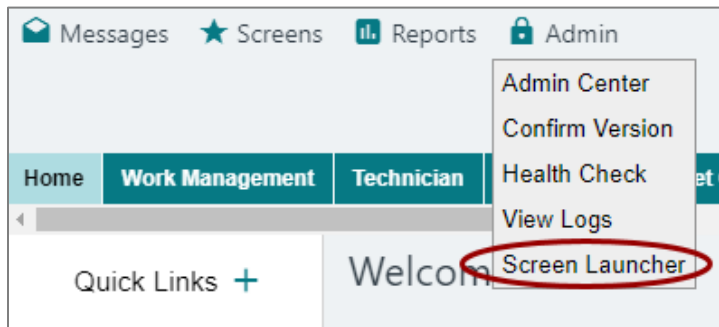
The UI Ctrl mode is disabled.

Modifying a UI Control for a Web Modules Page

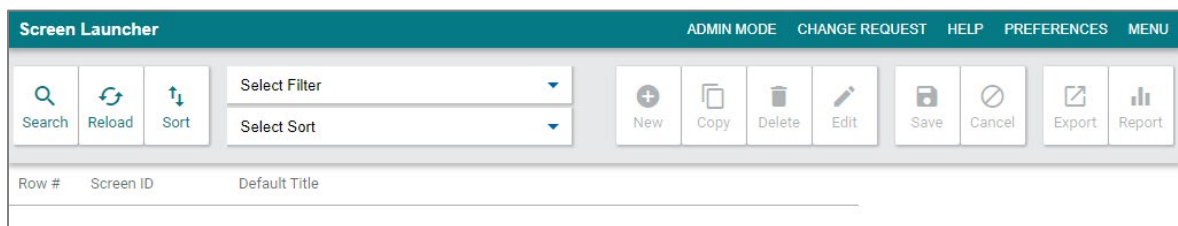
Administrators can use the following processes to modify a UI control for a Web Modules page through the Enterprise Portal Screen Launcher.

To open the screen for UI modification:

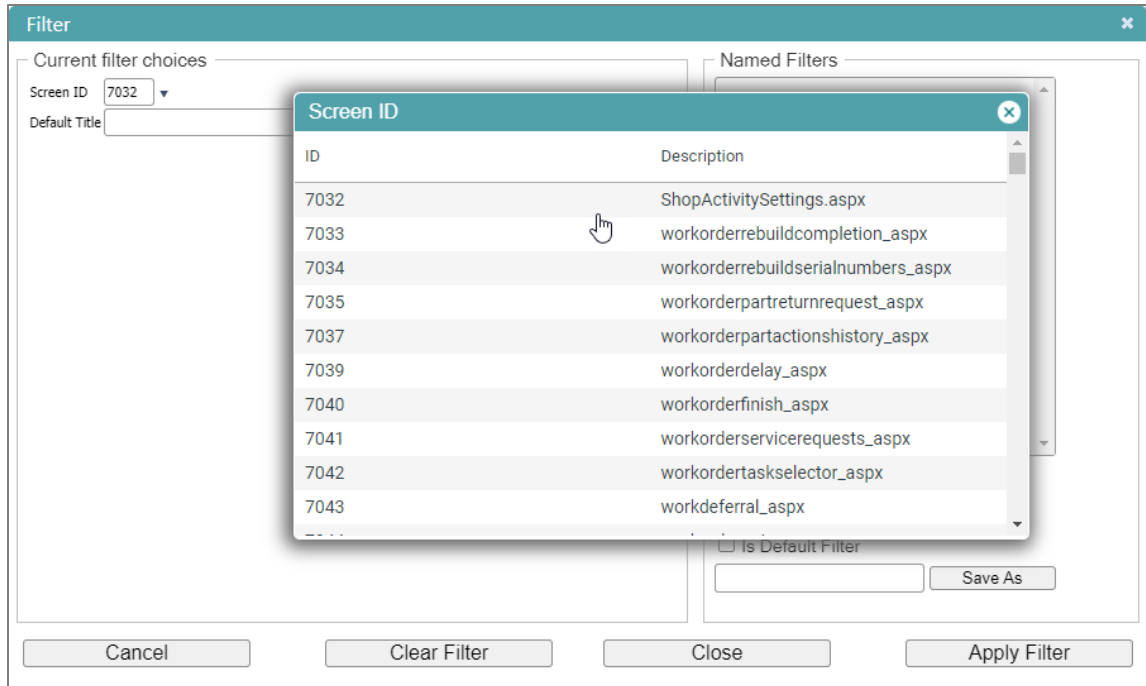
1. From the Web Modules, click the Admin shortcut and click Screen Launcher.



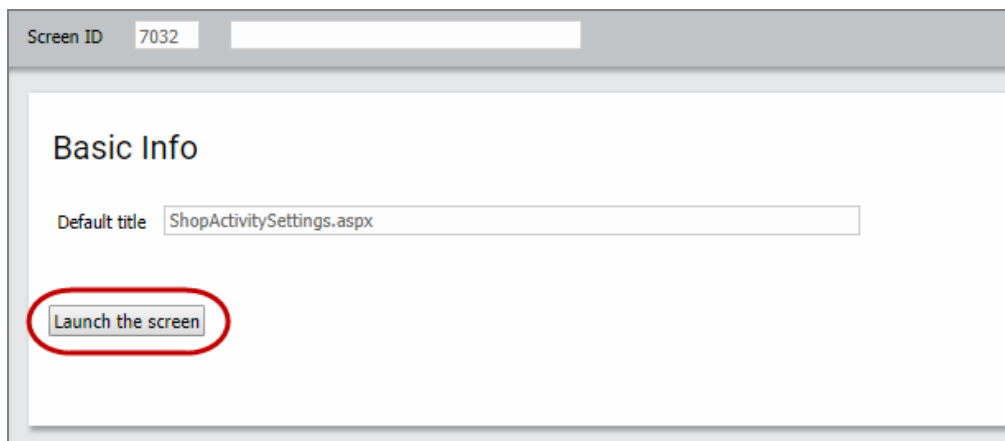
2. The Screen Launcher screen displays.



3. Click Search to find the screen you want to edit.



4. Click **Apply Filter**.
5. Click **Launch the screen**.



6. Use the appropriate **Admin Mode**, as described below, to edit the UI as needed.

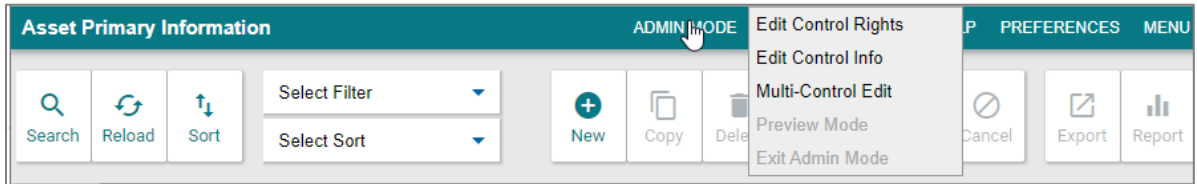
Admin Mode

Use Admin mode to control UI in the Enterprise Portal screens and Web Modules. You can choose to hide or display fields, change admin options, field titles, etc. To use admin mode, you must have administrative rights in the Enterprise Portal.

