Event Manager 6.9

Installation Guide

Copyright Terms and Conditions

202409090928

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Installation

The following instructions will take you through the process of installing Event Manager onto your server.

Before You Begin

Please ensure you have read the Installation Requirements below and ensure that the machine onto which you are installing the software meets the minimum requirements.

Installation Requirements

Before installing, ensure that you fulfill all the requirements described in the document: System Requirements.

Installed Software

- Windows Server 2012 or higher. Windows 2012 R2 Recommended
- SQL Server 2016 or higher with SQL Full-text Filter service installed
- IIS
- Anti-virus: Event Manager intensively uses the filesystem to make the solution more resilient and fault tolerant. In our experience, we have detected that the real-time anti-virus severely impacts on Event Manager product performance. We therefore recommend excluding the Event Manager installation folder from the anti-virus realtime scan. If there is any internal policy that does not allow the exclusion of full folders, the list of specific files to exclude is:
  - AccessServer\bin\*.log*
  - AccessServer\bin\cache\*.tmp
  - AccessServer\bin\logs\*.log*

- AutoDiscovery\logs\*.log*
- Bentham\Bentham.Service\calendars\*.*[Including subfolders]
- Bentham\Bentham.Service\logs\*.log*
- Bentham\Bentham.Web\*.log*
- DbSetAdmin*.log*
- DbSetAdmin\logs\*.log*
- Inspector\bin\cache\*.fld
- Inspector\bin\cache\*.tbl
- Inspector\bin\calendars\*.*[Including subfolders]
- Inspector\bin\logs\*.*
- Inspector\bin\Persistence\PMDBQueue\*.*
- Inspector\bin\transient\metrics\*.dat
- Inspector\bin\transient\metrics\*.db
- NiceLink\NiceLink Windows Daemon\Agents\Logs\*.log*
- Orchestrator\Orchestrator Engine\cache\*.dat
- Orchestrator\Orchestrator Engine\cache\*.ndx
- Orchestrator\Orchestrator Engine\calendars\*.*[Including subfolders]
- Orchestrator\Orchestrator Engine\Idx\idxfile\*.*
- Orchestrator\Orchestrator Engine\Idx\logs\*.log*
- Orchestrator\Orchestrator Engine\logs\*.log*
- Orchestrator\Orchestrator Engine\logs\*.syn*
- Orchestrator\Orchestrator Engine\transient\*.dat
- Orchestrator\Orchestrator Engine\transient\summary\*.dat
- PMDB\logs\*.log*
- Reports\calendars\*.*[Including subfolders]
- Reports\logs\*.log*

- Scheduler\log\*.log*
- SharedObjects\calendars\*.*[Including subfolders]
- SharedObjects\log\*.log*
- SmartConsole\Calendars\*.*[Including subfolders]
- SmartConsole\logs\*.log*
- SmartConsole\Messenger\logs\*.log*
- SmartConsole\Publisher\logs\*.log*
- SmartConsole WebClient\calendars\*.*[Including subfolders]
- SmartConsole WebClient\log\*.log*
- ThinkServer\cache\*.dat
- ThinkServer\cache\*.ndx
- ThinkServer\config\*.cfg
- ThinkServer\Java System i Server\logs\*.log*
- ThinkServer\JMXServer\logs\*.log*
- ThinkServer\logs\*.*[Including subfolders]
- ThinkServer\Persistence\*.dat* [Including subfolders]
- ThinkServer\Persistence\PMDBQueue\*.*
- ThinkServer\Persistence\t04Common\Orchestrated\*.*
- ThinkServer\PythonLib\Lib\KMBSM\TS_KMBSM_logs\*.log*
- ThinkServer\transient\*.dat
- ThinkServer\transient\summary\*.dat
- ThinkServer\ts_shared_referentials\*.*[Including subfolders]
- User Directory\bin\cache\*.dat
- User Directory\bin\cache\*.ndx
- User Directory\bin\logs\*.log*

  typically located at: <InstallationDiskUnit>\Program Files (x86)\Help Systems

Special considerations for installation

For Installations on Windows Server 2012 machines

Follow the installation instructions as described in Installation.

For Installations on machines without Windows features pre-installed or internet access or when Windows Server Update Services (WSUS) are being used

If the machine where Event Manager will be installed does not have the Windows features pre-installed or internet access or if Windows Server Update Services (WSUS) are being used, perform the following actions:

1. Insert the Windows disk.
2. Unzip the installer.
3. Go to **ISSetupPrerequisities\{1EB68898-6936-4381-A0B0-ECFC770DF16B}** and edit **IIS_Configuration.bat**.
4. At the end of every line starting with :cmd.exe /C%windir%\sysnative\DISM.EXE: add: /Source:<WindowsDiskUnit>/sources/sxs

   > EXAMPLE: cmd.exe /C%windir%\sysnative\DISM.EXE: **add: /Source:D:/sources/sxs**

5. Save the **.bat** file and run the setup.exe.

Upgrading a current installation of Alignia to Event Manager 6.x

Upgrading from 3.X versions or lower

> WARNING: You must uninstall the previous Alignia version before installing Event Manager 6.x.

- If the original version is Alignia 1.4, make a backup of the Business Processes and delete them from the configuration before the installation.
- Make a backup of the Tango04 installation Folder.
- Export all the Reports Configuration from the application. Go to **Reports** > **Settings** > **Export All Data** (select all).
- Uninstall the previous version (except the Visual Message Center Dashboards).
- Copy the L2config.cfg file from the backup folder to %Program Files%\Tango04\ThinkServer (old installation folder).
- Before running the Event Manager installer, the old installation folder and the %Program Files%\Common Files\Tango04 folder must be renamed.
- Run the Event Manager installer.
- Restart the machine.
- Import all the Reports Configuration from the application. Go to **Reports** > **Settings** > **Import All Data (select all)**.

Upgrade since 4.0 versions

- Stop all Alignia services and IIS.
- Run the Event Manager installer.
- Restart the machine.

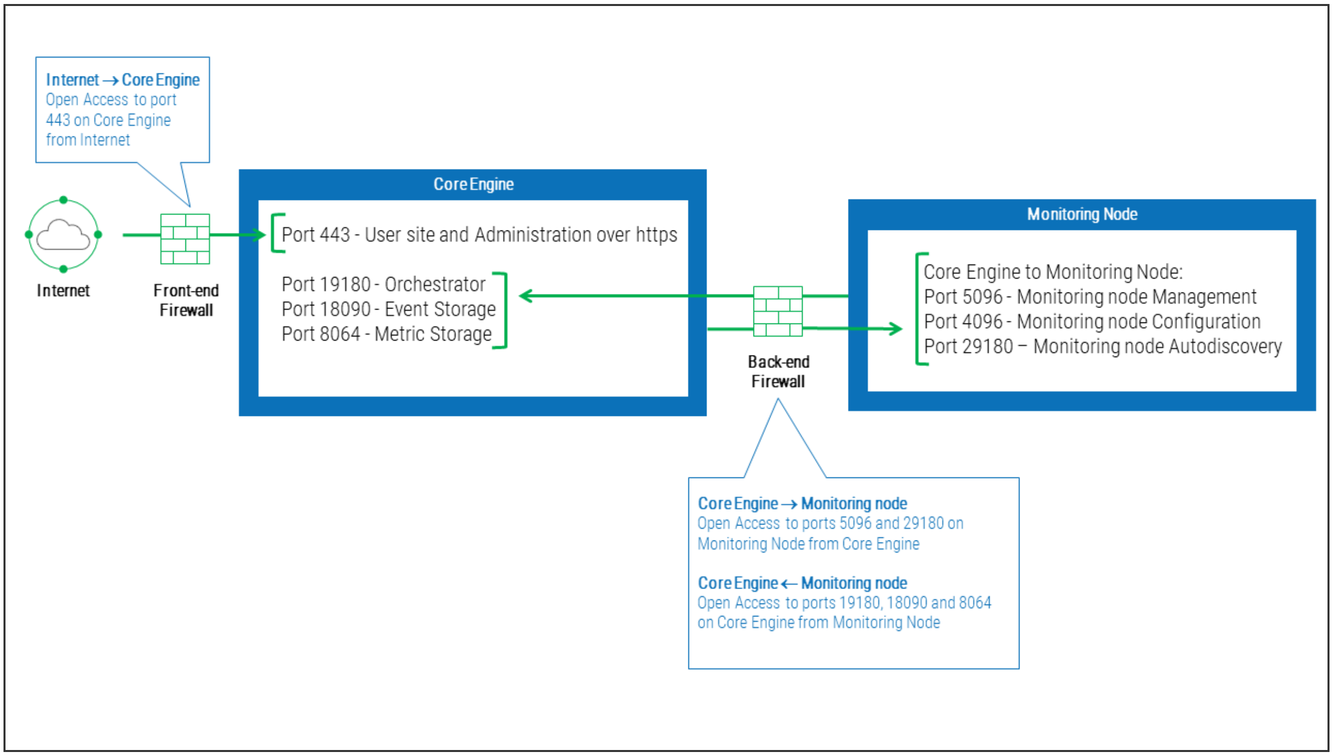
Migrating to a clean installation

To migrate existing data to a clean (fresh)installation of Event Manager please use the instructions in the Appendix of this guide.

Firewall Configuration

In order to ensure the correct functioning of the product, the front-end and back-end firewalls should be configured to open only specific port numbers required by the services.

The diagram below shows the firewall settings if the default port numbers were used in the Core Engine and Monitoring Node.



Internet → Core Engine
Open Access to port 443 on Core Engine from Internet

Core Engine → Monitoring node
Open Access to ports 5096 and 29180 on Monitoring Node from Core Engine

Core Engine ← Monitoring node
Open Access to ports 19180, 18090 and 8064 on Core Engine from Monitoring Node

Internet
Front-end Firewall
Core Engine
Port 443 - User site and Administration over https
Port 19180 - Orchestrator
Port 18090 - Event Storage
Port 8064 - Metric Storage
Back-end Firewall
Monitoring Node
Core Engine to Monitoring Node:
Port 5096 - Monitoring node Management
Port 4096 - Monitoring node Configuration
Port 29180 – Monitoring node Autodiscovery

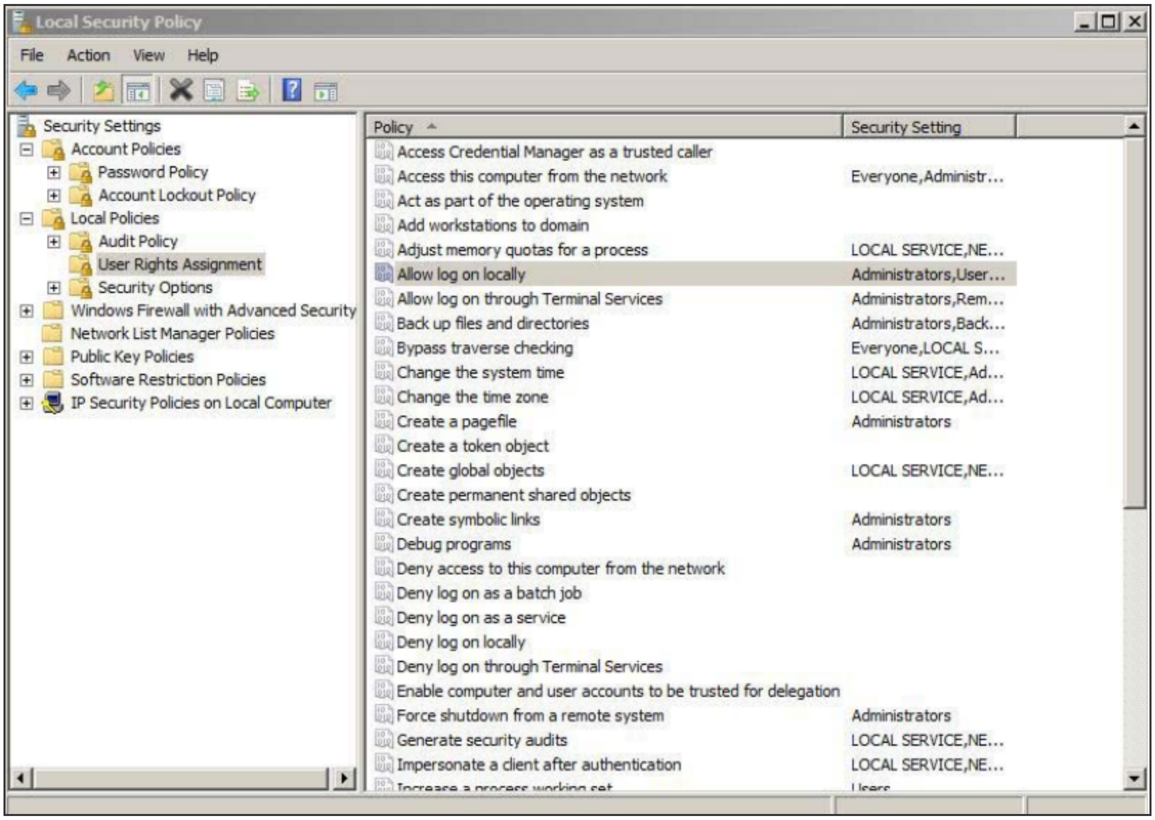
Security Administrator

Create a security administrator, and remember the credentials

A security administrator (SecAdm) is mandatory in AccessServer. The requirements user credentials are required to login and manage AccessServer and the SecAdmin is the only user allowed to register applications, therefore, if these details are lost it will be impossible to use AccessServer without resetting the SecAdm using the AS_SetSecAdm utility.

Requirements for the SecAdm user

The only requirement for the SecAdm user is that they can log on locally to the server where the user wants to install AccessServer and to be in the "Log on as a batch job" policy, any user type (normal user, local administrator or domain administrator) will be OK.



Policy	Security Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	Everyone,Administr...
Act as part of the operating system	
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NE...
Allow log on locally	Administrators,User...
Allow log on through Terminal Services	Administrators,Rem...
Back up files and directories	Administrators,Back...
Bypass traverse checking	Everyone,LOCAL S...
Change the system time	LOCAL SERVICE,Ad...
Change the time zone	LOCAL SERVICE,Ad...
Create a pagefile	Administrators
Create a token object	
Create global objects	LOCAL SERVICE,NE...
Create permanent shared objects	
Create symbolic links	Administrators
Debug programs	Administrators
Deny access to this computer from the network	
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	
Deny log on through Terminal Services	
Enable computer and user accounts to be trusted for delegation	
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE,NE...
Impersonate a client after authentication	LOCAL SERVICE,NE...
Increase a process working set	Users

> **NOTE:** Remember to use a Local user for Local Authentication, and a Domain user for Domain Authentication.

SecAdm user is changed at Windows / Active Directory

AccessServer does not store the SecAdm password (as this would be a security flaw) and therefore nothing will happen if the password is changed; however if the user who is assigned as the SecAdm for AccessServer is deleted from the system, the SecAdm user details will also be needed to be removed from AccessServer.

> **IMPORTANT:** Remember to delete the SecAdm from AccessServer and define a new SecAdmin before deleting the user who was previously set up as the SecAdm from the system.

Event Manager Product Download

Event Manager is supplied as a zip file. Download the latest product version from the following:

https://community.fortra.com/products-and-downloads/downloads

1. In the section marked **The following files are available for download**, look for the most recent version of the **Event Manager installer**.

> **NOTE:** A valid user id and password are required to access the Fortra Community Portal. Please sign in or register prior to downloading the required file.

2. Click **Download**. The file will automatically begin downloading to the default download folder specified in your browser. The file is very large so please be patient.
3. Navigate to the folder to where the Event Manager zip file was downloaded. Single right-click on this file and from the pop-up menu and select **Extract All**.
4. Specify the directory to which you want to extract the files and click **Extract**.

Starting the Installation

1. From the list of extracted files double-click **Setup.exe.** If not already installed, you are prompted to install the several components that Event Manager requires prior to continuing with the installation.

- **Microsoft Visual C++ 2008 SP1 Redistributable Package (x64)**
- **Microsoft Visual C++ 2010 SP1 Redistributable Package (X64)**
- **Microsoft Visual C++ 2015 Update 3 Redistributable Package (x86)**
- **Microsoft Visual C++ 2015 Update 3 Redistributable Package (x64)**
- **ODBC Driver 17 for SQL Server** (An error may be returned if this is already installed)

2. Click **Install** to continue. Once the installation of the required components is complete, the actual installation routine begins.
3. At the **Welcome to Install Wizard for HelpSystems Applications and Business Monitoring** dialog, click **Next** to continue and display the License Agreement. It is recommended that you read the full terms and conditions of the license agreement prior to continuing.
4. Select **I accept the terms in the license agreement** and then click **Next**.
5. Provide the user name and password for the Windows user that acts as the AccessServer Security Admin User (SecAdmin).
6. Click **Test** to verify that the user name and password combination are valid.
7. Click **Next** to continue.
8. You are now prompted to install one of the options:

   Default Setup
   Express Setup
   Advanced Setup

Default Installation

This installs the entire product locally using the default configuration values. An existing SQL Server database installation (local or remote) can be used. Databases and ODBC connections are automatically created.

