

FORTRA

Insite
3.08

Getting Started Guide

Copyright Terms and Conditions

Copyright © Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.

The content in this document is protected by the Copyright Laws of the United States of America and other countries worldwide. The unauthorized use and/or duplication of this material without express and written permission from Fortra is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to Fortra with appropriate and specific direction to the original content.

202305150443

Table of Contents

Welcome to Insite	1
Getting Started Checklist	3
Installation and Configuration Checklist	3
System Requirements	4
Installing or Updating Insite on Your Windows Server	9
Installing or Updating Insite on Your Windows Server - Quick Setup	11
Installing or Updating Insite on Your Windows Server - Single System	16
Installing or Updating Insite on Your Windows Server - Multiple Systems	22
Installing or Updating Insite on Linux or Power Linux Servers	33
Installing or Updating Insite on Your Linux Server - Single System	34
Installing or Updating Insite on Your Linux Server - Multiple Systems	37
Insite Integration Service	41
Important Notes	41
Startup Wizard	43
Adding a New Product Connection	49
Importing IBM i Product Connections	57
Securing an IBM i Product Connection	58
Authentication	61
Adding a Role	67
Adding a Default Profile	70
Adding a Security Group	71

Adding a User	74
Securing Insite	77
Generating a Self-Signed Certificate	77
Enabling the Certificate	78
Accessing the Page	79
Troubleshooting	80

Welcome to Insite

Insite gives you a single web interface where you can go to work with your Fortra 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®, Linux® or Power Linux® system, open the web interface in your favorite browser and point it to the server where Insite is installed. Within Insite you will connect to 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:

- **Automate Ops Console:** Use this to monitor and control your Automate Enterprise server resources, including workflows, tasks, processes, and agents.
- **Automate Schedule Ops Console:** Use this to display vital Automate Schedule statistics and activity from within Insite Dashboards.
- **Deployment Manager:** Use this to quickly and easily install, update, and license your Fortra products.
- **Event Manager:** Use this to display vital Event Manager statistics and activity from within Insite Dashboards.
- **Insite Analytics:** Use this to display information from your installation of Insite Analytics in a web-based interface.
- **Insite Watch List:** Use this to display the overall health of supported Fortra products in a single dashboard widget.
- **Network Security:** Use this to monitor and control access to networked systems that are set up in Network Security.
- **Powertech Multi-Factor Authentication:** Use this to implement multi-factor authentication for user sign on.
- **Powertech Antivirus:** Use this to monitor and manage Powertech Antivirus on endpoints across your network.
- **Password Self Help:** Use this to allow users to reset their own passwords without assistance from a help desk or system administrator.
- **Robot Console:** Use this to manage system messages, resource monitoring, and system log monitoring.
- **Robot Network:** Use this to monitor the performance and statuses of your IBM i partitions, and respond to statuses (Reply, Escalate, Assign, and etc.).

- **Robot Reports:** Use this to view or download reports that are set up and have run in Robot Reports.
- **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.

Getting Started Checklist

Installation and Configuration Checklist

Task	Detail	Complete
Download and Install	Log in to your Fortra account. Download and install the software for Insite. See Installing on Windows and Installing on Linux for more information.	
Run through the Startup Wizard	Use the Startup Wizard to help you through the initial product setup. See Startup Wizard .	
Add Product Connections	Add any more necessary product connections for your installed products. See Adding a Product Connection .	
Set up Authentication	This page allows you to set the session timeout, define the authentication method, and enable guest logins. See Authentication .	
Define Roles	User access to Insite and its products can be secured through the use of Roles, which are collections of authorities that define a user's permissions for managed systems and products. See Adding Roles .	
Set up Default Profiles	Default profiles allow you to connect to a role or system without needing to create a user. See Adding Default Profiles .	
Set up Security Groups	If you have a large number of users in Insite, you may find it useful to put them in groups. See Adding Security Groups .	
Set up Users	There are two ways a user can be added. You can create them manually from the Users page, or they will be created automatically for anyone who logs on to Insite through proper authentication channels. See Adding Users .	

System Requirements

Read this information completely before you install Insite on your Windows, Power Linux or Linux servers.