Starting Admin Mode

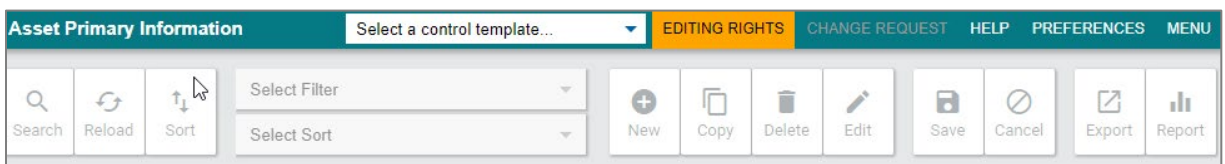
To start Admin mode:

1. On an Enterprise Portal screen, click **ADMIN MODE**.



2. Several options display:
 - **Edit Control Rights:** Edit user control rights for selected fields.
 - **Edit Control Info:** Edit control information such as hiding fields and tabs.
 - **Multi-Control Edit:** Edit multiples records at a time
 - **Preview Mode:** Choose a user group while in preview mode to see what that user group will see when using that page.
 - **Exit Admin Mode:** Exit any admin mode you are currently using. This option is greyed out unless you are currently in an admin mode and click **Admin Mode**.
3. Select the needed admin option.

Admin mode changes to Editing Rights, Editing Info, Multi-Edit Mode, or Preview Mode depending on the option chosen.



4. For more information on using the different options, refer to the options below.

Using Edit Control Rights

The option for editing control rights allows you to edit the rights for user groups. This changes what user groups have access rights to pages. Editing control rights cannot be accessed while editing a record or inserting a new record.

To edit rights:

1. Start the **Edit Control Rights** mode as explained in the [Starting Admin Mode](#) section.
2. To select a field or tab to edit rights to press and hold **Shift**, and then click the field.

The Edit Control dialogue displays control information on the left side of the dialogue and options for editing control rights on the right.

3. From the **Control Template** drop-down field, select a control template. This is the user group template (applied through the User Groups screen) that controls user access rights to screens, their tabs, data, and reports. For more information on user groups, refer to the help for the User Group screen.
4. Select **Deny View?**, **Deny Update?**, or **More Info?**.
 - **Deny View?:** Check this box to turn off access to the field. This hides the field on the screen.
 - **Deny Update?:** Check this box to turn off access to update the field. The user can see the field, but not edit.
 - **More Info?:** Check this box to make this field a more-info type field. More info fields are hidden or minimized on the web screen until a user clicks the button to expand those fields. This field applies to fields that display in the web screen only.
5. When you are done making changes, click one of the options at the bottom of the pop-in.
 - **Close:** Closes the pop-in without saving changes.
 - **Save and Close:** Saves the settings and closes the pop-in. This button is greyed out until a setting is changed.
 - **Save:** Saves the settings, but keeps the pop-in open (this also can be used while you are in progress to save the current changes without exiting). This button is greyed out until a setting is changed.

Using Edit Control Info

The option for editing control info allows you to change default text of a label, set a control as required or highlighted on the screen, and other options that change the way users interact with that control.

To edit control info:

1. Start the **Edit Control Info** mode as explained in the [Starting Admin Mode](#) section.
2. To select a field or tab to edit info for, press and hold **Shift**, and then click the field.

The Edit Control dialogue displays with control information on the left side of the dialogue, and your options for editing control info on the right.

3. Edit the necessary information fields. These fields can vary from control to control as to which options are available to edit:
 - **User Title:** Enter a title for the field to override the default title. For label controls, this changes the text shown to the user.
 - **Required Field?:** Check this box to make this a required field.
 - **Attention Field?:** Check this box to make this a field that is highlighted.
 - **Zoom Buttons:** Zoom buttons display as magnifying glasses and open a specific screen in the Enterprise Portal. These buttons use the screen, window, and control IDs found for specific areas when you are in admin mode. These buttons either show status of Enabled or Disabled on the Edit Control pop-in. You can

only have one zoom button set at a time for a field, either single zoom or multi-zoom.

- **Single Zoom Button:** Add a zoom button to the field. Click **Edit** to add or edit a zoom button. When you are done entering the following information, click **Save Zoom Button**, or click **Close** at any time to cancel out of this pop-in.

Enabled?: Check this box to enable the zoom button.

Screen ID: Enter the ID of the screen to open with the zoom button.

Window ID: Enter the window ID.

Control ID: Enter the control ID.

- **Multi Zoom Button:** Add a zoom button to the field. When you are done entering the following information, click **Save Zoom Button**, or click **Close** at any time to cancel out of this pop-in.

Add Control: Add a zoom control.

Remove Control: Remove the last zoom control on the list.

Enabled?: Check this box to enable the zoom button.

Screen ID: Enter the ID of the screen to open with the zoom button.

Window ID: Enter the window ID.

Control ID: Enter the control ID.

Source Window ID: The window ID of the item you want to fill in the target screen.

Source Control ID: The control ID of the item you want to fill in the target screen.

Target Window ID: The window ID of the field you want to fill with the source information.

Target Control ID: The control ID of the item you want to fill in with the source information.

- **Filter?:** This section enables you to set whether this field displays for the filter and sort buttons of the Enterprise Portal. Options allow you to turn on this field for both filter and sort, or only one or the other.

- **Custom List:** This drop-down contains the custom lists defined in your environment. Selecting a list from the drop-down allows users to access that list as their choice-list from the field.
 - **Entry must exist in defined list?:** If this box is checked, the user must choose an option from that list when filling in this field (if they enter any other value, a validation error will display). If this is unchecked, users can either select from the defined list or enter any value.
4. When you are done making changes, click one of the options at the bottom of the pop-in.
- **Close:** Closes the pop-in without saving changes.
 - **Save and Close:** Saves the settings and closes the pop-in. This button is greyed out until a setting is changed.
 - **Save:** Saves the settings but keeps the pop-in open (this also can be used while you are in progress to save the current changes without exiting). This button is greyed out until a setting is changed.

Using Multi-Control Edit Mode

Use the multi-control edit mode to edit multiple control right or control info items at the same time. With the following editing controls, you can edit both global rights, and rights that are controlled through user groups. In the editing area, these items are separated by the Template drop-down menu.

1. Items above the **Template** drop-down affect global rights. Users with rights to the screen affected by these changes, will see the options as they are set up regardless of which user groups they belong to.
2. Items below the **Template** drop-down are affected by the user group template, and changes will differ for users depending on which user groups they belong to. Select a template in this field to choose what those users can view, update, and see more info for.