1. From the Event Manager Setup dialog, select **Default Setup** and click **Next**. The installation routine begins.
2. Select the **Destination Folder** to which the installation will be completed. The default folder is **C:\Program Files (x86)\Help Systems**. Click **Change** to be able to specify an alternative folder.
3. On the **Database Server** dialog, enter the name of the server that will host the databases, for example, localhost or click Browse to navigate to the network path where the server where the database is installed.
4. Type the **Logon ID** needed to access the Database Server.
5. Type the **Password** associated with the entered user name.
6. Click **Test** to verify the connection. Once successful, click **Next** to continue. The databases are created.
7. When prompted, click **Install** to begin the installation. During this process various dialog windows open and close as various components are installed. There is no requirement for any user intervention during this time.
8. When prompted, enter the **Product key** that you have been sent in an email from Fortra. This can be left blank at this point and entered later if required.
9. Click **Use Free Plan** to continue. The program features, including reports, are now installed.
10. When prompted to configure the mail settings, click **Lets go**.
11. On the **Mail Settings** tab enter:

- The details of the **SMTP Server**.
- The **Default Email Address** from which alerts will be sent (For example, alerts@mymail.com)
- If the SMTP Server requires authentication enter a valid **User** and **Password** combination,

12. Click **Save and Exit**.
13. When prompted, click **Yes** to restart the HelpSystems services and click **OK** at the Successfully saved prompt.
14. Click **Restart Now** to restart the machine immediately. If you have any other windows or work open click **Restart Later** to give you opportunity to save your work before restarting.
15. Following the restart, open a web browser and type:
    https://localhost/HelpSystems

IMPORTANT: If you are using Internet Explorer, be sure that the site is not displayed using the "Compatibility View"

Express Installation

Express Installation is used exclusively for Trials and Free Versions of the Event Manager.

The Express Setup installs the entire product on a local server using the default configuration values. An instance of SQL Express is installed for the purpose of data storage. The SQL Server version is limited to a maximum number of 4 cores and a database size of 10GB.

1. From the Event Manager Setup dialog, select **Express Setup** and click **Next**. The installation routine begins. During this process various dialog windows open and close as various components are installed. There is no requirement for any user intervention during this time.
2. When prompted, enter the **Product key** that you have been sent in an email from Fortra. This can be left blank at this point and entered later if required.
3. Click **Use Free Plan** to continue. The program features, including reports, are now installed.
4. When prompted to configure the mail settings, click **Not right now** as these can be configured later.
5. Click **Restart Now** to restart the machine immediately. If you have any other windows or work open click **Restart Later** to give you opportunity to save your work before restarting.
6. Following the restart, open a web browser and type: **https://localhost/HelpSystems**

> IMPORTANT: If you are using Internet Explorer, be sure that the site is not displayed using the "Compatibility View"

Advanced Installation

The Advanced Installation routine allows you to customize which features are installed an what configuration values are used.

1. From the Event Manager Setup dialog, select **Advanced Setup** and click **Next**.

You can select to install one of the following:

- **Core Engine**: This is the core application that contains all the inventories, interfaces and functionality of the product.
- **Monitoring Node**: This is a collection engine, installed on a separate server (the same server or which the core engine is installed can also be used) that passes information back to the core application. Multiple instances of monitoring nodes can be installed on servers across your network enterprise.

Installing the Core Engine

This is the core application and should be installed once on a host server.

1. On the **Custom Setup** dialog, ensure that **Core Engine** is highlighted and click **Next**. A command window opens while the installation continues.
2. On the **Database Server** dialog, enter the name of the server that will host the databases, for example, localhost or click Browse to navigate to the network path where the server where the database is installed.
3. Type the **Logon ID** needed to access the Database Server.
4. Type the **Password** associated with the entered user name.
5. Click **Test** to verify the connection. Once successful, click **Next** to continue.
6. At the **Do you want to create new databases?** field, select **Yes** and click **Next**.
7. Click **Yes** to confirm the action There is a pause while the databases are created. Once created, click **Next** to continue.

8. On the **Database Server - Select Data Sources** display, leave all fields set to their defaults and click **Next**.
9. Click **Next** on the second page of **Database Server - Select Data Sources**.
10. On the **Web Site Settings** dialog, keep the **Website TCP Port** set to **443** and click **Next**.
11. Click **Install** to begin the installation.

> NOTE: Various windows open and close as part of the installation and the process can take several minutes to complete.

Once the installation process is complete you are prompted to select your data source.

Installing the Monitoring Node

See the Event Manager Configuration Guide for details on how to add a monitoring node.

Selecting the Data Sources

The next stage in the process is to select the ODBC data source to be used to store and manage AccessServer data.

> IMPORTANT: Only SQL Server database engine drivers are supported.

1. Ensure that **HS_APPSEC_Config** is highlighted and click **Next**.
2. Enter a valid **User Name** and associated **Password** combination which is used to access the **HS_APPSEC_Config** data source. Click **Next.**
3. Leave the **AccessServer Web Service Settings** at the default entries and click **Next**.
4. Enter the **User Name** (defaults to Administrator) and the associated **Password** required for the user that acts as the AccessServer Security Administrator (SecAdmin) user. Click **Next.**

5. At the **Ready!** dialog, click **Next** to register the Security Administrator profile to AccessServer.
6. When prompted, click **Finish** to complete the configuration.

Event Manager Product keys

At this point, the installation requests the entering of the Product Activation Key. If you have one, enter it here and click **Let's Go**.

Otherwise leave the value blank, click **Let's Go** and use the instructions provided in License Key Management to request and apply the key at a later stage.

Testing the Database Administrator Settings

On the **Database Administrator Settings** dialog, it is good practise to check that the Server and Web Application settings have been configured correctly.

1. To test the **AccessServer** configuration, click **Test Authentication**. The following message should be displayed. Click **OK** to close the dialog.
2. To test the connection to the machine where the HelpSystems web applications are installed, click **Test URL**. You should receive the same message as when you tested the AccessServer configuration. Click **OK** to close the dialog.

> WARNING: If one or both of these tests fail, there is a problem with your current configuration and Event Manager will not operate correctly. Either reconfigure the current settings, using the **Configure AccessServer** button or contact the technical support team for assistance.

3. Click **Save** to continue with these configuration settings.
4. When prompted, click **Yes** to restart the **Internet Information Services (IIS)**.
5. Click **OK** on the **Configuration Saved** dialog.
6. At the **Windows User Authentication** dialog, enter the **User** and **Password** combination required to access the **Database Administrator Settings** and click **Log In**.
7. After a short time, the **Database Administrator Settings** dialog is displayed with the databases pre-configured. Check that the configuration is as expected and then click ☒ **Exit**.
8. When prompted, click **Yes** to save the changes.
9. Restart IIS when prompted. Click **OK** to save the settings.
10. Click **Yes** to restart the HelpSystems services that are stopped.
11. On the **InstallShield Wizard Completed** dialog, click **Restart Now** to complete the installation.

Once the machine has restarted you can access Event Manager by typing:

http://{machine-name}/helpsystems

in your browser.

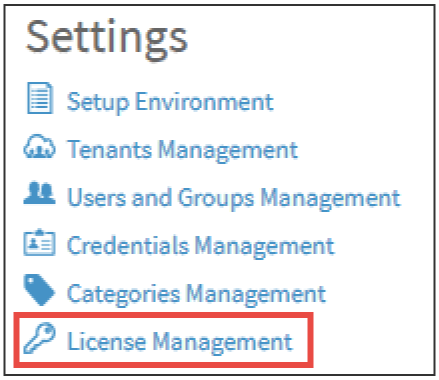
IMPORTANT: If you are using Internet Explorer, be sure that the site is not displayed using the "Compatibility View".

License Key Management

If you did not enter a license key at the point of installation, it is possible to enter it from within the Configuration Settings of Event Manager.

Getting there

1. Open a session of Event Manager and click **Configuration**.
2. From within the **Settings** section, click **License Management**.

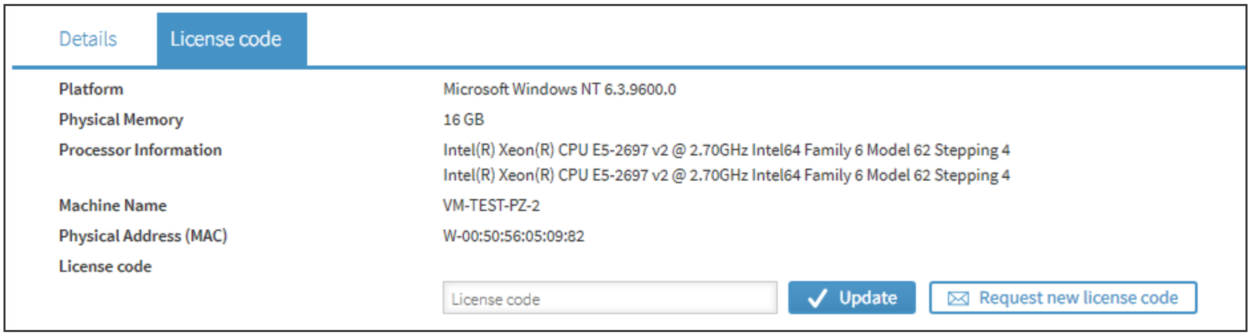


The **License Management** page is displayed with the **Details** tab open. This shows summary and detailed breakdown information of any license key that is already applied to this installation.

Entering a License Key

To apply a new license key:

1. On the **License Management** page, click the **License code** tab.



Platform: Microsoft Windows NT 6.3.9600.0
Physical Memory: 16 GB
Processor Information: Intel(R) Xeon(R) CPU E5-2697 v2 @ 2.70GHz Intel64 Family 6 Model 62 Stepping 4
Intel(R) Xeon(R) CPU E5-2697 v2 @ 2.70GHz Intel64 Family 6 Model 62 Stepping 4
Machine Name: VM-TEST-PZ-2
Physical Address (MAC): W-00:50:56:05:09:82
License code: License code

2. Type, or Copy and Paste the license key from the Fortra email, into the **License code** field and click **Update**.

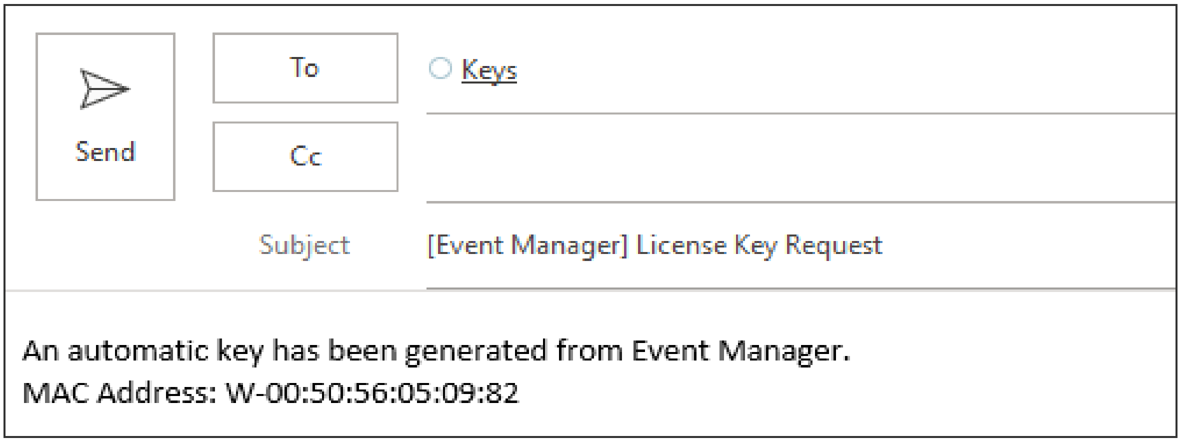
The License code is updated and the summary and breakdown information of the license is now available from the **Details** tab.

Requesting a License Key

To request a new license key:

1. On the **License Management** page, click the **License code** tab.
2. Click **Request new license code**.

An email is automatically opened, providing you have an associated email account, ready to send a request to keys@Fortra.com, for a license code specific to the machine from which the request was generated.



To: Keys
Subject: [Event Manager] License Key Request

An automatic key has been generated from Event Manager.
MAC Address: W-00:50:56:05:09:82

After You Are Done

Congratulations! Event Manager is now installed. Read the following for additional information and your next steps.

Database Maintenance

Database maintenance allows you to define the periods of time over which operational, security, system messages and performance data are kept. You can define settings for:

- **Short Term Database**: Keep details of events that are important to your current operational status
- **Historical Database**: Keeps details of events that have preciously been recorded and may be required for reporting purposes
- **Archive Database**: A repository of all previous events that is never deleted.

When database maintenance occurs, at a user-defined time and day, events are moved between the databases to ensure continuity and accuracy of information.

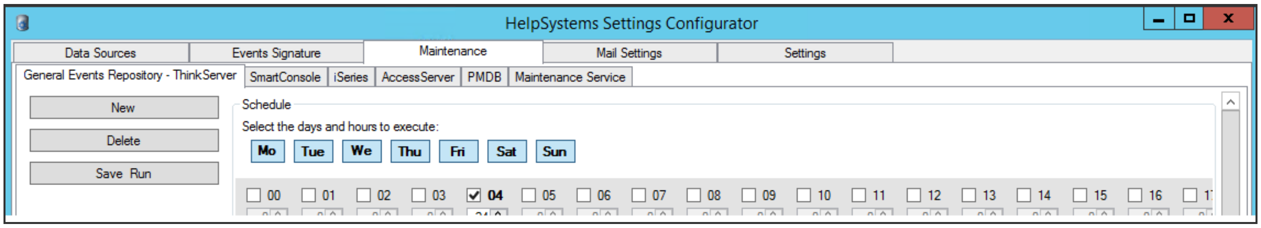
> **NOTE:** If no historical databases are configured the data is deleted from the short-term database after the defined time period, without any transfer or backup of data.

Database Maintenance Configuration

From the Windows Desktop use the **Administrator Search** facility to open the **HelpSystems Settings Configurator**.

When prompted, enter your **Windows User Authentication User Name and Password** combination. If prompted Click **Login**.

From the **HelpSystems Settings Configurator** dialog, click the **Maintenance** tab.



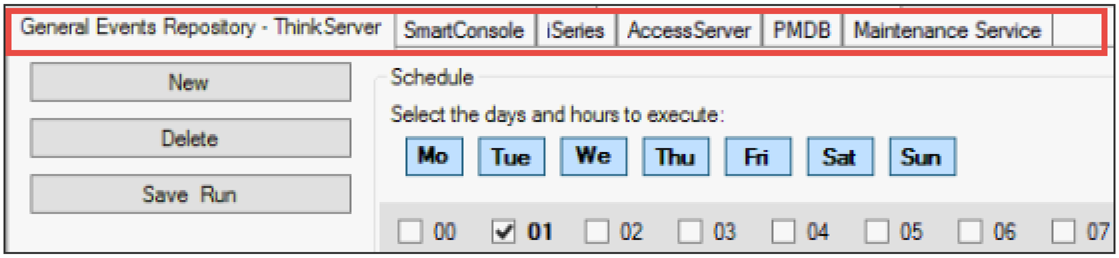
Setting the Schedule

The schedule controls the days and times at which the data for the selected event is moved between databases. This can be set to different days and times for different events. The following system defaults apply:

- **For ThinkServer Events and Security Data**: At 01.00 hours Sunday through Monday
- **For SmartConsole BSM**: At 03:00 hours Sunday through Monday
- **For SmartConsole Messages**: At 05:00 hours Sunday through Monday
- **Performance Management (PMDB)**: uses a set of retention policies (see Configuring the Performance Management Retention Levels for more information)

To change the existing schedule:

Use the **Database Administration** tabs to set the schedule for each element.



By default, all days are selected in the schedule.

1. Click on a day and the name changes from emboldened text to normal to signify that this day has been deselected. No movement of data will take place on this day.
2. Continue to remove or add days as required to complete the required day schedule.

By default, the time of data transfer is set to 01:00 hours. More than one time slot per day can be set for the transfer.

1. Click on a new time within the 24 hour clock at which you want the data transfer to start. A tick mark appears to denote its selection. Minutes for the selected hour can be set by using the selection box directly beneath the chosen hour(s).
2. Click in any existing time slots that you want to remove from the schedule. The tick mark is removed to indicate deselection.