- If there are any firewalls between your PC and the server, verify that your profile has access to the PC.
- Your network must be configured and working using TCP/IP configuration.
- Insite supports GNU Tar. Be sure you are using that version of tar.
- Installation on an Active Directory server is not supported.
- If connecting to an IBM i system, we install a library called INSITELIB and two User Profiles, INSITEADM and INSITEUSR. For more information, see [INSITELIB, INSITEADM, and INSITEUSR: What are They and How are They Used?](#)
- When performing an Insite 3.x install, all Insite servers need to be part of a valid domain for certificates to be created for Insite services.
- If Insite is at 2.00 to 2.04, Insite will need to be updated to 2.08 prior to updating to 3.x or above. If you are running Insite 1.x, contact support for assistance on the upgrade process.
- If you are using Multifactor Authentication 1.4 or below with Insite, please contact Multifactor Authentication support for assistance on the upgrade process for both products.
- We always recommend backing up Insite before updating.

The following products are compatible with Insite:

- Automate BPA Server 10.5 or higher
- Automate Schedule 4.3 or higher
- Insite Analytics 1.0 or higher
- Insite Watch List 1.0 or higher
- Powertech Antivirus 5.0 or higher
- Powertech Event Manager 6.1 or higher
- Powertech Exit Point Manager for IBM i R7M04 or higher
- Powertech Multi-Factor Authentication 1.0 or higher
- Powertech Password Self Help 3.001 or higher
- Robot Console 7.03 or higher
- Robot Network 11.00 or higher
- Robot Reports 7.70 or higher

- Robot Schedule 10.30 or higher
- Vityl IT & Business Monitoring 1.0 or higher

NOTE: IBM i systems that will be connecting to your Insite Server must be at V7R2 or higher.

Insite Server Requirements

To install Insite, your server must meet the following requirements.

Supported Operating Systems:

- Windows Server 2012*
- Windows Server 2012 R2*
- Windows Server 2016
- Windows Server 2019
- RedHat Enterprise/Centos 7
 - X86_64
 - PPC64LE
 - PPC64
- RedHat Enterprise/CentOS 8
 - X86_64
 - PPC64LE
- Suse Enterprise Linux 12
 - X86_64
 - PPC64LE
- Suse Enterprise Linux 15
 - X86_64
 - PPC64LE
- Ubuntu Linux 16
 - X86_64
 - PPC64LE
- Ubuntu 18.04
 - X86_64

NOTE:

- Insite can only run on 64-bit Windows operating systems; 32-bit Windows is not supported. In addition, Insite cannot be installed on the following Windows versions: Windows XP SP2 x64, Windows Server 2003 SP2 x64, Windows Vista x64, Windows Server 2008 x64, Windows 7 x64, Windows Server 2008 R2 x64, Windows 8 x64, Windows 8.1 x64, and Windows 10 x64.
- In order to install on a Windows server, we must have RemoteSigned or Unrestricted PowerShell access. To check what is currently set, use command `Get-ExecutionPolicy` in PowerShell. To change access, use the command `Set-ExecutionPolicy` with an argument of either `RemoteSigned` or `Unrestricted`.

* The browser that ships with Windows Server 2012, Internet Explorer 10, is not supported. See below for supported browsers.

Other Required Software:

- Perl 5.6 or later (Linux)
- GNU Tar (Linux)
- openssl (Linux)
- net-tools (Linux)

Minimum Hardware Requirements:

- *Insite version 3.x*
 - For Insite 3.x NOT using Powertech Antivirus (PTAV):
 - 8 GB RAM
 - 10 GB free space
 - 4 CPU
 - For Insite 3.x using PTAV with up to 500 PTAV connections:
 - 16 GB RAM
 - 50 GB free space
 - 4 CPU
 - For Insite 3.x using PTAV with up to 1000 PTAV connections:
 - 16 GB RAM
 - 50 GB free space
 - 8 CPU
 - System is dedicated to Insite (not shared with other server apps)
- *Insite version 2.x and 1.x*

- 4 GB RAM available
- 3 GB free space

Web Browser Requirements

Insite is compatible with the latest versions of these browsers:

Computer-Based Browsers:

- Chrome
- Firefox
- Internet Explorer
- Safari (only on iOS)
- Microsoft Edge

Mobile-Based Browsers:

- Browsers on iOS 11 or higher
- Browsers on Android OS 4.4 or higher using Chrome

Other browsers and browser versions may work, but be aware that features in Insite might not load correctly.

Server and Exit Point Considerations:

Server	Exit Point
RMTCMD	QIBM_QZRC_RMT
SIGNON	QIBM_QZSO_SIGNONSRV
DATABASE	QIBM_QZDA_SQL1 and QIBM_QZDA_SQL2
FILE	QIBM_QPWFS_FILE_SERV
NETPRT	QIBM_QNPS_ENTRY

Note: Robot Network also uses the DDM and TELNET TCP/IP servers.