To use multi-control edit mode:

1. Start the **Multi-Control Edit Mode** as explained in the [Starting Admin Mode](#) section.
2. Press and hold **Shift** and **click** fields to select them.

Basic Info

Job type: **REPAIR** (dropdown), Equipment ID: [highlighted], License number: [text field]

Meter 1: [text field], Meter 1 validation: [highlighted], Life meter 1 usage: [text field]

Meter 2: [text field], Meter 2 validation: [highlighted], Service status: [text field]

Account ID: [text field]

Priority ID: [text field]

Employee ID: [text field]

Fields display with yellow highlighting when selected.

3. Click the slider to open the edit menu.

MULTI-EDIT MODE

Select a control template... (dropdown)

Required? [Set All] [Clear All]

Highlighted? [Set All] [Clear All]

Template: [Select a control template... (dropdown)]

Deny View? [Set All] [Clear All]

Deny Update? [Set All] [Clear All]

More Info? [Set All] [Clear All]

[Save Controls]

1 Selected Controls

Model year	Required?	Highlighted?	Deny View?	Deny Update?	More Info?
Window ID: 12347	☐	☐	☐	☐	☐
Control ID: 2	☐	☐	☐	☐	☐

Selected controls display in the bottom section of the edit menu.

4. To remove a selection, press and hold **Shift** and click the highlighted field, or click the **X** in the top-right corner of the selected control in the slider menu.
5. Edit the items as needed. Edit multiple items with the same edits, or specific controls for individual items.

To edit all selected items:

- Click **Set All** or **Clear All** to set all selected controls with the same option. For example, click **Set All** for the **Required?** option to set all the selected items to be required.



Note: For the user-group affected options (under the **Template** field), you must select a control template before editing controls for the selected user group.

To edit individual items:

- Check or uncheck the options in the individual controls to set each control.
- When you are finished making changes, click **Save Controls**.

The controls are saved and the page refreshes. Your selections will remain selected in case there are other changes to make.

Using Preview Mode

Use the preview mode to view a page with the rights of a specific user group. This allows you to ensure you have the correct settings and available fields, tabs, pages, etc. for the groups that need them.



Note: You must click **New** to create a new record or click **Edit** to edit the record on the current screen to have access to the preview mode.

To view the preview mode:

1. Start the **Preview Mode** as explained in the [Starting Admin Mode](#) section.
2. From the **Select a user group** choice-list, select the user group for this screen.

The screen displays as the selected user group will see when they use the page.

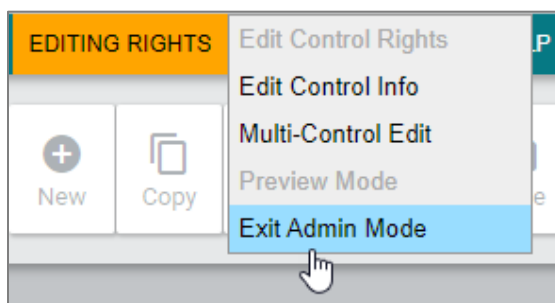
3. Change the user group as needed to see any group's screen views.

Exiting Admin Mode

Closes the administration mode and returns the user back to the normal Enterprise Portal mode.

To exit Admin Mode:

1. In the top-right corner of the Enterprise Portal, click **EDITING RIGHTS**.



2. Then click **EXIT ADMIN MODE**.

The Enterprise Portal returns to the mode for regular use.

Access a Web Modules Tab via a Properly Formatted URL

Via a properly formatted URL, clients can link into Web Modules from an external system. It is possible to access a specific Web Modules portal/page and to access a user's default Web Modules tab. For formatting information, please refer to [A.3 Formatting a URL to Access a Web Modules Tab](#).

Customize the Logo

To display your company's logo at the top of all Web Modules pages, replace the file mylogo.gif (found in the Web Modules server's **WebImages** directory) with your organization's logo picture file. The new file must be named mylogo.gif and should ideally be between 180-475 pixels wide by 45-62 pixels tall.

 If you customize the logo, it is necessary to give security rights for AUTHENTICATED USER and IUSR to access the custom **mylogo.gif** file.

Appendix A. Technical Configuration

A.1 Sharing and Migrating Tabs

Tabs and module settings are managed in the database. This makes it easier to manage multiple web instances that share the same tabs but may require additional steps if you are upgrading from a prior version.

To control the tabs in any additional web instances that you install, you can now use the **Portal Name** setting in **Configurator** (on the **Advanced** tab):

- If you want to have two different web instances that have different tabs and module settings, each instance needs a unique Portal Name.
- If you want to have two or more different web instances to have the same tabs and module settings (for example: you are using a load balancer), each instance needs to share the same Portal Name.

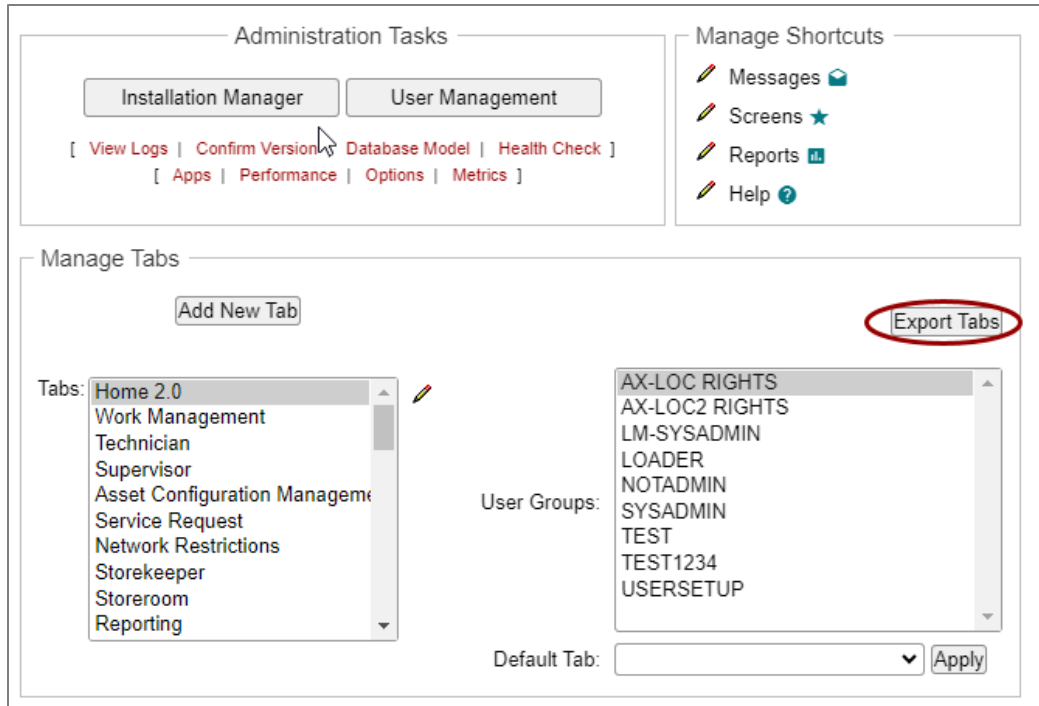
If you deploy two web instances with the same portal name, then users can connect to either web instance and see the exact same tabs and the same module settings.