Configuring the Event Manager Events Databases

1. From the **HelpSystems Settings Configurator** dialog, select the **General Events Repository - ThinkServer** tab.
2. In the left-hand panel of this display click **HS_APPSEC_Events**. The associated database settings are displayed in the main panel.

Short-term Database

The Short-term database was configured as part of the installation. The default time period for data retention in this database is 62 days.

1. If required, either overtype this entry or use the up/down arrows to change the current setting.
2. Click **Disable Data Deletion** if you want to permanently retain data in this database.

Historical Database

1. Click ... **Browse** next to the **DSN** parameter to browse for the required datasource via the **Select Data Source** dialog.
2. Select the **Machine Data Source** tab.
3. From the listed Data Sources, select **HS_APPSEC_Events_Hist** and click **OK**.
4. On the **SQL Server Login** dialog, enter the **User** and **Password** combination that was created in Selecting the Data Sources. Click **OK**. The Historical database has a default time period for data retention in this database of 365 days.
5. If required, either over-type this entry or use the up/down arrows to change the current setting.
6. Click **Disable Data Deletion** if you want to permanently retain data in this database.

Archive Database

1. Click on the **Search** icon next to the **DSN** parameter to browse for the required datasource via the **Select Data Source** dialog.
2. Select the **Machine Data Source** tab.
3. From the listed Data Sources, select **HS_APPSEC_Events_Arch** and click **OK**.
4. On the **SQL Server Login** dialog, enter the **User** and **Password** combination that was created in Selecting the Data Sources. Click **OK**. There is no time retention period for archive data. It is kept indefinitely.
5. Click **Save** to confirm the specified database settings.

> NOTE: Click **Save** and **Run** to save the current settings and immediately run a data transfer session between databases.

Configuring the Event Manager Security Databases

1. From the **HelpSystems Settings Configurator** dialog, select the **General Events Repository - ThinkServer** tab.

2. In the left-hand panel of this display click **HS_APPSEC_Security**. The associated database settings are displayed in the main panel.

Short-term Database

The Short-term database was configured as part of the installation. The default time period for data retention in this database is 62 days.

1. If required, either overtype this entry or use the up/down arrows to change the current setting.
2. Click **Disable Data Deletion** if you want to permanently retain data in this database.

Historical Database

Use the same procedure as when creating the HS_APPSEC_Events database but use the database **HS_APPSEC_Security_Hist** instead.

Archive Database

Use the same procedure as when creating the HS_APPSEC_Events database but use the database **HS_APPSEC_Security_Arch** instead.

Click **Save** to confirm the specified database settings.

Configuring the SmartConsole Database

There are two elements to consider when configuring the SmartConsole Database:

- **BSM**: This records details of asset status changes in the SmartConsole and the information is widely used to produce Service Level Agreement (SLA) reports.
- **Messages**: - This records details of messages generated by SmartConsole events.

Use the same procedures described when configuring the Event Manager Events Databases.

For the **SmartConsole BSM Short-term Database** use the **HS_APPSEC_ SmartConsole** data source.

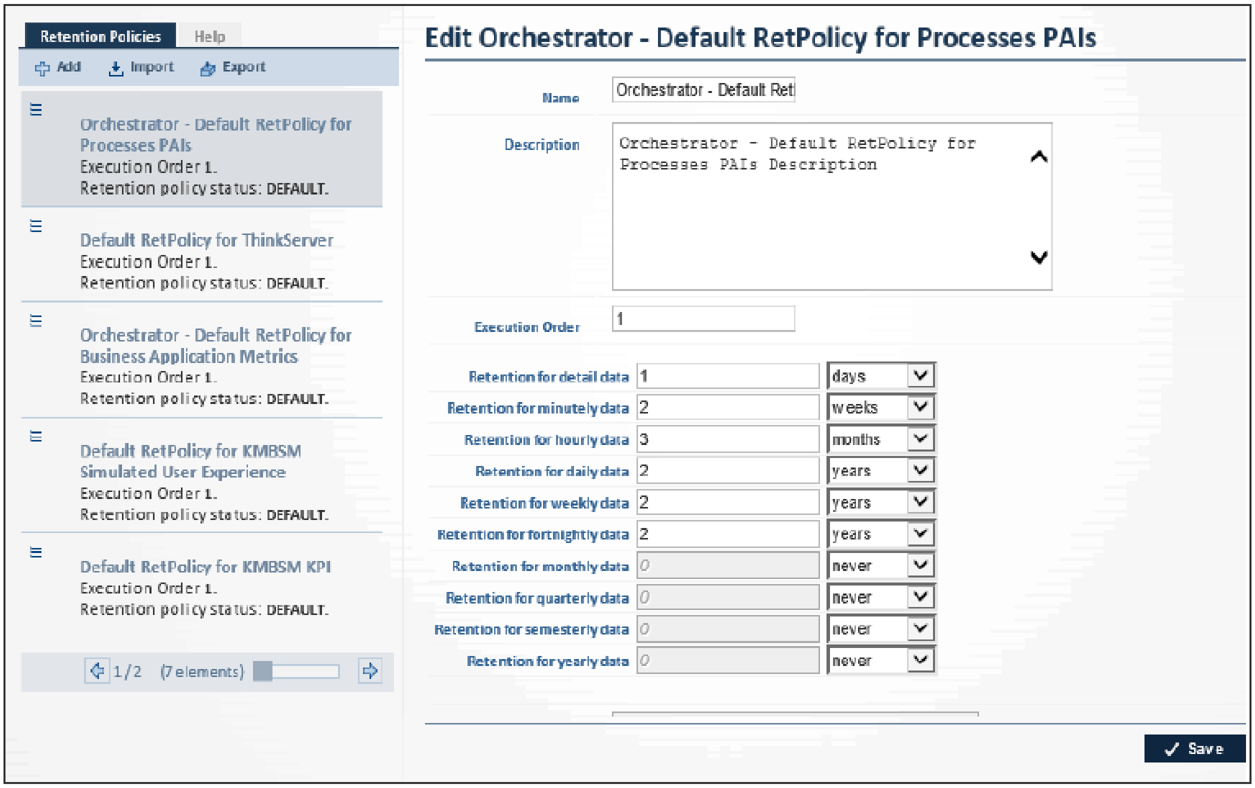
For the **SmartConsole BSM Historical Database** use the **HS_APPSEC_ SmartConsole_Hist** data source

For the **SmartConsole Messages Short-term Database** use the **HS_APPSEC_ SmartConsole** data source.

Configuring the Performance Management Retention Levels

The Performance Management Retention levels dictate the period of time over which specific performance records are retained. The retention levels are set by a specific areas in which performance is measured by Event Manager.

From the **HelpSystems Settings Configurator** dialog, select the **PMDB** tab.



Orchestrator - Default RetPolicy for Processes PAIs
Execution Order 1.
Retention policy status: DEFAULT.

Default RetPolicy for ThinkServer
Execution Order 1.
Retention policy status: DEFAULT.

Orchestrator - Default RetPolicy for Business Application Metrics
Execution Order 1.
Retention policy status: DEFAULT.

Default RetPolicy for KMBSM Simulated User Experience
Execution Order 1.
Retention policy status: DEFAULT.

Default RetPolicy for KMBSM KPI
Execution Order 1.
Retention policy status: DEFAULT.

1/2 (7 elements)

Edit Orchestrator - Default RetPolicy for Processes PAIs

Name	Orchestrator - Default Ret	
Description	Orchestrator - Default RetPolicy for Processes PAIs Description	
Execution Order	1	
Retention for detail data	1	days
Retention for minutely data	2	weeks
Retention for hourly data	3	months
Retention for daily data	2	years
Retention for weekly data	2	years
Retention for fortnightly data	2	years
Retention for monthly data	0	never
Retention for quarterly data	0	never
Retention for semesterly data	0	never
Retention for yearly data	0	never

The following retention policies are available:

- Orchestrator Default Retention Policy for Processes PAIs
- Default Retention Policy for ThinkServer
- Orchestrator Default Retention Policy for Business Application Metrics
- Default Retention Period for KMBSM Simulated User Experience
- Default Retention Period for KMBSM KPI

For each retention policy the time duration and period can be set for each of the following options and frequency level:

- Detail data
- Minutely data
- Hourly data
- Daily data
- Weekly data

- Fortnightly data
- Monthly data
- Quarterly data
- Semesterly data
- Yearly data

If required, you can change the length of time over which each individual option is retained by amending the number and time period settings.

If any of the settings are changed, click **Save** to confirm the changes.

Data Integrity Check Configuration

Data Integrity check runs during scheduled database maintenance process. See Database Maintenance Configuration for more details.

Disabling Data Integrity check

By default, Data Integrity checks are enabled automatically.

To disable the data integrity check:

1. From the **Windows Desktop** use the **Administrator Search** facility and type **HelpSystems Settings Configurator**.
2. When prompted, enter your **Windows User Authentication User Name and Password** combination. If prompted, click **Login**.
3. From the **HelpSystems Settings Configurator** dialog, click the **Events Signature** tab.
4. Set the **DSN** to **HS_APPSEC_Security (Default Security Datasource)**.
5. Enter a valid **User and Password** combination.

6. Once connected, clear the **Signed** checkbox and click on **Add** and then **Save** buttons to disable Data Integrity checks.

> TIP: You can re-enable Data Integrity checks whenever you want by following the above procedure and selecting the Signed checkbox then clicking on the Add and Save buttons.

Advanced Configuration

Data Integrity check includes checking for deleted or modified security events. All security events are checked for deletions, but depending on your amount of security events, not all can be checked daily looking for evidence of tampering.

By default, the product will check for a maximum number of 500,000 controlled events (randomly selected) and takes a maximum time of 20 minutes for every database (Short Term, Historical and Archive). At the first limit reached, whether time or events, the check process ends. If you have more events than are covered by either of these limits, then a tampered event may not be found immediately. But, as checked events are randomly selected each time, then Event Manager will eventually find the tampered event.

> NOTE: You can review the number of controlled events at each of your Event Manager databases (Short Term, Historical and Archive) by looking at number of records in table T4SECEVTCTL.

If you want to increase the number of events and time for integrity check you have to:

1. Edit file **T4BD.Config**. This is within the Event Manager\CommonFiles folder. You may want to change the following values:

   - **maxTamperedEventsToReview**: This is the value for the maximum number of controlled events checked every scheduled maintenance process

   - **maxSecondsToReviewTamperedEvents**: This is the maximum time allowed for the integrity check

- **maxSingleTamperedEventAlerts**: This is an additional parameter that refines how Data integrity check alerting works. Usually, for every tampered event found an alert is generated but if more than this number is found in an specific day, a final summary event with the additional number of tampered events is generated.

> NOTE: Once, you have changed these values you need to restart windows service **HelpSystems - Database Maintenance** in order for them to be applied.

Enabling Windows Integrated Authentication

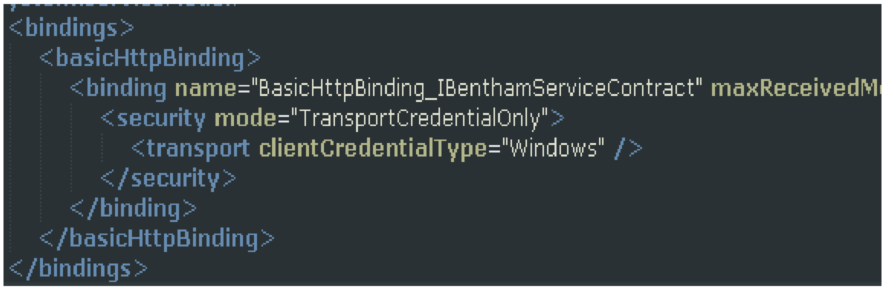
This section will explain how to enable Windows Integrated Authentication in VISUAL Message Center Web applications. This solution requires editing preferences in the following applications:

- Internet Information Services (IIS) Manager
- Web Browser

Event Manager

1. Go to %Program Files%/HelpSystems/Bentham/Bentham.Web and edit the web.config.file.
2. Add the following tag inside a binding tag with a name attribute equal to: BasicHttpBinding_IBenthamServiceContract:

   ```
   <Security mode=”TransportCredentialOnly”>
   <transport clientCredentialType=”Windows” />
   </security>
   ```

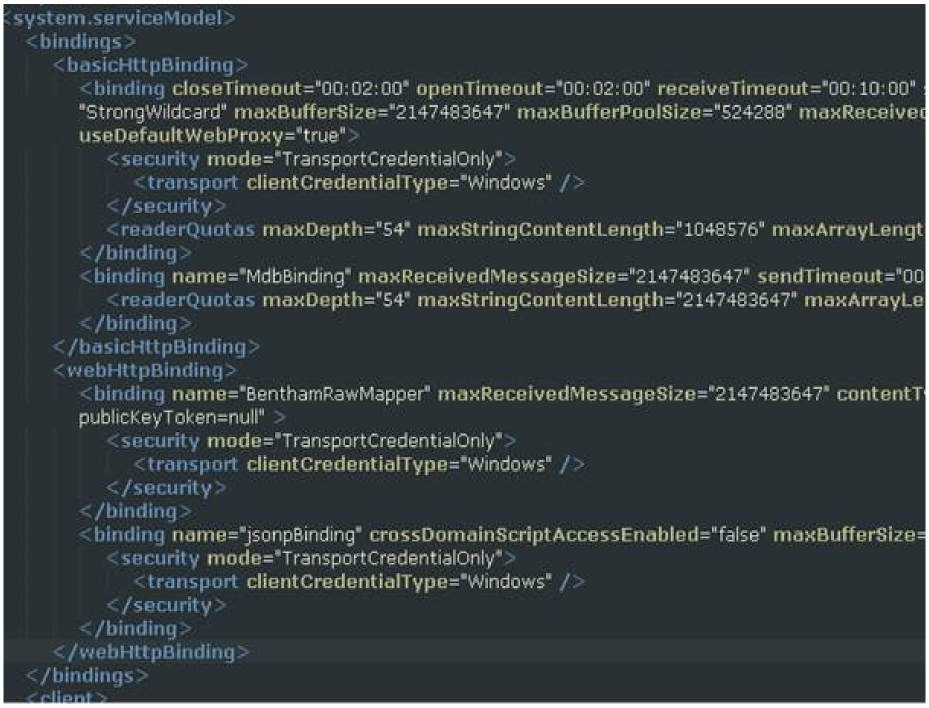


```
<bindings>
  <basicHttpBinding>
    <binding name="BasicHttpBinding_IBenthamServiceContract" maxReceivedM
      <security mode="TransportCredentialOnly">
        <transport clientCredentialType="Windows" />
      </security>
    </binding>
  </basicHttpBinding>
</bindings>
```

3. Go to %Program Files%/HelpSystems/Bentham/Bentham.Service and edit the web.config file:
4. Add the followiing tag inside a binding tag with a name attribute equal to: BenthamRawMapper, jsonpBinding and the binding tag without a name attribute to:

```
<security mode=”TransportCredentialOnly”>
<transport clientCredentialType=”Windows” />
</security>
```

5. Set the attribute **crossDomainScriptAccessEnabled** to **false** in the binding tag where the name attribute value is jsonpBinding.