*****IMPORTANT***** Read the following before using Powertech Network Security for Insite.

If *PUBLIC is locked down in your current Network Security configuration, in order to use Insite, you must create rules that allow the Insite profiles access to specific server functions.

The Insite user profile that is used for authentication needs access to the following:

Server Function

*SIGNON RETRIEVE

Any user profile that is used by the admin for a product connection needs access to the following:

Server Function

*NDB ADDLIBL
 *RMTSRV DSTPGMCALL
 *RMTSRV RMTCMD
 *SIGNON RETRIEVE
 *SQL INIT
 SQLSRV OPENFETCH
 SQLSRV PRPDESCRB
 SQLSRV EXECUTE

Any user profile that is set up by any user other than the admin needs access to the following:

Server Function

*RMTSRV DSTPGMCALL
 *RMTSRV RMTCMD
 *SIGNON RETRIEVE
 QNPSERV INIT

For information on granting access to the above functions, see the Powertech Network Security for Insite online help.

Port Considerations:

You must have open ports on the webserver in order to install the Insite software. These ports are configured during installation. For more information, see [Ports and URLs used by Insite](#).

We recommend that the exit points (listed above) and ports be open to the RBTUSER, RBTADMIN, RBTNETPT, and user profiles logging on to Insite.

Installing or Updating Insite on Your Windows Server

Installing Insite allows you to access your Fortra products through a web browser interface. Currently, Insite allows you to access the following products:

- Automate BPA Server 10.5 or higher
- Automate Schedule 4.3 or higher
- Insite Analytics 1.0 or higher
- Insite Watch List 1.0 or higher
- Powertech Antivirus 5.0 or higher
- Powertech Event Manager 6.1 or higher
- Powertech Exit Point Manager R7M04 or higher
- Powertech Multi-Factor Authentication 1.0 or higher
- Powertech Password Self Help 3.001 or higher
- Robot Console R7M03 or higher
- Robot Network R11M00 or higher
- Robot Schedule R10M30 or higher
- Vityl IT & Business Monitoring 1.0 or higher

Make sure your system meets the [minimum requirements](#) before installing or updating Insite on your Microsoft Windows Server.

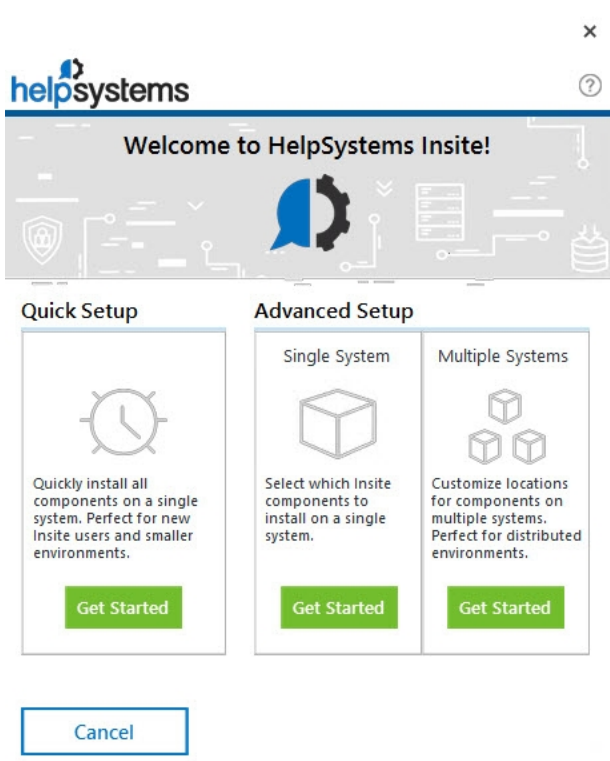
NOTE:

- You can download the installer from the customer portal. The installer is available whether you are requesting a free trial of our software, updating your software, or converting your software.
- The ports that Insite uses must be open on all servers that Insite components will be installed. See [Ports and URLs Used by Insite](#) for a listing of these ports.
- If Insite is at 2.00 to 2.04, Insite will need to be updated to 2.08 prior to updating to 3.x or above. If you are running Insite 1.x, contact support for assistance on the upgrade process.
- If you are using Multifactor Authentication 1.4 or below with Insite, please contact Multifactor Authentication support for assistance on the upgrade process for both products.
- If you are using Multi-Factor Authentication, end it before updating Insite by ending the processes in this order: the Message Broker, the Database server, the Authentication Manager service. Contact support if needed.
- We always recommend backing up Insite before updating.
- Installation on Windows requires a user account that is a member of the Administrators user group.

Complete the following steps to download and install Insite on your Windows server.