Migrating Tabs from Test to Production

Use this process to migrate tabs from a test server to a production server.

This will migrate the tabs and their modules, but will **not** migrate the module settings

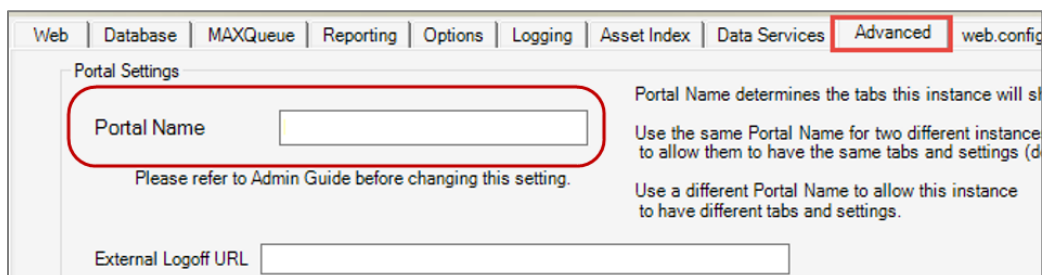
1. Navigate to the Web Modules **Admin Center** on the test server.
2. Click Export Tabs.



The **PortalCfg.xml** file will be exported to the LogDir folder.

3. Stop the internet service on the production server.
4. Copy **PortalCfg.xml** from the **Logs** folder of the test server to the **web** folder of the production server (to the same folder that contains **web.config**). If there is already a **PortalCfg.xml** file in that folder, rename it to "**PortalCfg.xml.old**" before copying.
5. Navigate to the **bin** folder of the production instance.
6. Launch **Configurator.exe**.
7. Go to the **Advanced** tab.
8. Change the new portal name to a unique value, such as **Prod**. To force the instance to reload the PortalCfg.xml file, you must confirm that no other web instances against the database are using the Portal Name value.

 Note: Only change the new web portals. Leave old production portals as they are already named.



9. Use a web browser to access the Web Modules production instance and the new modules/tabs will be migrated.
10. To migrate the tabs from test to additional production instances, go to each additional instance's web/bin folder, launch **Configurator.exe**, set the Portal Name to the same name you used in **Step 8**, and save then exit Configurator. Use a web browser to test each additional instance and verify that the tabs are consistent with the other instances using the same Portal Name. If you encounter errors, check **InfoCenter.log** for details.

A.2 Creating URLs to Launch Web Modules Reports

This appendix explains how to construct an URL that will automatically launch a Web Modules report with pre-defined filter criteria.

This is especially useful when used in the Dashboards Module as an element's drill down URL (the URL that is launched when a dashboard element is double-clicked). It is also useful when building HTML links to pre-defined reports.

URL Construction

To construct a URL, it is necessary to follow the conventions as listed in this section.

The generic form of the reporting URL is as follows:

http://<WebserverName>/<VirtualDirectoryName>/Reporting/ReportViewer.aspx?ReportName=<ReportPath>%2f<ReportName>&Page=Report&<FilterCriteria>

Where:

- **<WebserverName>** is the name or IP address of the Web Modules Server
- **<VirtualDirectoryName>** is the name of the Web Modules Virtual Directory (typically "Web Modules")



If the Web Modules environment uses HTTPS or a load balancer, it may be easier to omit the <WebserverName> and <VirtualDirectoryName> elements, leaving the URL as:

Reporting/ReportViewer.aspx?ReportName=<ReportPath>%2f<ReportName>&Page=Report&<FilterCriteria>

While you cannot test the URL in this format by pasting it into the Internet Explorer (IE) address bar, this is the preferred format as it handles multiple-server environments.

- **<ReportPath>** is the folder or folders where the report you want to run is located.

- **<ReportName>** is the filename of the report you want to run. This is the filename of the report, not the title of the report. Example: for the report titled **Labor by Task/Class**, the filename is **FA-LaborByTaskClass.rpt**. The filename can be found on the report's About page (through the Reporting tab).



All spaces need to be replaced with a plus sign (“+”). Example: the “Shop Operations” folder must be referred to as “Shop+Operations”.



If you need to refer to a subdirectory, use “%2f” instead of a forward slash.

- **<FilterCriteria>** is the list of all filter elements for the report, with filter values. Rules for creating this section are described in the area below titled *Detail on Filter Criteria*.

An example of an URL pointing to the Equipment Inventory List by Department, for all departments, all assets would be:

`http://localhost/InfoCenter/Reporting/ReportViewer.aspx?ReportName=Equipment+Info%2fFA-EQInvList-Dept.rpt&Page=Report&Depts=[ALL]&Asset=All`

Detail on Filter Criteria

In the above example, the filter criteria are as follows:

`Depts=[ALL]&Asset=All`

As you can see, each filter on a report has a specific parameter name that must be used in the URL (for example, “Depts” and “Asset”).

The easiest way to find the parameter names for a given report is by following the steps below:

1. Log into Web Modules and go to the **Reporting** portal.
2. Find the report you want to link to and click on the report name to view.
3. Click the **XML** button next to the report.
4. Open the file in a text editor.
5. Locate `<ReportSettings>` -> `<FilterItem>` -> `<Name>` to see the parameter name.



All filter parameter names must be included in the URL for it work correctly. If not, the URL will take the user to the Filter page, where the missing filter criteria must be entered.

Testing the URL

To test your Web Modules Reporting URL, follow the steps below.

1. Log into Web Modules using a User ID that has access to Web Modules Reporting.

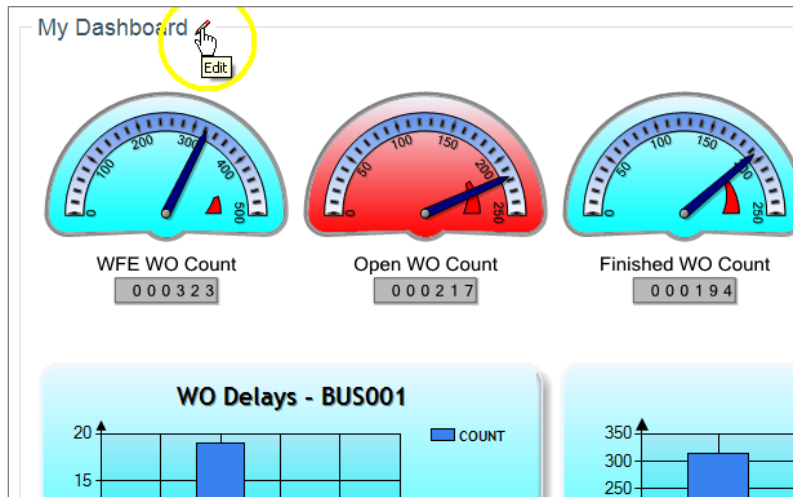
2. Paste your URL into the Internet Explorer address line.
3. Hit **Enter**.