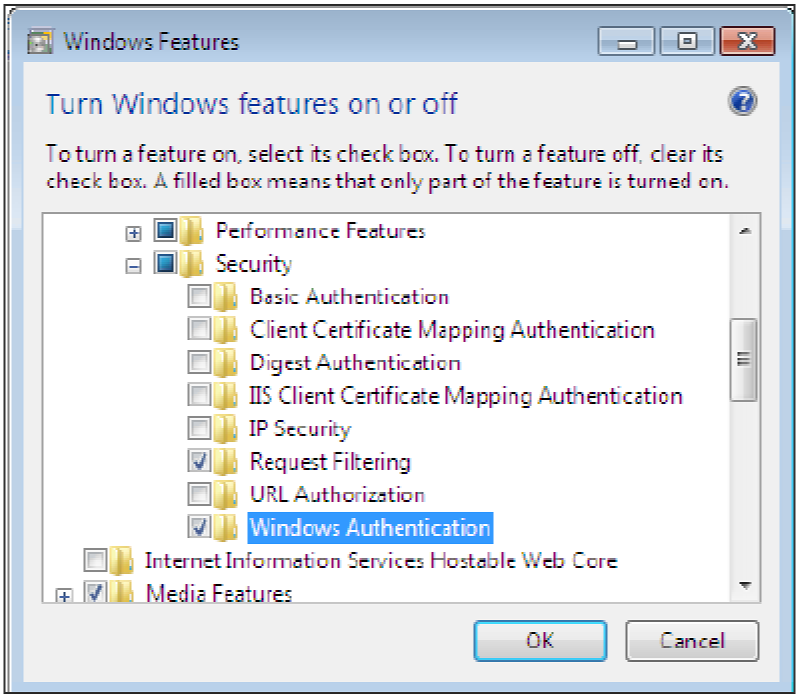
```
<system.serviceModel>
  <bindings>
    <basicHttpBinding>
      <binding closeTimeout="00:02:00" openTimeout="00:02:00" receiveTimeout="00:10:00"
      "StrongWildcard" maxBufferSize="2147483647" maxBufferPoolSize="524288" maxReceivec
      useDefaultWebProxy="true">
        <security mode="TransportCredentialOnly">
          <transport clientCredentialType="Windows" />
        </security>
        <readerQuotas maxDepth="54" maxStringContentLength="1048576" maxArrayLengt
      </binding>
      <binding name="MdbBinding" maxReceivedMessageSize="2147483647" sendTimeout="00
        <readerQuotas maxDepth="54" maxStringContentLength="2147483647" maxArrayLe
      </binding>
    </basicHttpBinding>
    <webHttpBinding>
      <binding name="BenthamRawMapper" maxReceivedMessageSize="2147483647" contentT
      publicKeyToken=null" >
        <security mode="TransportCredentialOnly">
          <transport clientCredentialType="Windows" />
        </security>
      </binding>
      <binding name="jsonpBinding" crossDomainScriptAccessEnabled="false" maxBufferSize=
        <security mode="TransportCredentialOnly">
          <transport clientCredentialType="Windows" />
        </security>
      </binding>
    </webHttpBinding>
  </bindings>
  <client>
```

Internet Information Server Settings

IIS 7.x

To enable Windows Integrated Authentication in IIS 7:

1. Open the **Control Panel**
2. Click **Turn Windows features on or off** under the Programs option to open the Windows Features window.
3. Navigate to Windows Authentication by expanding the following branches: **Internet Information Services** > **World Wide Web Services** > **Security** and select the **Windows Authentication** check box.



Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

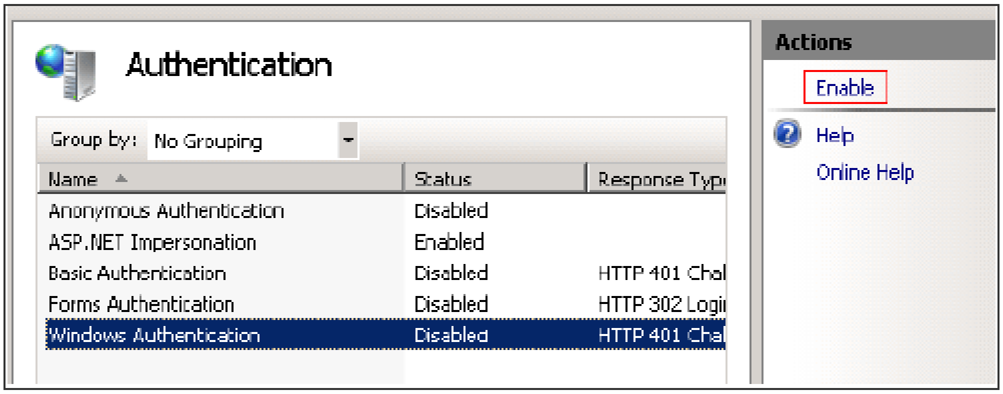
- ⊞ ■ Performance Features
- ⊟ ■ Security
  - □ Basic Authentication
  - □ Client Certificate Mapping Authentication
  - □ Digest Authentication
  - □ IIS Client Certificate Mapping Authentication
  - □ IP Security
  - ☑ Request Filtering
  - □ URL Authorization
  - ☑ Windows Authentication
- □ Internet Information Services Hostable Web Core
- ⊞ ☑ Media Features

4. Open the Internet Information Services Manager.

   Click the **Windows Start** button > **Administrative Tools** > **Internet Information Services (IIS) Manager**

5. Expand the **Sites** branch if it is collapsed and right-click on the Web Site for the *specific application* to open the Properties window and double-click **Authentication**.

6. Disable Anonymous Authentication and enable Windows Authentication by selecting them in list and clicking the *enable* or *disable* action in the Actions panel. This step should be undertaken for both the HelpSystems.Service and HelpSystems.Web sites.



Authentication

Group by: No Grouping

Name	Status	Response Typ
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Enabled	
Basic Authentication	Disabled	HTTP 401 Chal
Forms Authentication	Disabled	HTTP 302 Logi
Windows Authentication	Disabled	HTTP 401 Chal

Web Browser Settings

Firefox

To enable Windows Integrated Authentication in Firefox:

1. Open Firefox.
2. Type: about:config In the address bar.
3. Navigate to the network.automatic-ntlm-auth.trusted-uris preference in the Preference List.

   Right-click on the *Preference Name*, select Modify and type: http://serverName where serverName is the name of the server where *specific application* is installed.

TIP: Multiple sites can be added separated by a comma.

Internet Explorer

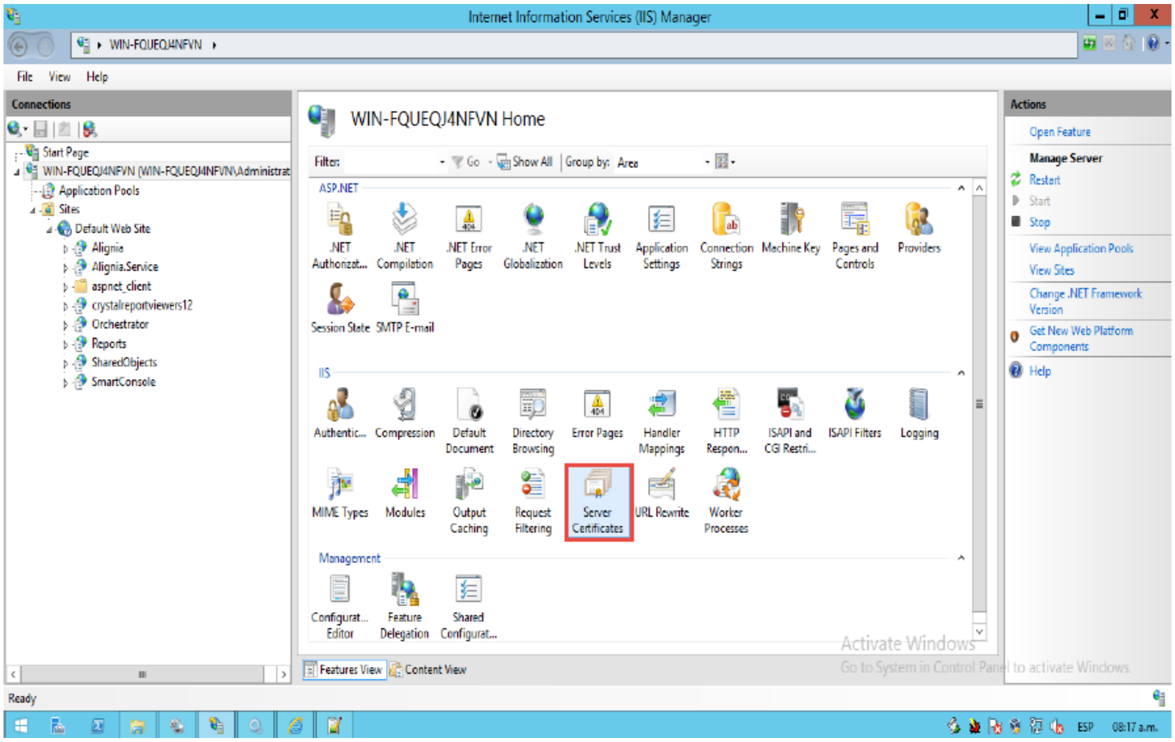
To enable Windows Integrated Authentication in Internet Explorer (V11 or higher):

1. Open Internet Explorer (v11 or higher)
2. Click **Tools** from the menu bar and select **Internet Options**.
3. Click the **Security** tab, select **Local intranet** and click the **Sites** button to add a new site.
4. In the Internet Options window click the **Advanced** tab and select the **Enable Integrated Windows Authentication** check box.
5. Click **OK** to exit and save settings.

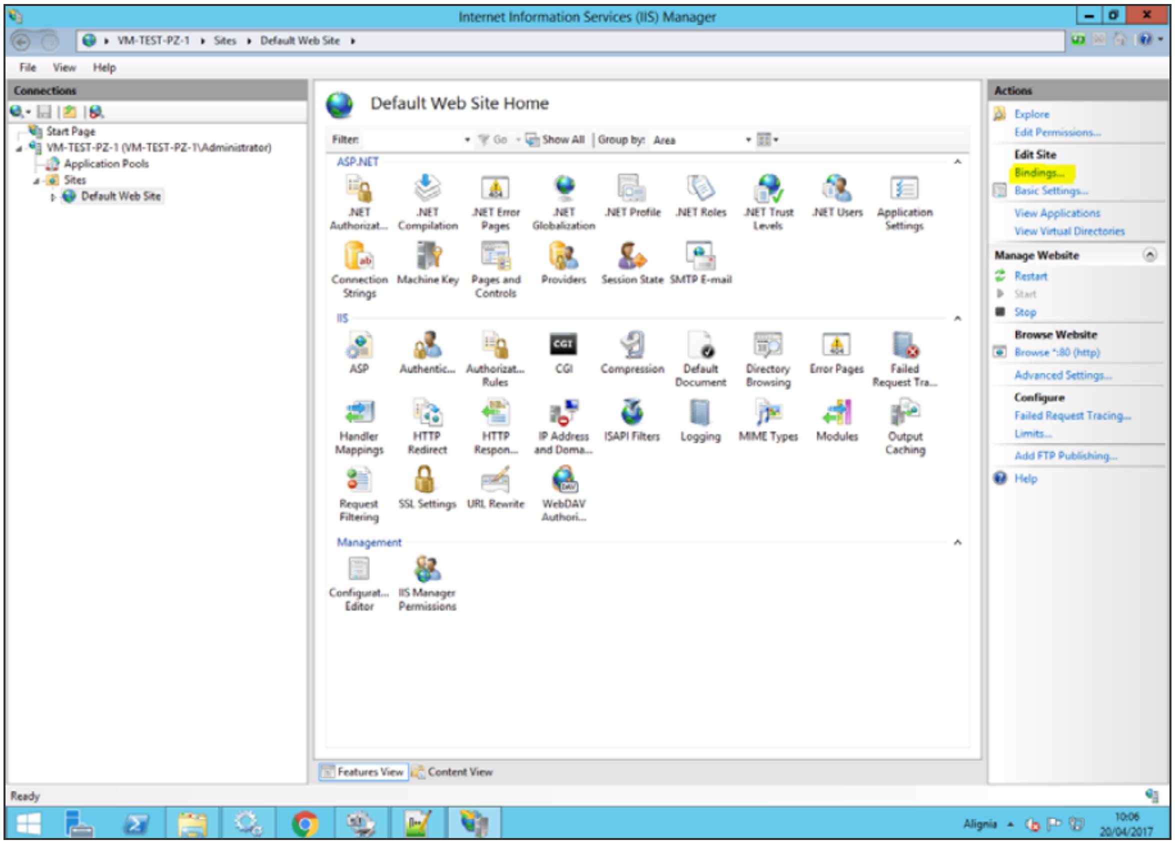
How to Configure HTTPS for Event Manager

Self-signed certificate creation on IIS

1. Access the **IIS Manager** program.
2. Open **Server Certificates.**



3. Click on **Create Self-Signed Certificate**.
4. Click on the **Default website** and select **Bindings**.



5. Add a new binding with the following credentials:

   Type: https
   Port: 443
   SSL Certificate: previously created

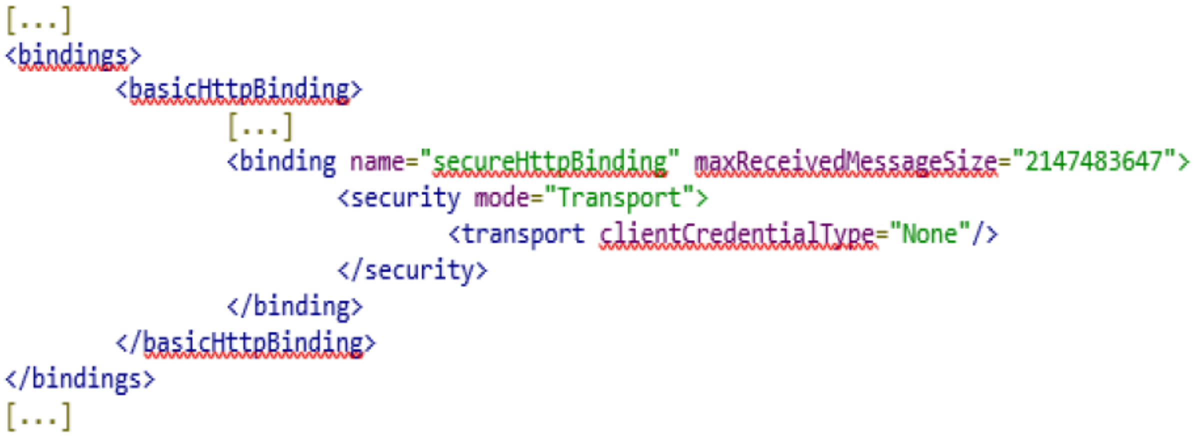
6. Remove **Port 80** binding.

Event Manager sites configuration

IMPORTANT: It is necessary to stop IIS before performing these changes.

Orchestrator Web

Modify the Orchestrator Web web.config file (backup the existing file) adding the following binding:

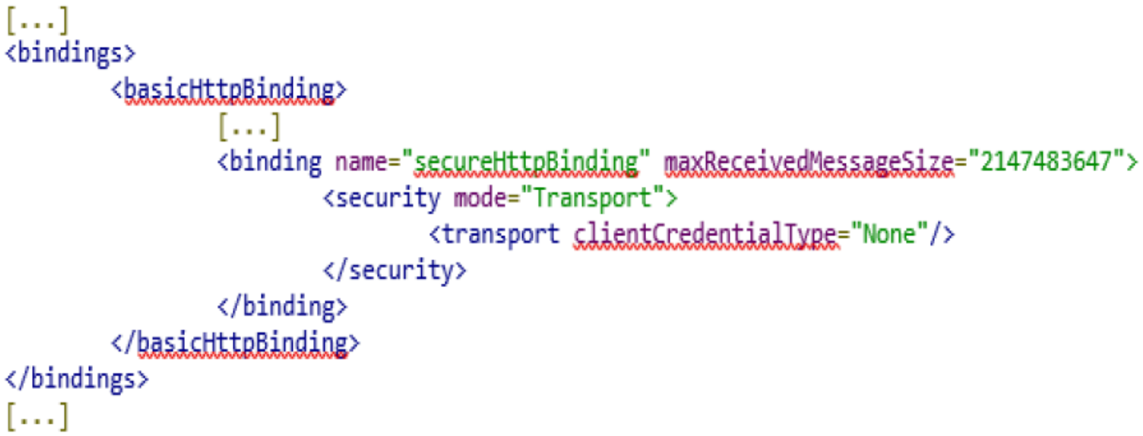


```
[...]
<bindings>
        <basicHttpBinding>
                [...]
                <binding name="secureHttpBinding" maxReceivedMessageSize="2147483647">
                        <security mode="Transport">
                                <transport clientCredentialType="None"/>
                        </security>
                </binding>
        </basicHttpBinding>
</bindings>
[...]
```

Bentham Service

Modify the Bentham.Service web.config file (backup the existing file)

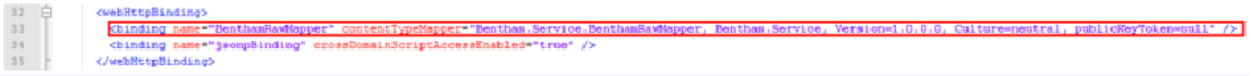
Add the following binding



```
[...]
<bindings>
        <basicHttpBinding>
                [...]
                <binding name="secureHttpBinding" maxReceivedMessageSize="2147483647">
                        <security mode="Transport">
                                <transport clientCredentialType="None"/>
                        </security>
                </binding>
        </basicHttpBinding>
</bindings>
[...]
```

Modify the BenthamRawMapper binding

Replace:



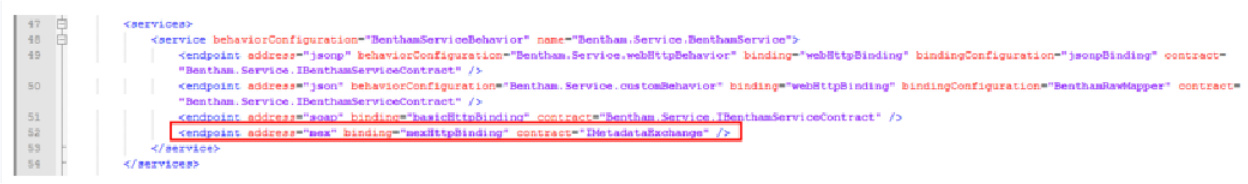
```
<webHttpBinding>
  <binding name="BenthamRawMapper" contentTypeMapper="Bentham.Service.BenthamRawMapper, Bentham.Service, Version=1.0.0.0, Culture=neutral, publicKeyToken=null" />
  <binding name="jsonpBinding" crossDomainScriptAccessEnabled="true" />
</webHttpBinding>
```

With:

```
<binding name="BenthamRawMapper" maxReceivedMessageSize="2147483647"
contentTypeMapper="Bentham.Service.BenthamRawMapper, Bentham.Service, Version=1.0.0.0,
Culture=neutral, publicKeyToken=null">
        <security mode="Transport">
                <transport clientCredentialType="None"/>
        </security>
</binding>
```

Modify the mexHttpBinding endpoint

Replace:



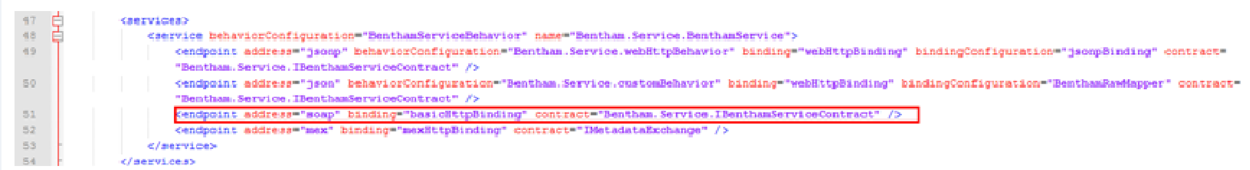
```
<services>
  <service behaviorConfiguration="BenthamServiceBehavior" name="Bentham.Service.BenthamService">
    <endpoint address="jsonp" behaviorConfiguration="Bentham.Service.webHttpBehavior" binding="webHttpBinding" bindingConfiguration="jsonpBinding" contract=
    "Bentham.Service.IBenthamServiceContract" />
    <endpoint address="json" behaviorConfiguration="Bentham.Service.customBehavior" binding="webHttpBinding" bindingConfiguration="BenthamRawMapper" contract=
    "Bentham.Service.IBenthamServiceContract" />
    <endpoint address="soap" binding="basicHttpBinding" contract="Bentham.Service.IBenthamServiceContract" />
    <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />
  </service>
</services>
```

With:

```
<endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange" />
```

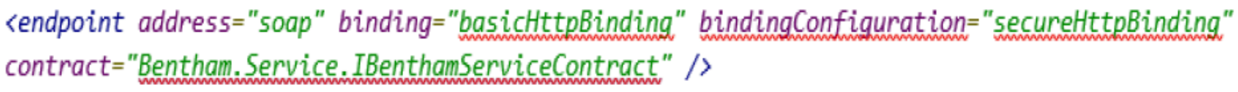
Modify the basicHttpBinding endpoint

Replace:



```
<services>
    <service behaviorConfiguration="BenthamServiceBehavior" name="Bentham.Service.BenthamService">
        <endpoint address="jsonp" behaviorConfiguration="Bentham.Service.webHttpBehavior" binding="webHttpBinding" bindingConfiguration="jsonpBinding" contract=
        "Bentham.Service.IBenthamServiceContract" />
        <endpoint address="json" behaviorConfiguration="Bentham.Service.customBehavior" binding="webHttpBinding" bindingConfiguration="BenthamRawMapper" contract=
        "Bentham.Service.IBenthamServiceContract" />
        <endpoint address="soap" binding="basicHttpBinding" contract="Bentham.Service.IBenthamServiceContract" />
        <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />
    </service>
</services>
```

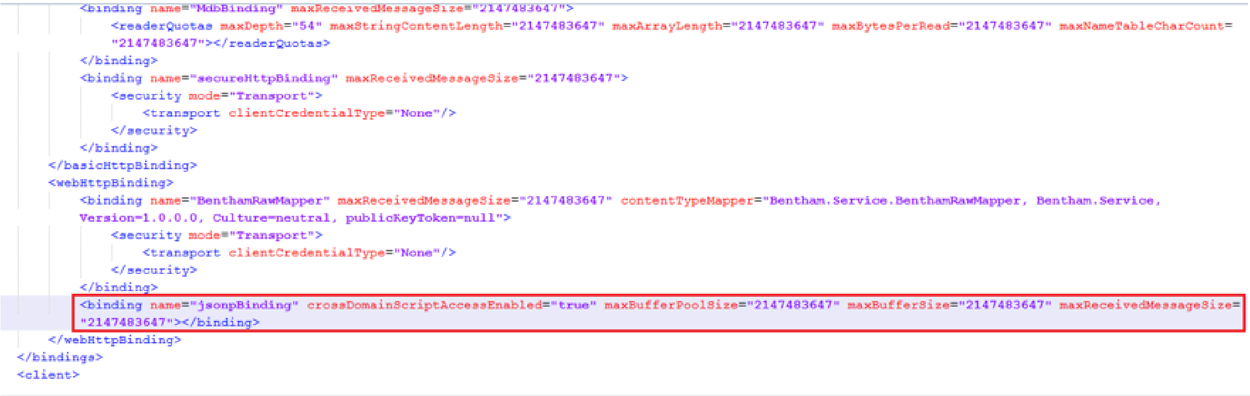
With:



```
<endpoint address="soap" binding="basicHttpBinding" bindingConfiguration="secureHttpBinding"
contract="Bentham.Service.IBenthamServiceContract" />
```

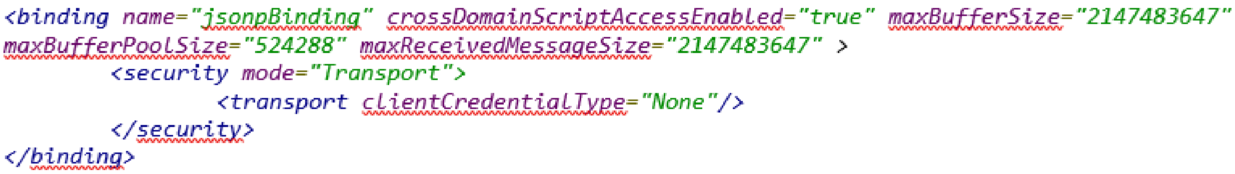
Modify the jsonpBinding

Replace:



```
            <binding name="MdbBinding" maxReceivedMessageSize="2147483647">
                <readerQuotas maxDepth="54" maxStringContentLength="2147483647" maxArrayLength="2147483647" maxBytesPerRead="2147483647" maxNameTableCharCount=
                "2147483647"></readerQuotas>
            </binding>
            <binding name="secureHttpBinding" maxReceivedMessageSize="2147483647">
                <security mode="Transport">
                    <transport clientCredentialType="None"/>
                </security>
            </binding>
        </basicHttpBinding>
        <webHttpBinding>
            <binding name="BenthamRawMapper" maxReceivedMessageSize="2147483647" contentTypeMapper="Bentham.Service.BenthamRawMapper, Bentham.Service,
            Version=1.0.0.0, Culture=neutral, publicKeyToken=null">
                <security mode="Transport">
                    <transport clientCredentialType="None"/>
                </security>
            </binding>
            <binding name="jsonpBinding" crossDomainScriptAccessEnabled="true" maxBufferPoolSize="2147483647" maxBufferSize="2147483647" maxReceivedMessageSize=
            "2147483647"></binding>
        </webHttpBinding>
    </bindings>
    <client>
```

With:



```
<binding name="jsonpBinding" crossDomainScriptAccessEnabled="true" maxBufferSize="2147483647"
maxBufferPoolSize="524288" maxReceivedMessageSize="2147483647" >
        <security mode="Transport">
                <transport clientCredentialType="None"/>
        </security>
</binding>
```

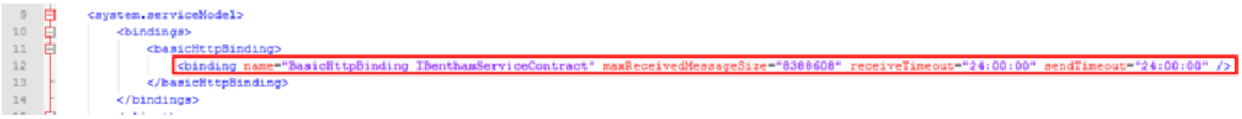
Bentham Web

Modify the Bentham.Web web.config file.

> IMPORTANT: Backup the existing file first.

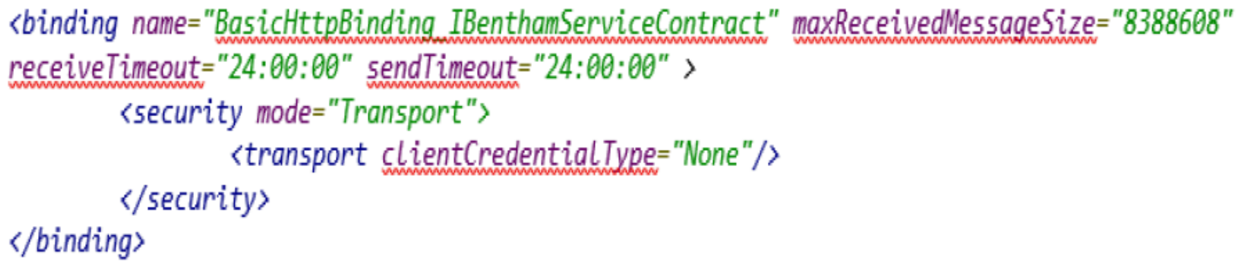
Modify the BasicHttpBinding_IBenthamServiceContract Binding

Replace:



```
<system.serviceModel>
    <bindings>
        <basicHttpBinding>
            <binding name="BasicHttpBinding_IBenthamServiceContract" maxReceivedMessageSize="8388608" receiveTimeout="24:00:00" sendTimeout="24:00:00" />
        </basicHttpBinding>
    </bindings>
```

With:

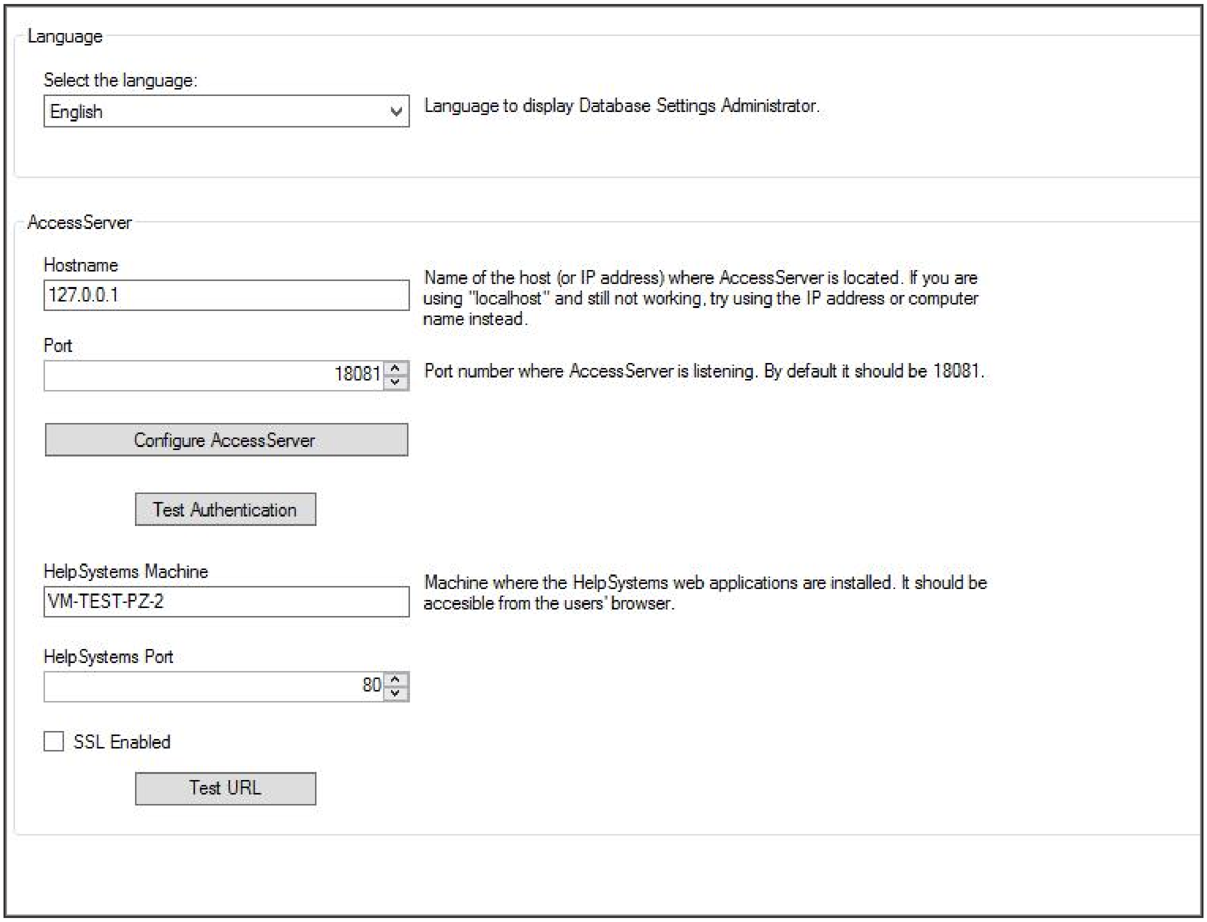


```
<binding name="BasicHttpBinding_IBenthamServiceContract" maxReceivedMessageSize="8388608"
receiveTimeout="24:00:00" sendTimeout="24:00:00" >
        <security mode="Transport">
                <transport clientCredentialType="None"/>
        </security>
</binding>
```

IMPORTANT: Restart IIS at this point.

Database Settings Administrator

1. Click on the **Settings** tab.
2. Set the **HelpSystems port** to **443** and enable SSL.



Language

Select the language: English

Language to display Database Settings Administrator.

AccessServer

Hostname: 127.0.0.1

Name of the host (or IP address) where AccessServer is located. If you are using "localhost" and still not working, try using the IP address or computer name instead.

Port: 18081

Port number where AccessServer is listening. By default it should be 18081.

HelpSystems Machine: VM-TEST-PZ-2

Machine where the HelpSystems web applications are installed. It should be accesible from the users' browser.

HelpSystems Port: 80

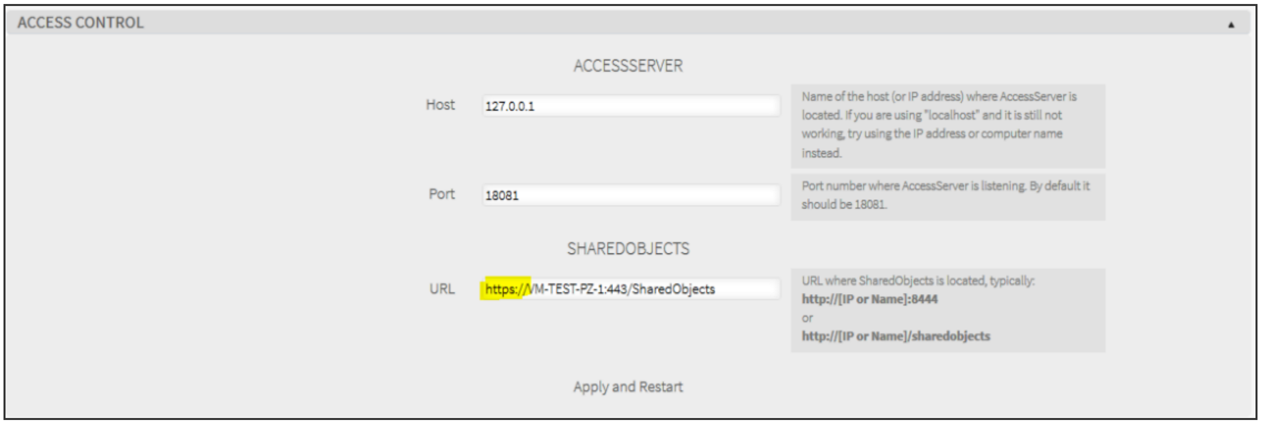
□ SSL Enabled

Browser

Perform the following actions in the browser:

- Clean the cache.
- Access the Event Manager website using the https protocol.
- Go to HelpSystems settings > Access control.

1. Change the SharedObjectURL to https protocol.



ACCESS CONTROL

ACCESSSERVER

Host: 127.0.0.1

Name of the host (or IP address) where AccessServer is located. If you are using "localhost" and it is still not working, try using the IP address or computer name instead.

Port: 18081

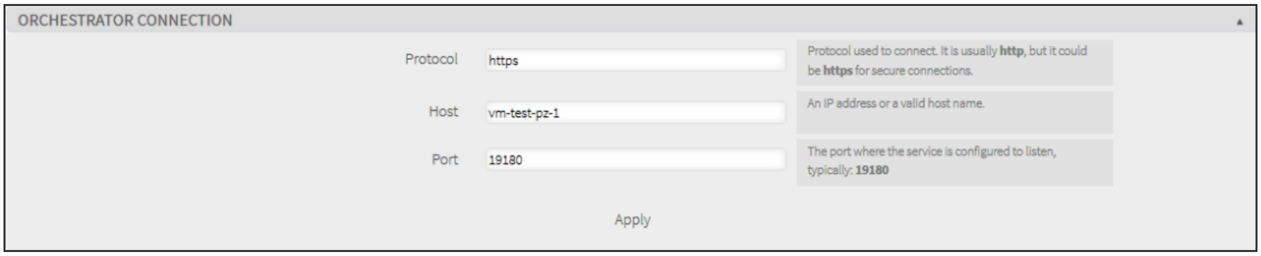
Port number where AccessServer is listening. By default it should be 18081.

SHAREDOBJECTS

URL: https://VM-TEST-PZ-1:443/SharedObjects

URL where SharedObjects is located, typically:
http://[IP or Name]:8444
or
http://[IP or Name]/sharedobjects

2. Change the Orchestrator connection to https.



ORCHESTRATOR CONNECTION

Protocol: https

Protocol used to connect. It is usually **http**, but it could be **https** for secure connections.

Host: vm-test-pz-1

An IP address or a valid host name.

Port: 19180

The port where the service is configured to listen, typically: **19180**

Installing and Accessing Insite

Insite gives you a single web interface where you can go to work with yourFortra products, all while using your browser on your desktop, or even on a mobile device, such as a phone or tablet.

After you download and install Insite on a Windows or Linux system, open the web interface in your favorite browser and point it at your Automate Enterprise server or IBM i system where you have the Fortra products installed. No updates are needed for the products you currently have running on those systems.

With Insite, you can access the following products (provided they're installed on the Automate Enterprise server or the IBM i):

- **Access Authenticator**: Use this to implement multi-factor authentication for user sign on.
- **Authority Broker**: Use this to allow System Administrators the ability to limit access to powerful user profiles and control access to sensitive databases and programs.
- **Automate Ops Console**: Use this to monitor and control your Automate Enterprise server resources, including workflows, tasks, processes, and agents.
- **Deployment Manager**: Use this to quickly and easily install, update, and license your Fortra products.
- **Insite Analytics**: Use this to display information from your installation of Insite Analytics in a web-based interface.
- **Password Self Help**: Use this to allow users to reset their own passwords without assistance from a help desk or system administrator.
- **Network Security**: Use this to monitor and control access to networked systems that are set up in Network Security.

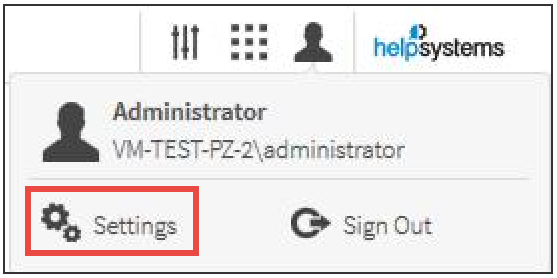
- **Robot Network**: Use this to monitor the performance and statuses of your IBM i partitions, and respond to statuses (Reply, Escalate, Assign, and etcetera).
- **Robot Schedule**: Use this to monitor and manage the jobs that are set up in Robot Schedule.
- **Vityl IT & Business Monitoring**: Use this to display information from your installation of Vityl IT & Business Monitoring in a web-based interface.
- **Webdocs for IBM i**: Use this to go paperless by automating business processes and digitally managing the entire life cycle of your business information.

You can download Insite from: https://www.fortra.com/products/it-operations-dashboard

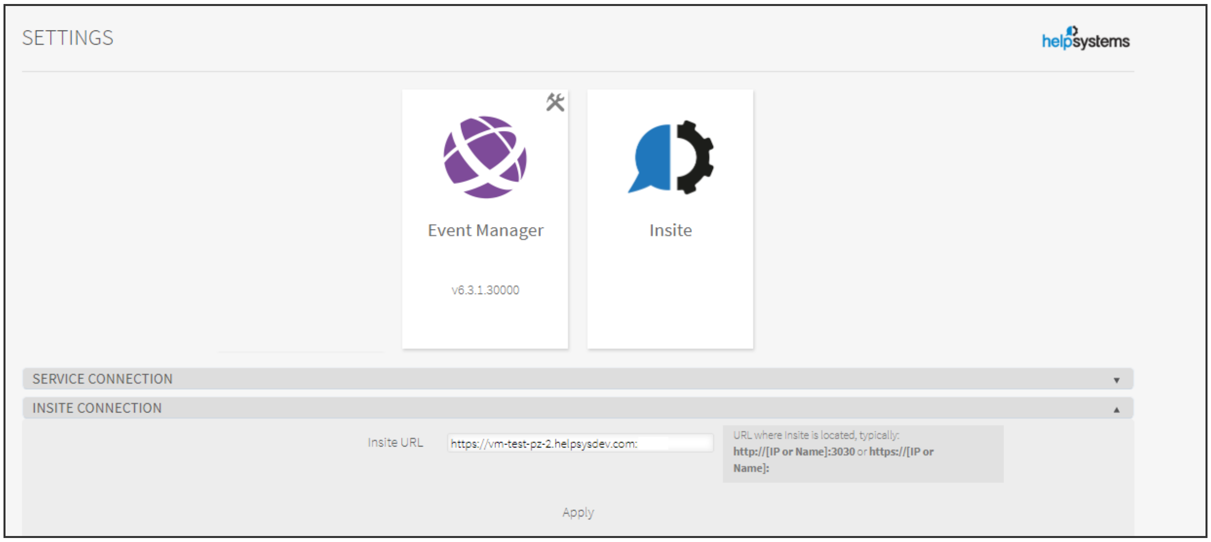
A link to access Insite already exists on the Event Manager Interface but it must be configured to point to the installation with which you are working.

> **NOTE:** You need Administrator permissions to be able to amend the following settings.

1. From the main interface page, click 👤 **User**.
2. From the drop-down menu options select **Settings**.



3. Expand the **Insite Connection** options.



SETTINGS

Event Manager

v6.3.1.30000

Insite

SERVICE CONNECTION ▾

INSITE CONNECTION ▴

Insite URL: https://vm-test-pz-2.helpsysdev.com:

URL where Insite is located, typically: **http://[IP or Name]:3030** or **https://[IP or Name]:**

Apply

4. Edit the **Insite URL** with the address at which your installation is running.
5. Click **Apply**.

The Insite button on the Event Manager interface is now configured to access your Insite installation.

Removing Event Manager

In the event you want to uninstall Event Manager you can remove it using the Windows Control Panel.

For a complete uninstall:

1. Remove Event Manager

> **NOTE:** Removing IIS and .Net is optional.

Appendix 1

How to avoid problems relating to Windows Updates during Installation

Windows Updates

Sometimes, during an installation or update of Event Manager there may be Windows Updates that can stop the installation. There are some steps that can be done to avoid this.

Before starting a new installation or a new update it is important to be sure that the system is up to date. This can be done with the Windows Update option in the system settings.

If there are pending updates, it is important to wait until all of them are installed. Sometimes they may need a shutdown before starting a new installation.

If the installation stops

Even with the system up to date prior to installation, there may be new windows features that need to be updated during the Event Manager installation. If that’s the case, the installation can be stopped.

If the installation process is taking more than one hour to complete it may mean that something is wrong or simply that the process has been stopped by the system to check for updates.

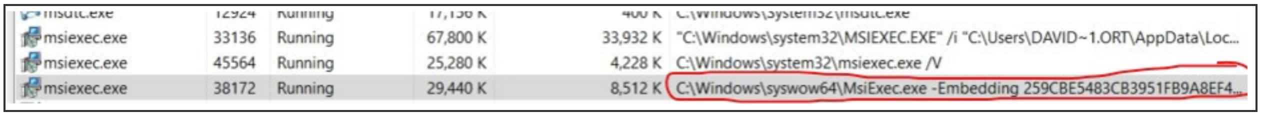
The following is a work around procedure to continue with the installation in these circumstances.

1. Review again and manually check for updates. In most of the cases this will resume the installation. This is because the system is always looking for new updates, and sometimes these take priority over an installation setup. Manually checking for updates will make sure that there are no more updates remaining. When this check is finished, the system will grant the priority again to the installation or update setup.
2. If after checking for new updates the installation setup remains stopped, check the installation log to see what the last step was performed by the installer.

   To locate the installation log, navigate to the TEMP folder, which can be found by entering "%temp%" on the address bar. The installation log is a file that starts with "MSI". If the last few lines seen on the log are something like:

   ```
   MSI (c) (AC:D4) [14:07:17:144]: Doing action: Script_BackupReportsFolder
   Action 14:07:17: Script_BackupReportsFolder.
   Action start 14:07:17: Script_BackupReportsFolder.
   ```

   It means that the installation setup is stopped by another installation process or by the system itself.
3. If that’s the case, check in the Task Manager for the other process. Find one that looks like this (note that the code may be different):

msdtc.exe	12924	Running	17,156 K	400 K	C:\Windows\System32\msdtc.exe
msiexec.exe	33136	Running	67,800 K	33,932 K	"C:\Windows\system32\MSIEXEC.EXE" /i "C:\Users\DAVID~1.ORT\AppData\Loc...
msiexec.exe	45564	Running	25,280 K	4,228 K	C:\Windows\system32\msiexec.exe /V
msiexec.exe	38172	Running	29,440 K	8,512 K	C:\Windows\syswow64\MsiExec.exe -Embedding 259CBE5483CB3951FB9A8EF4...

4. Now wait for that other process to finish, or kill it and resume it later.

After that the installation should continue.

Appendix 2

How to migrate existing data to a clean installation of Event Manager

Pre-Requirements

The user of the source machine database should be the same as the user of the target machine, while the databases from the source are copied to the new environment

If the databases remain at the source machine, they should be cloned. The installation process should be completed and any subsequent configurations made on these databases. Once the application is being used, checks can be undertaken to ensure that all works properly without the risk of losing any information. Once confirmed that all is OK, mapping can be changed to the original databases.

Before Installing

1. Clone the databases:
   a. **1st Case**: The migration is completed, meaning that both the configuration of the system and the databases are being moved to a new environment. This is when the databases have to be cloned.
   b. **2nd Case**: Databases remain at the origin and only the configuration is migrated. The databases must be cloned and renamed and the DSNs must be connected to the machine of origin and the new databases. This is important because it prevents that, in the event of a system failure, the production environment is not affected.
   c. BD Reports has to be created empty and then the DSN of Reports must be connected to the new database, not the old one. This is also the database where the configuration will be imported later.

2. In the database properties, change **Full Recovery Model** to **Simple**.
3. Copy the file structure of the source machine to the target machine, as shown in the following table. These files must be copied onto the same directory where the installation is taking place, which is by default **C:\Program Files (x86)\HelpSystems**.

Source	Target
ThinkServer	
ThinkServer\tsuuid	ThinkServer\tsuuid
ThinkServer \ RetentionPolicies.cfg	ThinkServer\RetentionPolicies.cfg
ThinkServer\l2config.cfg	ThinkServer\l2config-old.cfg (this file is copied and renamed)
ThinkServer\config\T04ConfigDatabase	ThinkServer\config\T04ConfigDatabase
ThinkServer\config\PMDBConfig.cfg	ThinkServer\config\PMDBConfig.cfg
ThinkServer\config\T4BDSR.cfg	ThinkServer\config\T4BDSR.cfg
ThinkServer\pythonlib\lib\t04Common\config\thinkserver.cfg	ThinkServer\pythonlib\lib\t04Common\config\thinkserver.cfg
ThinkServer\pythonlib\lib\t04Custom\	ThinkServer\pyhtonlib\lib\t04Custom\
ThinkServer\Autodiscovery\config\AdServer.cfg	ThinkServer\Autodiscovery\config\AdServer.cfg
ThinkServer\Persistence\	ThinkServer\Persistence
ThinkServer\pythonlib\lib\TSExtensions\WindwosBaseline\config\	ThinkServer\pythonlib\lib\TSExtensions\WindowsBaseline\config\
ThinkServer\pythonlib\lib\TSExtensions\WindowsBaseline\BaselineConfiguration.xml	ThinkServer\pythonlib\lib\TSExtensions\WindowsBaseline\BaselineConfiguration.xml
ThinkServer\ts_shared_referentials\Business Consumers\	ThinkServer\ts_shared_referentials\Business Consumers\

Source	Target
ThinkServer\ts_shared_referentials\Integrations	ThinkServer\ts_shared_referentials\Integrations
Orchestrator	
Orchestrator\Orchestrator Engine\config\	Orchestrator\Orchestrator Engine\config\
Orchestrator\Orchestrator Web\config\	Orchestrator\Orchestrator Web\config\
PMDB	
PMDB\config\AccessServer.pem	PMDB\config\AccessServer.pem
PMDB\config\pmdblog.properties	PMDB\config\pmdblog.properties
PMDB\config\StorageConfig	PMDB\config\StorageConfig
SmartConsole	
SmartConsole\Config\	SmartConsole\Config\
SmartConsole WebClient	
SmartConsole WebClient\config\hydra.config	SmartConsole WebClient\config\hydra.config
SharedObjects	
SharedObjects\calendars\	SharedObjects\calendars\
Scheduler	
Scheduler\scheduler.db	Scheduler\scheduler.db
AccessServer	
AccessServer\bin\config\LDAPProvider.cfg	AccessServer\bin\config\LDAPProvider.cfg
AccessServer\bin\config\AccessServer.cfg	AccessServer\bin\config\AccessServer.cfg
Reports	
Reports\datasources\system.xml	Reports\datasources\system.xml

4. Export the Reports configuration from the source. Go to **Settings/Export Reports Data**, and select **Full Export**.
5. Create the **DSN** corresponding to the **AccessServer** database with the same name as the old machine.

Installation

1. Run the latest version of the Event Manager installer.
2. Select **Advanced mode** in the installation wizard. Click **Next**. The "Select the program features" screen is displayed.
3. Verify that the installation path matches with the path where previously configuration files were copied. Click **Next**. The Security Administrator window is displayed.
4. Insert the password and verify if it is correct by clicking the **Test** button. If all is correct, the **Next** button is enabled. Click **Next**. The database connection window is displayed.
5. The Server, Login ID and Password fields are already filled. In the option "**Do you want the create new databases?**", select **No**. Test the connection and if it is successful, click on **Next**.
6. Now map the databases with DSNs. In versions prior to version 6, the databases were created manually, so their names can be different, they will be referred to by the module name to which they belong. The migrated system will need new databases creating, these are indicated in italics in the tables below.