The report desired, with the appropriate filters applied, should appear in your web browser

Using Web Modules Reporting URLs in the Dashboard Module

Once you have a fully formed and tested URL, it can be used as the Drill Down URL for a Web Modules Dashboard element. To do so, follow the steps below:

1. Log into Web Modules using a User ID with system administrator privileges.
2. On any Dashboards area, click the **Edit**  icon next to the module title.



3. Click on **Gauges**.
4. Select the gauge element you wish to update.

If you want to link to an URL or Report, enter the URL in **Drill Down URL** and skip to Step 6. If you want to link to an Enterprise Portal Web Screen, proceed to Step 5.

5. Click the **Web Screen Link** button to build the web screen link.

Gauge Editor

Choose a gauge to modify: My OPEN Work Orders (Gauge-Speedometer) Delete

Gauge Definition

KPI: Choose KPI Work Orders - Count OPEN at My Location

Name: My OPEN Work Orders Type: Speedometer

Description: Open Work Orders at my Location

Tooltip Text: Open WOs

Label Text: Work Orders - Count OPEN at My Location

Drill Down URL: top:cash:openEPWindow(2037,2037,189-9={FAVAR_USERSSESSIONLOC}); ☒ Open in new window

Refresh Save Back

Web Screen Link

Screen ID: 2037

Optional Filters:

- Window ID: 189 Control ID: 9 Value: {FAVAR_USERSSESSIONLOC}
- Window ID: Control ID: Value:

Available variables from KPI - copy and paste into Value field (including the {}s):
{FAVAR_UsersSessionLoc}

Build Link URL

- Place a check in **Open in New Window** if you want the link to open in a separate window from the main Web Modules Dashboards IE instance.
- Click **Save**.

Double-clicking on the specified gauge element will now launch the Web Modules report.

Special Dashboard Filter Rules

The Web Modules Dashboard elements may automatically filter themselves based on the user logged into the system. For example, a gauge may be configured to display the count of open work orders at the user's session location. These same user-contingent filter criteria may be worked into the Drill Down URL filter criteria.

In place of actual data values, any of the following user-based variables may be inserted into the URL filter criteria area:

Variable Name	Function
{FAVAR_UsersSessionLoc}	The session location ID of the logged-in user (as defined on the Users screen)
{FAVAR_UsersEmployeeID}	The associated employee ID of the logged-in user (as defined on the Users screen)
{FAVAR_UsersOperatorID}	The associated operator ID of the logged-in user (as defined on the Users screen)
{FAVAR_UsersVendorID}	The associated vendor ID of the logged-in user (as defined on the Users screen)
{FAVAR_UsersOperatorsDept}	The department ID of the associated operator ID of the logged-in user (as defined on the Operators – Primary Information screen)
{FAVAR_Now}	The current datetime, at the moment the URL is launched.
{FAVAR_TodayStart}	Datetime of today's date, at midnight.

Variable Name	Function
{FAVAR_WeekStart}	Datetime of the previous Sunday, at midnight.
{FAVAR_MonthStart}	Datetime of the first of the current month, at midnight.
{FAVAR_QuarterStart}	Datetime of the first of the month of the current quarter start (January, April, July, or October) at midnight.
{FAVAR_YearStart}	Datetime of the first of January, current year, at midnight.

Example 1

http://localhost/InfoCenter/Reporting/ReportViewer.aspx?ReportName=Equipment+Info%2fFA-EQInvList-Dept.rpt&Page=Report&Depts={FAVAR_UsersOperatorsDept}&Asset=All



The above variables can also be used as filter values in Ad Hoc Query reports, but ONLY if the Ad Hoc Query report is used to drive the data for a Gauge/Chart in Dashboards module. It is only possible to test this variable where clause value by first creating the Ad Hoc Query report, saving it (under the category "KPI"), and then assigning it to a Gauge or Chart in Dashboards module (via the **Choose KPI** button, on the Ad Hoc Query KPI tab).

Using Web Modules Reporting URLs in Web Modules HTML Pages

Local Reporting

An HTML area may be added to any Web Modules tab. To create a link to a Web Modules report in an HTML section, use the following format:

```
<a href="URL">Description</a>
```

Where **URL** is the Web Modules Reporting URL and **Description** is how you want the link to read on the page.

For example:

```
<a
href="http://localhost/InfoCenter/Reporting/ReportViewer.aspx?ReportName=Equipment+Info%2fFA-EqRegistrationExpiration.rpt&Page=Report&Dept=[ALL] &NumDays=90">Link to Vehicles Coming Due for Registration in 90 Days.</a>
```

This code creates a link to a report in any HTML area.

External Reporting

Users must go through internal authentication code in order to be able to run external reports since reports are handled through a separate web application.

Use the following javascript:

```
top.PortalBanner.LaunchCrystalReport("[0]")
```

- where [0] is the relative folder & filename of the report (for example, Equipment Info/FA-EQDetail.rpt).

A.3 Formatting a URL to Access a Web Modules Tab

Link into Web Modules from an external system through a properly formatted URL. The sections below provide information and examples to properly format a URL to access a specific Web Modules portal/page and to access a user's default Web Modules tab.

URLs to Access a Web Modules Portal/Page

The Web Modules Login page will parse the user and password from the URL. It decrypts these values and attempts to login. If the login is successful, Web Modules will parse the jumpto arguments to build the proper URL redirection necessary for jumping directly into a specified portal. Some portals will support further jumpto arguments to jump directly to a page within the portal.

If the server, instance, user, password and asset ID are passed into a correctly built URL string, the user will be logged in and load the portal or page that is specified.

Building a URL Directly to a Web Modules page

`http://[HOST]/[INSTANCE]/ICLogin.aspx?e=2&jumpto=[PORTAL].[Page]&[vars]`

Keyword/ Letter	Description
e = 2	Indicates Rijndael Encryption (Optional, leave out if encryption is not used. Recommend always using in production so that user name and password will not be exposed.)
jumpto	Specifies the portal to directly load and may contain further arguments to specify the page.
<keys>	Some pages may require specific keys to load the page properly.

Example to the EquipmentManagement Page:

`http://[HOST]/[INSTANCE]/ICLogin.aspx?e=2&jumpTo=SupervisorPortal.EquipmentManagement&equipid=EQID`

`http://[HOST]/[INSTANCE]/ICLogin.aspx?e=2&jumpTo=TechnicianPortal.EquipmentManagement&equipid=EQID`



Each variable should be URL encoded to protect against using unsafe URL characters.

Portal jumping and some limited page jumping is supported. To jump to a portal, the name of the starting **.aspx** can be used to load any portal supported/built into the Web Modules instance. Jumping to a page though requires some extra setup. The Web Modules instance must go through the proper portal setup/workflow before loading a page directly. Currently, there are two such pages provided. Jumping to a page also requires that the correct portal is specified.

Format of Portal.Page Jumping:

`http://[HOST]/[INSTANCE]/ICLogin.aspx?e=2&jumpTo=[PORTAL].[Page]&[vars]`

Supported [PORTAL] ids (partial list):

- AccountingPortal
- CustomerAccess
- EquipmentPlanning
- EquipmentPortal
- PerformancePortal
- ProductionManagerPortal
- ReplacementPortal
- ServiceRequest
- StorekeeperPortal
- SupervisorPortal
- TechnicianPortal
- WarrantyProcessorPortal
- WarrantySupervisorPortal
- WarrantyWriterPortal

Supported [Page] IDs and required [vars] (variables):

- EquipmentManagement requires equipid=<EQ>
- WorkOrderMain requires workorder=<WOLOC-YR-NO>

Portal Jumping Examples:

`http://[HOST]/[INSTANCE]/ICLogin.aspx?e=2&jumpTo=AccountingPortal`

`http://[HOST]/[INSTANCE]/ICLogin.aspx?e=2&jumpTo=EquipmentPlanning`

`http://[HOST]/[INSTANCE]/ICLogin.aspx?e=2&jumpto=ServiceRequest`

`http://[HOST]/[INSTANCE]/ICLogin.aspx?e=2&jumpto=StorekeeperPortal`

Page Jumping Examples:

`http://[HOST]/[INSTANCE]/ICLogin.aspx?e=2&jumpto=SupervisorPortal.EquipmentManagment
&equipid=EQ1`

`http://[HOST]/[INSTANCE]/ICLogin.aspx?e=2&jumpto=TechnicianPortal.EquipmentManagment
&equipid=EQ1`

`http://[HOST]/[INSTANCE]/ICLogin.aspx?e=2&jumpto=SupervisorPortal.WorkOrderMain&workorder=WOLOC1-2012-20`

`http://[HOST]/[INSTANCE]/ICLogin.aspx?e=2&jumpto=TechnicianPortal.WorkOrderMain&workorder=WOLOC1-2012-20`



[PORTAL]s [Page]s and [vars] are not user definable, these are static out of the box provided values noted above.

A.4 Mobile and Mapping DNS Settings

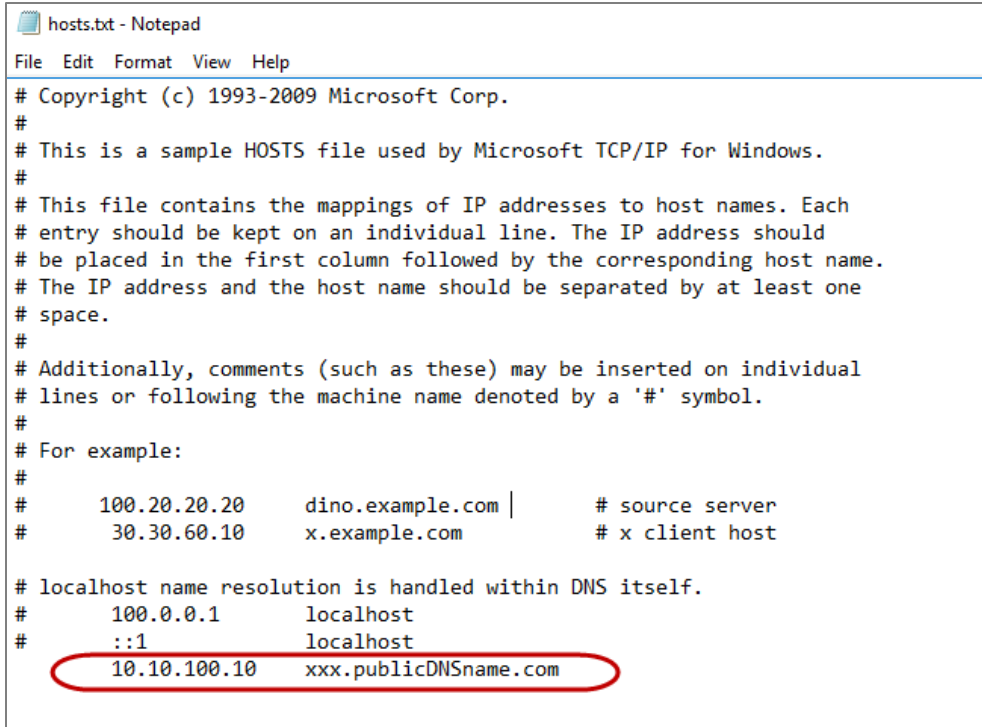
DNS forwarding for organizations using mobile and mapping capabilities may not be recognized between the internal IP and the external ID on the same machine. This address mapping is needed for mobile data services to work correctly. To fix this, edit the hosts file to add your internal IP and the public DNS name.

To edit the Hosts file:

1. Open the Hosts file. This file is found in the following location:

C:\Windows\system32\drivers\etc\hosts

2. Enter your internal IP and public DNS name after the # entries as shown in the screenshot below.



```

hosts.txt - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       100.20.20.20    dino.example.com |    # source server
#       30.30.60.10     x.example.com       # x client host
#
# localhost name resolution is handled within DNS itself.
#       100.0.0.1       localhost
#       ::1             localhost
#       10.10.100.10    xxx.publicDNSname.com

```

3. Save and close the file.

A.5 Running Applications in Console Mode

Data Services

To facilitate simpler troubleshooting for administrators, commands can be entered when Data Service is in console mode. The following is a list of commands that can be entered. This list is also available from within console mode by typing help.

Command	Result
help	Help menu will be displayed. Command list is available.
clear	Clears the console.
reloadmaps	Maps will be reloaded.
rebuildindex	If using Elasticsearch, index will be rebuilt.
healthcheck	Health check will display.
quit	Closes the console and data services.

A.6 Restarting Web Modules

If Web Modules must be restarted, there is a particular order that the several services and programs need to be restarted. This will ensure that all programs and services come back up cleanly and in the right order. As a good memory clean up and precautionary task, it is recommended to find a suitable low usage or downtime and using the Configurator to set a restart of all these items on a periodic basis. Some organizations may want this to be performed daily or weekly. We recommend daily restart for the web app, but this should be based on needs/usage.