Table 1 Mapping Databases VMC

DBs	DSNs
DB_AccessServer	HS_APPSEC_Config
DB_Thinkserver	HS_APPSEC_Events

DBs	DSNs
HS_APPSEC_Performance	HS_APPSEC_Performance
HS_APPSEC_Security	HS_APPSEC_Security
DB_Smartconsole	HS_APPSEC_SmartConsole
DB_Thinkserver_HST	HS_APPSEC_Events_Hist
DB_Thinkserver_ARC	HS_APPSEC_Arch
HS_APPSEC_Security_Hist	HS_APPSEC_Security_Hist
HS_APPSEC_Security_Arch	HS_APPSEC_Security_Arch
HS_APPSEC_SmartConsole_Hist	HS_APPSEC_SmartConsole_Hist
HS_APPSEC_Reports	HS_APPSEC_Reports

Table 2 Mapping Databases 302

DBs	DSNs
DB_AccessServer	HS_APPSEC_Config
DB_ThinkServer	HS_APPSEC_Events
DB_PMDB	HS_APPSEC_Performance
HS_APPSEC_Security	HS_APPSEC_Security
DB_SmartConsole	HS_APPSEC_SmartConsole
DB_Thinkserver_HST	HS_APPSEC_Events_Hist
HS_APPSEC_Events_Arch	HS_APPSEC_Events_Arch
HS_APPSEC_Security_Hist	HS_APPSEC_Security_Hist
HS_APPSEC_Security_Arch	HS_APPSEC_Security_Arch
HS_APPSEC_SmartConsole_Hist	HS_APPSEC_SmartConsole_Hist
HS_APPSEC_Reports	HS_APPSEC_Reports

Table 3 Mapping Databases 405 and 505

DBs	DSNs
DB_AccessServer	HS_APPSEC_Config
DB_ThinkServer	HS_APPSEC_Events
DB_PMDB	HS_APPSEC_Performance
DB_Security	HS_APPSEC_Security
DB_SmartConsole	HS_APPSEC_SmartConsole
DB_Thinkserver_HST	HS_APPSEC_Events_Hist
DB_Thinkserver_Arch	HS_APPSEC_Events_Arch
DB_Security_Hist	HS_APPSEC_Security_Hist
DB_Security_Arch	HS_APPSEC_Security_Arch
HS_APPSEC_SmartConsole_Hist	HS_APPSEC_SmartConsole_Hist
HS_APPSEC_Reports	HS_APPSEC_Reports

Table 4 Mapping Databases 6.2

DBs	DSNs
HS_APPSEC_Config	HS_APPSEC_Config
HS_APPSEC_Events	HS_APPSEC_Events
HS_APPSEC_Performance	HS_APPSEC_Performance
HS_APPSEC_Security	HS_APPSEC_Security
HS_APPSEC_SmartConsole	HS_APPSEC_SmartConsole
HS_APPSEC_Events_Hist	HS_APPSEC_Events_Hist
HP_APPSEC_Events_Arch	HS_APPSEC_Events_Arch
HS_APPSEC_Security_Hist	HS_APPSEC_Security_Hist

DBs	DSNs
HS_APPSEC_Security_Arch	HS_APPSEC_Security_Arch
HS_APPSEC_SmartConsole_Hist	HS_APPSEC_SmartConsole_Hist
HS_APPSEC_Config	HS_APPSEC_Reports

7. Click **Next**. The port configuration screen is displayed, with a default setting of 443.
8. Click **Next**. The installation home screen is displayed.
9. Click on **Install**. Once the licensing screen is displayed:
   a. Overwrite **AccessServer.cfg** file in the path **C:\Program Files (x86) \Help Systems\AccessServer\bin\config** for the same file located in the source machine. Restart the AccessServer service for this change become to be effective.
   b. Then run the **AS_SetSecAdm.exe file** located in **C:\Program Files (x86)\Help Systems\AccessServer\bin**. This action allows insert the new SecAdmin user, this user should be match with the user inserted in step 4.
   c. In the target machine, overwrite the **system.xml** file that was copied from the source machine prior to the starting the installation. This step is required as this file is deleted during the installation process.
10. When prompted, enter the Event Manager licenses or use the Free Plan.
11. The First Run of Reports is now run.
12. The Database Setting Administrator is run. For versions prior to version 6, excluding VMC:

    The Orchestrator and Bentham DSNs are changed and the following DSNs are created and mapped to the corresponding databases:

DBs	DSNs
DB_ORCHESTRATOR	DB_ORCHESTRATOR

DBs	DSNs
DB_BENTHAM	DB_BENTHAM

Then, the following tabs are modified:

- Tab Orchestrator: HS_APPSEC_Config -> DB_ORCHESTRATOR
- Tab Bentham: HS_APPSEC_Config -> DB_BENTHAM

The Maintenance DSNs are modified manually for matching the configuration of the source machine.

13. The changes are saved.
14. Subsequently, the final window of the installer is displayed and the machine is restarted.

Post Installation

1. Verify that all application services are started.
2. For versions lower than version 6:
    a. Copy System.NLK file from the source located at:
        - **VMC**: C:\Program Files (x86)\Common\Tango04
        - **302**: C:\Program Files (x86)\Common\Tango04
        - **405**: C:\Program Files (x86)\Alignia\CommonFiles
        - **505**: C:\Program Files (x86)\Alignia\CommonFiles

    b. Copy on the target machine, path **C:\Program Files (x86)|Help Systems\CommonFiles**
3. Stop the service of SmartConsole and copy old **GUID** in the **kernel.cfg** file located in **C:\Program Files (x86) \Help Systems\SmartConsole\Config**, because it is removed during the installation.

4. For versions prior to version 6, if the operating system on which it is installed is newer than Windows Server 2012, run the console as an application by accessing the path **C:\Program Files (x86) \Help Systems\SmartConsole\SmartConsole.exe**. If the operating system version is lower than Windows Server 2016, access to the console can be made through an interactive session, by starting the SmartConsole service.
5. Access **Settings (https://localhost/helpsystems/settings)** and verify in the Orchestrator connection that the machine name is correct and no longer references the old machine.
6. Start Orchestrator Web and in **Management/Environment/SmartConsole**, select the action "**Edit this SmartConsole connection parameters and variables**". If necessary, modify the Host Name field by accessing the Orchestrator Database and executing the following query:

   UPDATE [BD ORCHESTRATOR]. [DBO]. [MDB_SmartConsole] SET HOSTNAME = 'NewMachineName' WHERE SMARTCONSOLEUUID = 'uuid of the old machine'
7. Then, access **IIS** and restart the **Application Pool SmartConsole**. Refresh the page that had been previously accessed and verify that the Host Name field has changed. Check the connection.
8. Modify the **Web Client URL** with the correct URL: **https://hostname/SmartConsole/**. Verify that the user can be recorded satisfactorily.
9. Update the URLs of **Reports**, **Alignia Web** and **Orchestrator Web** with the name of the current machine. Save the changes.
10. In Management, access the **PMDB** configuration. Select the **Edit** action and in the **Host Name** field, change the old name for the current name. Save the configuration and verify that connection is successful.
11. If you are migrating from **VMC**, navigate to:

    C:\Program Files (x86)\Help Systems\ThinkServer\logs\LocalLog.log file.

If there is a message saying: "TS Manager: The new ThinkServer can't work with old configuration files. You need to execute the migration utility tool to migrate existing configuration before being able to start ThinkServer!" ... use the following tool:

C:\Program Files (x86)\Help Systems\ThinkServer\ConfigMigrator.exe to execute the migration and then restart the "HelpSystems - ThinkServer" windows service.

12. Go to the **L2Config.cfg** file located in **C:\Program Files (x86)\Help Systems\ThinkServer**, and ensure the **TSUuidToUseForMdbServer** field is empty. This is so that ThinkServer does not reference the old instance of Orchestrator. Restart the ThinkServer service.

> NOTE: If this field is completed with the same ID, it indicates that the Orchestrator version on the source machine is the same as on the target machine. If not, this field is filled with the ID of the current version of Orchestrator.

13. Check in **Orchestrator/Management/Status** that everything is correct.

> NOTE: If the console takes time to update, accessed the Orchestrator Engine logs folder and check if a file exists that indicates the action being performed during synchronization, for example: **SmChangeHosts_20191127090926.syn**. Once this file disappears, check to see if the console has been updated. If it is not updated, it is because it the Business View tree was updated before the monitors. You must restart the ThinkServer. Once done, the console tree must be updated with the health corresponding to the monitors.

14. The calendars configuration, copied before installing, is overwritten during the installation process. If the calendars still exist in the origin, overwrite the **Calendar** folder in **C:\Program Files (x86)\Help Systems\SharedObjects** with the files of this same folder located on the source machine.

a. On **IIS**, restart the **SharedObjects Application Pool**

b. Restart the **Orchestrator service**

c. Restart the **SmartConsole service** to synchronize the Business View tree with the calendars added

15. If a different configuration exists on the source machine in terms of the number of running processes (file **C:\Program Files (x86) \Help Systems\ThinkServer\config\I2ProcessConfig.cfg**), modify this file on the target machine. Restart the **ThinkServer service**.
16. Check that the **Online Business Services** and **Business Processe**s have been migrated correctly, as well as, the security assets and controls (Event Manager).

17. To import services in versions prior to version 5:
    a. Access the old OBS configurator (**C:\Program Files (x86)\Help Systems\Online Business\Designer\KMBSMDataBuider.exe**) and connect to the cloned OBS Database. Export the services.
    b. Import services from the web in the new configurator.
18. Access Reports. Import the previously exported xml file by using **Settings/Import Reports Data** and select **Full Import**. Modify the corresponding configuration fields and click on **Save**. Ensure that the DSN and Host selected is correct, pointing to the new database that was previously created.

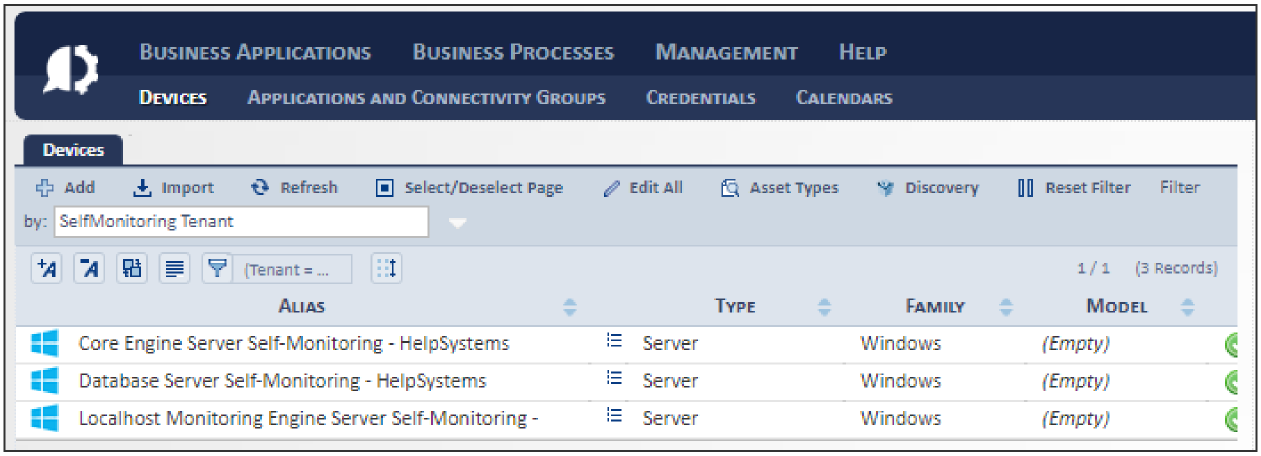
Checking that the application works correctly

1. Verify that the Events and Security databases have been upgraded to the latest version in the table T4Settings (version 30, in this case).
2. Verify that the SmartConsole tree is correct.
3. Access BA Home and verify that the assets are displayed correctly.
4. Access ThinkServer Configurator and verify that the monitors have been migrated and have the correct status.
5. Access Reports (Check that the configuration has been imported correctly and modify, if necessary, the data sources in Management).

Amending the Self-monitoring Server details

Changing the IP Address

1. Open your instance of Event Manager.
2. From the **Settings** menu click **Self Monitoring Advanced Configuration**. A session of Orchestrator is opened.
3. In the **Devices** section, Filter by **SelfMonitoring Tenant** as in the screen shot below:

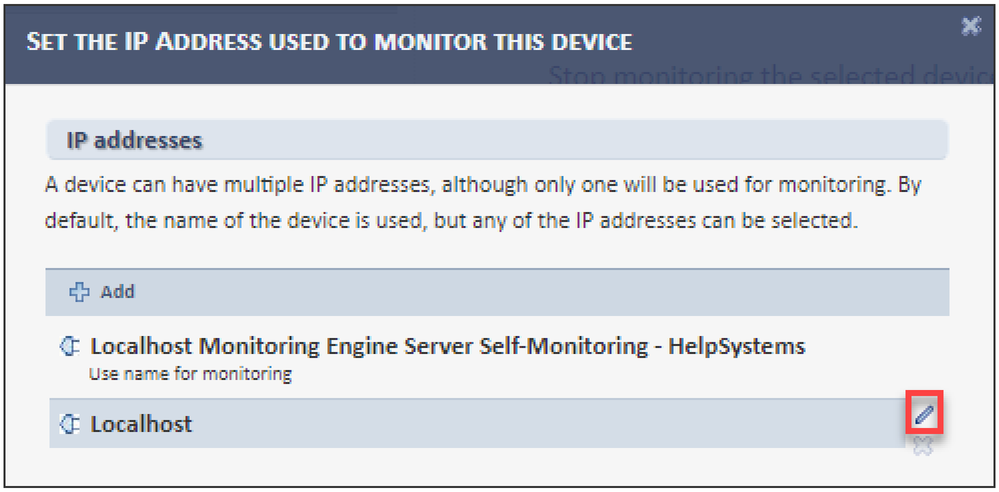


Alias	Type	Family	Model
Core Engine Server Self-Monitoring - HelpSystems	Server	Windows	*(Empty)*
Database Server Self-Monitoring - HelpSystems	Server	Windows	*(Empty)*
Localhost Monitoring Engine Server Self-Monitoring -	Server	Windows	*(Empty)*

4. Select the **Localhost Monitoring Engine Server Self-Monitoring - HelpSystems** entry so that it is highlighted.

5. From the **Asset Actions** menu, click **Set the IP Address used to monitor this device**.

6. In the **Set The IP Address Used To Monitor This Device** dialog, hover over and then click on the **Edit** icon to the right of the Local Host Entry.


Set the IP Address used to monitor this device
Stop monitoring the selected device
Add

IP addresses

A device can have multiple IP addresses, although only one will be used for monitoring. By default, the name of the device is used, but any of the IP addresses can be selected.

Localhost Monitoring Engine Server Self-Monitoring - HelpSystems
Use name for monitoring

Localhost

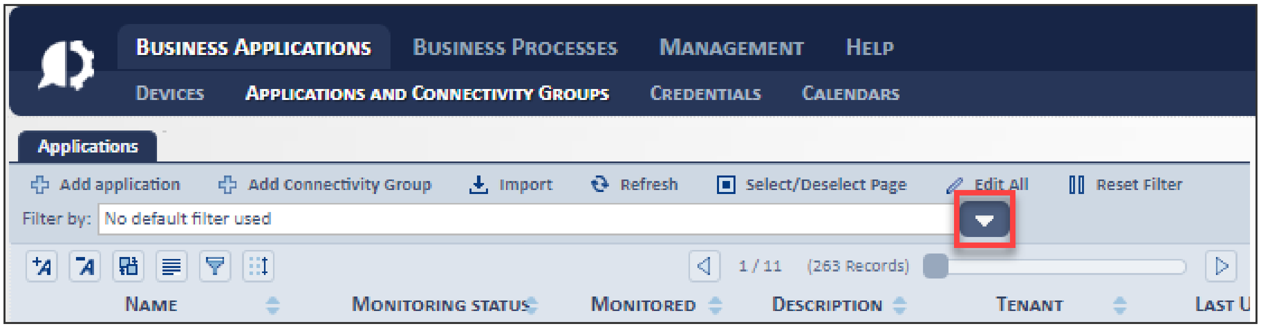
7. In the **Edit IP Address** dialog, enter the IP Address of the new machine of which you have migrated the installation of Event Manager.

8. Click **Accept**.

IMPORTANT: Repeat steps 4 to 8 for the **Core Engine Server Self-Monitoring - HelpSystems** and **Database Server Self-Monitoring - HelpSystems** devices.

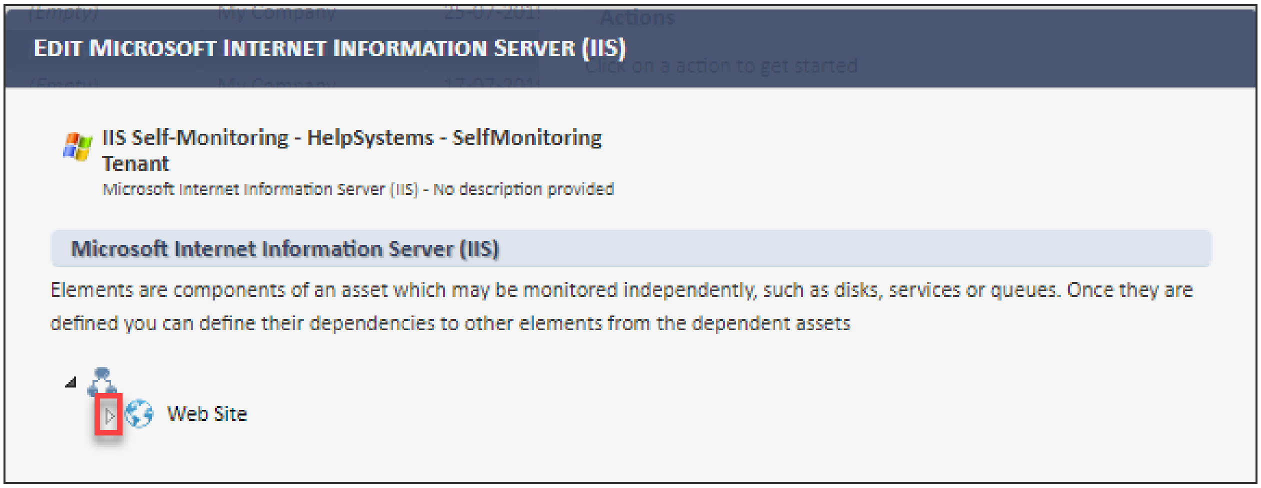
Changing the IIS Self Monitoring Settings

1. Remain in the Orchestrator session and click **Applications and Connectivity Groups**.
2. Use the filter arrow to display a drop-down selection list.