To restart Web Modules:

1. Stop the Job Scheduler service (if using the Scheduling Module for reports scheduling).
 2. Through the IIS Management tool, stop the web application pool for the instances of Web Modules you wish to restart.
 3. Stop Crystal's Report Application Server (if using Reporting).
 4. Stop all instances of the Application being used for Web Modules.
 5. Start all instances of the Application being used for Web Modules.
 6. Start Crystal's Report Application Server (if using Reporting).
 7. Using the IIS Management tool, restart the web application pool or application for the instances of Web Modules you wish to restart.
 8. Start the Job Scheduler service (if using the Scheduling Module for reports scheduling).
-  Please contact Customer Support if you have questions regarding your organization's specific setup or certain situations that may require additional items to be restarted.

A.7 Network Configuration and Anti-virus Recommendations

EAM Suite components should be installed on an internal secure server and should not be publicly accessible.

The network should be configured so Web Modules and Data Services ports shall be accessible to clients and users that use those EAM components. Typically, the application server only needs to be accessible on the same machine as Web Modules, Data Services, and

MAXQueue. At times, application ports can be made accessible internally only so EAM components on other local servers (such as MAXQueue on its own machine) can use the server. This should only be done so these internal machines can reach the application server.

 It is recommended to never expose an application port externally.

If you do choose to use a DMZ server to allow a public facing Web Modules (for example, if it is needed to expose EAM for contractors outside of the network), ensure only essential ports are exposed such as the standard secure web port 443.

For anti-virus scanning, it is recommended to not scan the Trapeze folder where the EAM Suite components are installed to ensure the best performance of EAM. A specific scan of the Web Modules "Upload" folder should be setup which can be configured through EAM Suite configuration.

A.8 Configure Single Sign-On (SSO)

There are three areas you must configure to allow Single Sign-On:

1. Windows security settings/permissions to allow the correct authenticated users access to the website – this varies depending on the organization's security needs and settings. You may choose to use windows domain authentication, for example to allow only users in the domain to access the web server. With Single Sign-On, users typically are required to provide valid windows credentials (user, domain, and password) when first connecting to the web server, then are automatically logged into Web Modules based on whether their windows login is mapped to a user.
2. User setup via the GUI to set the **External identifier** field to map to a valid windows user ID, but only for the trusted users that have windows accounts on the server/domain.
3. Web Modules settings via Configurator or manual IIS configuration if advanced settings are required.

SSO Methods

For details and specific instructions for each method, please refer to the SSO Configuration Guide. Currently supported SSO methods are as follows:

1. ADFS - Active Directory Federation Services
2. Kerberos or NTLM - Integrated Windows Authentication
3. LDAP - Lightweight Directory Access Protocol
4. OAuth 2.0 - Open Authorization 2.0

5. OIDC - OpenID Connect

- ⚠** MobileFocus, FuelFocus, and MAXQueue use different authentication methods and are not designed to work in an SSO environment. When configuring MobileFocus and FuelFocus, you must use a non-SSO web service URL. Please see the *MAXQueue Administrator Guide* for details on configuring MAXQueue.

GUI User Setup for SSO Activation

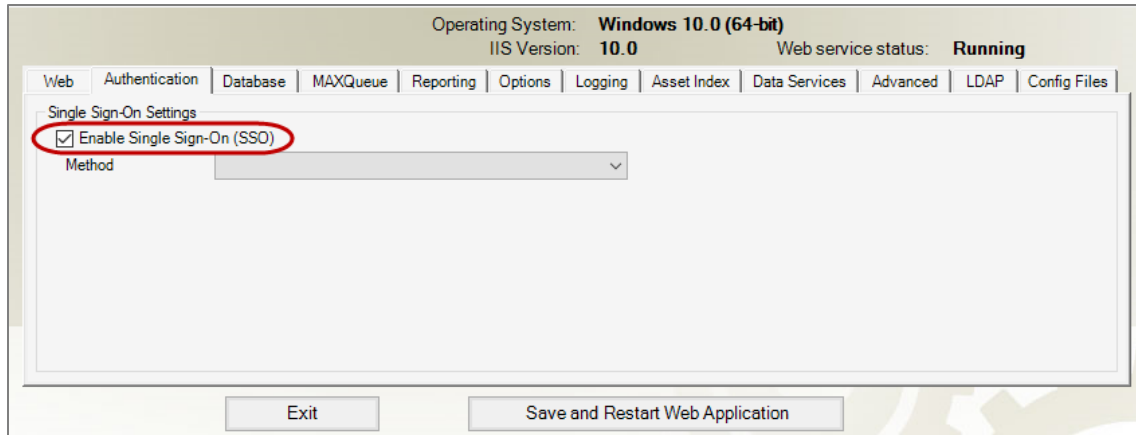
1. Start a GUI Instance.
2. Select **System Mgmt > Setup > Access Rights > Users**.
3. On the Basic Info Tab, enter the **User ID** for which you would like to enable SSO.
4. Enter the user's associated login name in the **External Identifier** field.

The screenshot shows a web form for user setup. At the top, there are tabs: 'Basic Info', 'Groups Currently Assigned', 'Comments', 'Security Options', and 'Printers'. The 'Basic Info' tab is active. Below the tabs, there are several input fields. The 'User ID' field at the top is highlighted with a red rectangle. Below it, there are fields for 'Name', 'Phone', 'New password', 'Email address', 'Associated employee', 'Associated operator', 'Session location ID', 'User currency ID', 'Report group ID', 'Associated vendor ID', 'External identifier', 'FASuite InfoCenter ID', and 'Supported web applications'. The 'External identifier' field is also highlighted with a red rectangle.

5. Save changes and exit the GUI.
6. Complete SSO activation through the Configurator as described below.

Enable SSO via Configurator

1. From the Authentication Tab, check **Enable Single Sign-On (SSO)**.



2. Select the SSO **Method** from the drop-down list.
3. Follow instructions based on method selected.

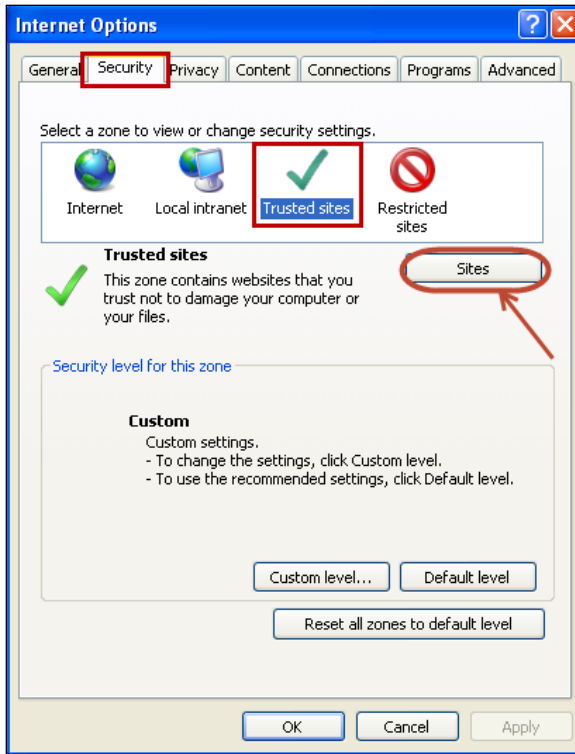
Single Sign-On Browser Configuration

This section provides instructions for single sign-on (SSO) browser configuration using Internet Explorer.