Filter by: No default filter used

3. Scroll down through the list to find **Standalone Application** > **Web Server** > **Microsoft Internet Information Server (IIS)** and click so it is selected.
4. From the options that now appear, click **IIS SelfMonitoring - HelpSystems**.
5. From the **Assets Action** menu select **Edit elements and their dependencies**.
6. On the **Edit Microsoft Internet Information Server (IIS)** click the arrow next to **Web Site** to expand the branch.



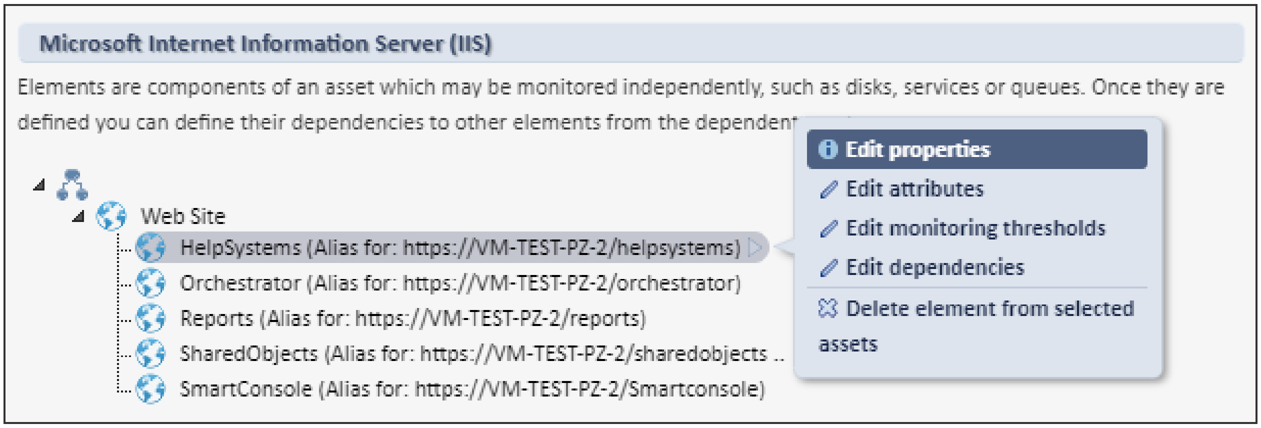
IIS Self-Monitoring - HelpSystems - SelfMonitoring Tenant

Microsoft Internet Information Server (IIS) - No description provided

Microsoft Internet Information Server (IIS)

Elements are components of an asset which may be monitored independently, such as disks, services or queues. Once they are defined you can define their dependencies to other elements from the dependent assets

7. Hover over the first entry in the list (HelpSystems) and an arrow appears at the end of this entry. Click the arrow to display a pop-up menu and select **Edit Properties**.



Microsoft Internet Information Server (IIS)

Elements are components of an asset which may be monitored independently, such as disks, services or queues. Once they are defined you can define their dependencies to other elements from the dependent

Web Site

HelpSystems (Alias for: https://VM-TEST-PZ-2/helpsystems)

Orchestrator (Alias for: https://VM-TEST-PZ-2/orchestrator)

Reports (Alias for: https://VM-TEST-PZ-2/reports)

SharedObjects (Alias for: https://VM-TEST-PZ-2/sharedobjects ..

SmartConsole (Alias for: https://VM-TEST-PZ-2/Smartconsole)

Edit properties
Edit attributes
Edit monitoring thresholds
Edit dependencies
Delete element from selected assets

8. In the **Name** field, amend the host name of the current entry (in this instance, VM-TEST-PZ-2) to that of the new machine where the software has been migrated. Click **Accept**.
9. Repeat the last two steps for all the remaining entries in the Web Site branch.

Appendix 3

How to change the domain of a machine with Event Manager installed

Before starting the change of domain it is necessary to export the Reports application from the AccessServer directory. This is because the Reports application does not register when the AS_Cfg file is executed.

1. On the Windows Server to be changed, navigate to the AccessServer/bin directory, open a CMD, run as Administrator, and execute the following command:

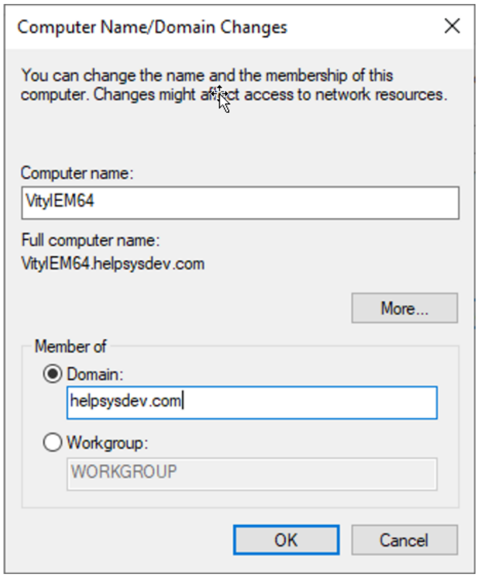
   ```
   AS_ExIm.exe export -a Reports -f Reports.smd -u USER -pass PASSWORD -d DOMAIN
   ```

IMPORTANT: The User, Password and Domain values must be from the current SecAdmin user.

2. Open Windows Explorer and right click on 🖥 **This PC** icon. Select **Properties**.

   The System window opens.

3. Select **Change settings**. With the System Properties window open, click **Change** in the Computer Name tab.
4. Select **Domain** in the 'Member of' section and enter the domain name.


Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: VitylEM64

Full computer name: VitylEM64.helpsysdev.com

Member of

● Domain: helpsysdev.com

○ Workgroup: WORKGROUP

5. When prompted, enter the **Username** and **Password** of an account with sufficient permissions to join the domain. A message is displayed confirming the change.

Before restarting the machine, it is very important to add the domain user with which the machine is going to be accessed.

1. In the System window (previously opened), select **Remote settings**.
2. Click **Select Users** and add the domain user.
3. Restart the machine.
4. Log onto the machine with the added Domain user.

Adding Administrator permissions to the domain user to access and execute tools of Event Manager.

1. Navigate to **Control Panel**, select **User Accounts** and then **Manage User Accounts**.
2. Select the domain user, click on **Properties**, and select **Administrator role**.

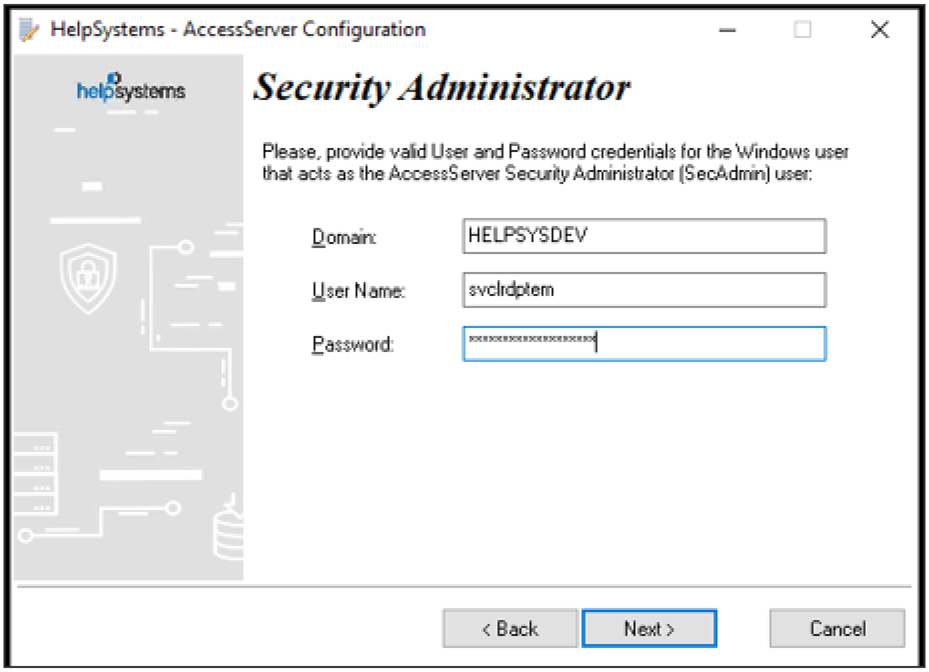
> **NOTE:** You must use Windows Administrator credentials for this procedure.

3. Navigate to: Installation Directory\Help Systems\AccessServer\bin and execute the AS_Reset.exe file. Execute from Command Console, using the following command:

   AS_Reset.exe <user> <pass> [<domain> <AS_Address:AS_Port>]

> EXAMPLE: C:\Program files (x86)\Help Systems\AccessServer\bin>AS_Reset.exe administrator MyPass1234 127.0.0.1:18081

4. Execute the **AS_SetSecAdm.exe** file to set a new Security Administrator.
5. In CMD, set the **Domain Name**, **User Name** and **Password**.
6. Execute the **AS_Cfg.exe** to register applications with new domain.
7. In Security Administrator window, set the new **Domain**, **User Name** and **Password**.



Please, provide valid User and Password credentials for the Windows user that acts as the AccessServer Security Administrator (SecAdmin) user:

Domain: HELPSYSDEV

User Name: svclrdptem

Password: ******************

Once the application registration is complete, you must access the Database Settings Administrator: (Installation Directory\Help Systems\DbSetAdmin\EvLgCnfg.exe).

1. Navigate to **Settings** tab and add the domain name behind the name of the machine (**HostName** and **HelpSystems Machine** fields).

2. Check the connection and click on **Save and Exit**.
3. Navigate to the system using the url: https://<MachineName>.<domain>/HelpSystems.

Access to all applications is now available, except Reports. The registration of the Report application must be done manually. For this we will use the file that we exported in step 1 at the start of this process.

1. Open the exported file (Reports.smd) in a text editor and modify **User** and **Domain** in the following line:

   actor="User@User@Domain@WindowsNT"/>

IMPORTANT: Only the first User value must be modified.

EXAMPLE:
actor="<newSecAdmin>@User@<newSecAdminDomain>@WindowsNT"/>

2. Replace with these values all the occurrences that exist in the file. Save the changes.
3. Then, navigate to AccessServer/bin directory, open a CMD, and execute the following command:

   AS_ExIm.exe import -a Reports -f <Report export file route> -u <newSecAdmin User> -pass <newSecAdmin Password> -d <newSecAdmin Domain>

NOTE: The Report export file is, in this case, the "Reports.smd" file exported in the first step of this section.

TIP: The import may not be instantaneous, it may take time, and its progress is not displayed, therefore we recommend waiting for the console to successfully complete the process.

Appendix 4

Encrypting Event Manager Events

If you want to secure the Event Manager databases by encrypting its events, you can use Microsoft Transparent data encryption (TDE).

TDE protects data at rest, which is the data and log files. It performs a real-time I/O encryption and decryption of these files. Therefore, once applied, it is transparent from an Event Manager point of view. With TDE applied in your databases, even if a malicious party steals these files such as physical media drives or backup tapes, it will be impossible to restore or attach the database and browse its data. See Microsoft TDE documentation for more details.

Steps for enabling TDE encryption for Event Manager

Once you have decide to enable TDE you must plan it properly as it may take some time to complete the process.

First of all list all the Event Manager databases. Event Manager can have up to 3 databases:

- **Short-term Database**. The default name is HS_APPSEC_Security.
- **History Database**. The default name is HS_APPSEC_Security_Hist.
- **Archive Database**. The default name is HS_APPSEC_Security_Arch.

Find out the number of records in each database. In a ‘normal’ environment, encryption speed could be about 2.500 records / second. For example, if you have about 25 million of records it will take about 3 hours to enable TDE.

Once you have an approximate downtime you can start with the following steps:

> **NOTE:** Steps 4 and onwards are identical for SQL versions ranging from 2016 to 2022. If you are using a different one, consult the Microsoft documentation for TDE.

1. It is highly recommended that you backup the Event Manager Databases before encrypting them, just in case you need to roll back changes. Another option would be to create a snapshot of the system where SQL Server and databases are installed.
2. Stop all Event Manager Windows services on the system on which it is installed. Their names start with ‘HelpSystems -‘
3. Stop IIS (Internet Information Server) on the system on which Event Manager it is installed. Do this by stopping Windows service ‘World Wide Web Publishing Service.’
4. Create a Master Key for the master database
    a. Run SQL query:

       Use master;

       GO

       CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<UseStrongPasswordHere>';
5. Create or obtain a certificate protected by the master key.
    a. Run SQL query:

       USE master;

       GO

       CREATE CERTIFICATE MyServerCert WITH SUBJECT = 'My DEK Certificate';
6. Create a database encryption key and protect it by using the certificate for Short-term database (named HS_APPSEC_Security by default).
    a. Run SQL query:

       USE HS_APPSEC_Security;

       GO

CREATE DATABASE ENCRYPTION KEY WITH ALGORITHM = AES_256 ENCRYPTION BY SERVER CERTIFICATE MyServerCert;

GO

7. Set the Short-term database to use encryption.

   a. Run SQL query:

      ALTER DATABASE HS_APPSEC_Security SET ENCRYPTION ON;

      This is where encryption of data files start. This encryption operation is scheduled on background threads by SQL Server. You must wait for completion of this step. You can use the following query to check it:

      select DB_NAME(database_id), encryption_state, percent_complete from sys.dm_database_encryption_keys.

      While field ‘encryption_state’ returns 2 for database HS_APPSEC_Security it means that encryption is in progress. You have a field ‘percent_complete’ which could help you in estimate how much time it will take. Encryption is completed once field ‘encryption_state’ returns value 3.

8. Create a database encryption key and protect it by using the certificate for History database (named HS_APPSEC_Security_Hist by default).

   a. Run SQL query:

      USE HS_APPSEC_Security_Hist;

      GO

      CREATE DATABASE ENCRYPTION KEY WITH ALGORITHM = AES_256 ENCRYPTION BY SERVER CERTIFICATE MyServerCert;

      GO

9. Set the History database to use encryption.

   a. Run SQL query:

      ALTER DATABASE HS_APPSEC_Security_Hist SET ENCRYPTION ON;

      You can check encryption progress for this database with the query in step 7.

10. Create a database encryption key and protect it by using the certificate for Archive database (named HS_APPSEC_Security_Arch by default).

    a. Run SQL query:

    ```
    USE HS_APPSEC_Security_Arch;
    GO
    CREATE DATABASE ENCRYPTION KEY WITH ALGORITHM = AES_256
    ENCRYPTION BY SERVER CERTIFICATE MyServerCert;
    GO
    ```

11. Set the Archive database to use encryption.

    a. Run SQL query:

    ```
    ALTER DATABASE HS_APPSEC_Security_Arch SET ENCRYPTION ON;
    ```

12. During TDE enabling steps you will receive a message like this:

    "*Warning: The certificate used for the database encryption key has not been backed up. You should immediately back up the certificate and the private key associated with the certificate. It the certificate ever becomes unavailable or if you must restore or attack the database on another server, you must have backups of both the certificate and the private key or you will not be able to open the database.*"

    You should perform the backup mentioned here. Please refer to Microsoft TDE documentation for more details.

13. Once encryption is completed for the 3 databases, you can start IIS and all the Event Manager Windows services. Alternatively, you can restart system where Event Manager is installed. After a few minutes application should be available and working normally.

Performance with TDE enabled

Once TDE is enabled, database operations (read, insert and update) could experience a slight drop in performance (about 10%), but the overall Event Manager experience shouldn't be affected.

Disabling TDE

In case you need it you can remove the encryption in a database. Refer to Microsoft TDE documentation for more details.

Contacting Fortra

Please contact Fortra for questions or to receive information about Event Manager. You can contact us to receive technical bulletins, updates, program fixes, and other information via electronic mail, Internet, or fax.

Fortra Portal

For additional resources, or to contact Technical Support, visit the Fortra Support Portal at https://support.fortra.com.

For support issues, please provide the following:

- Check this guide's table of contents and index for information that addresses your concern.
- Gather and organize as much information as possible about the problem including job/error logs, screen shots or anything else to document the issue.