- ✓ Adding the host (web server IP or hostname) to your trusted sites ensures the following features work better:
 - Automatic single sign-on
 - File uploads and file links using absolute pathname
 - Enterprise Portal (and other pop-up windows) shows correct title bar
 - Pop-up blocker issues fixed Single Sign-On

To configure your browser for Single Sign-On:

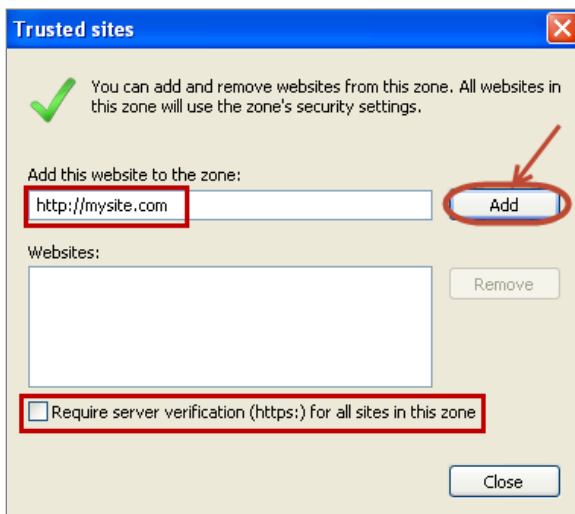
1. Browse to your Web Modules URL.
2. If prompted for a windows logon, enter your username and password to log on.
3. Open the Tools Menu and choose **Internet Options**. If you do not see the Tools menu, hold the ALT key to show the Tools menu.
4. Select the **Security** tab and click **Trusted sites** security zone.
5. Click the **Sites** button.



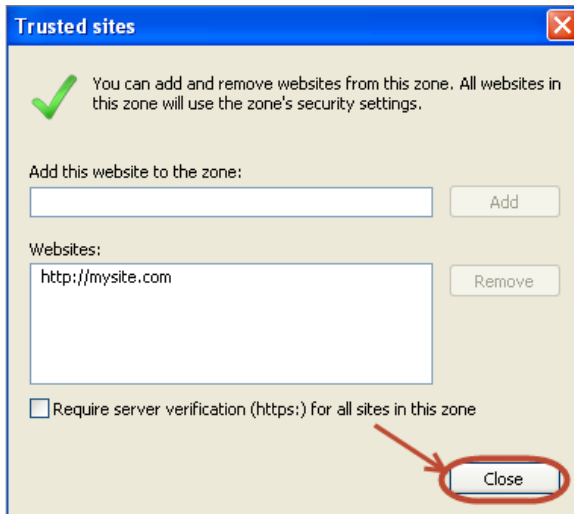
6. Un-check the box: Require server verification (https:) for all sites in this zone.
7. Verify the site in the Add this website to the zone: box. It should be the website that hosts the EAM Web Modules.

 Only the hostname or IP is required. For example, if the website URL is "http://mysite.com/mysite/default.aspx," then the website you add should be "http://mysite.com."

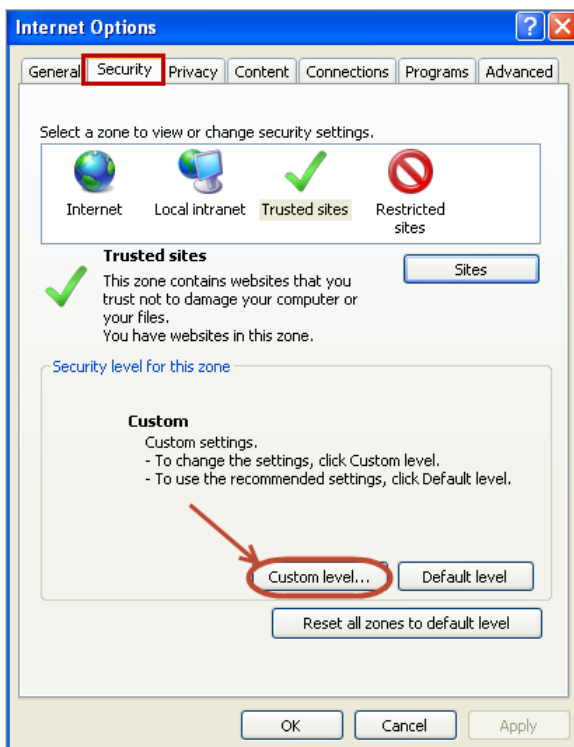
8. Click the **Add** button.



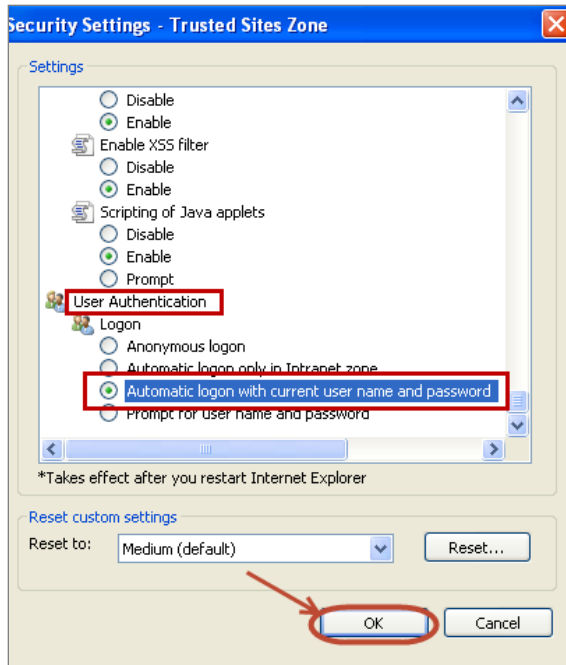
9. Click the **Close** button.



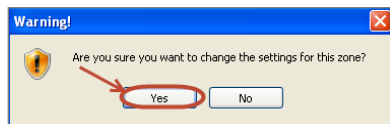
10. Back on the **Security** tab, click the **Custom level** button.



11. Scroll all the way down to find the User Authentication section and select the radio button for Automatic logon with current user name and password.
12. Click the OK button.



13. If prompted to change settings, click the **Yes** button.



14. Click the **OK** button to complete the browser configuration for Single Sign-On.



Testing Automatic Single Sign-on

To ensure automatic Single Sign-On works correctly:

1. Close browser.
2. Reopen browser.
3. Navigate to the Web Modules URL.
4. When prompted, enter username and password, and check **Remember my password**.
5. Once successfully logged into the product, close Internet Explorer again.
6. Repeat steps 4-5. You should no longer be prompted to enter your saved password. If you are, there are likely other security settings in play.