1. Download the **Helpsystems Insite.exe** installation file on the customer portal.
2. Double-click the **HelpSystems Insite.exe** file.

3. You are presented with your installation options. Choose the option that best serves your needs. The detail pages for each option are listed below.



[Quick Setup](#)

[Single System](#)

[Multiple Systems](#)

Installing or Updating Insite on Your Windows Server - Quick Setup

Make sure your system meets the [minimum requirements](#) before installing or updating Insite on your Microsoft Windows Server.

NOTE:

- You can download the installer from the customer portal. The installer is available whether you are requesting a free trial of our software, updating your software, or converting your software.
- If you are updating Insite and have specific configuration you would like to retain, we recommend backing up Insite prior to updating.

The Quick Setup option is for users that are new to Insite and are only installing or updating on a single system. This option will install all of Insite's prerequisite services and products. You will not have the option to exclude any products or services.

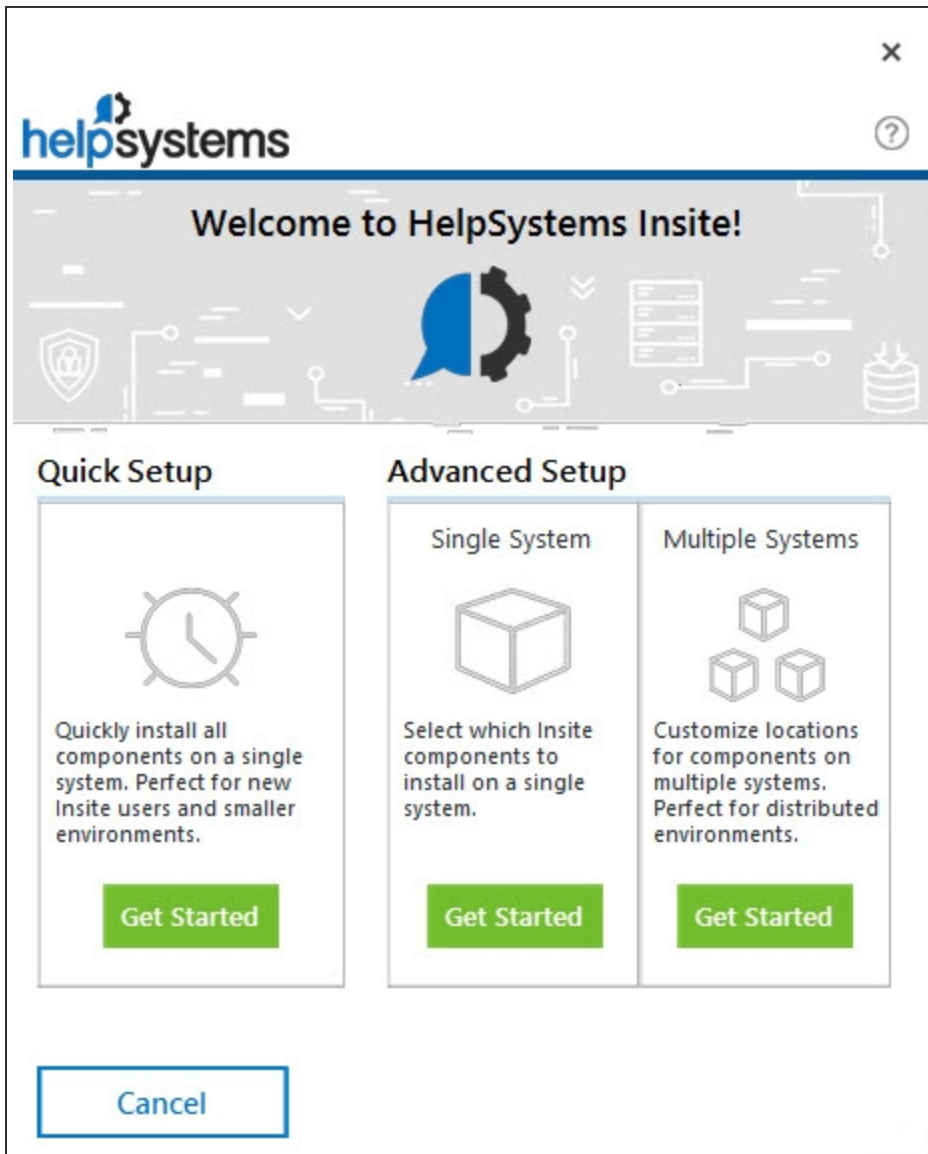
Installation on Windows requires a user account that is a member of the Administrators user group.

NOTE:

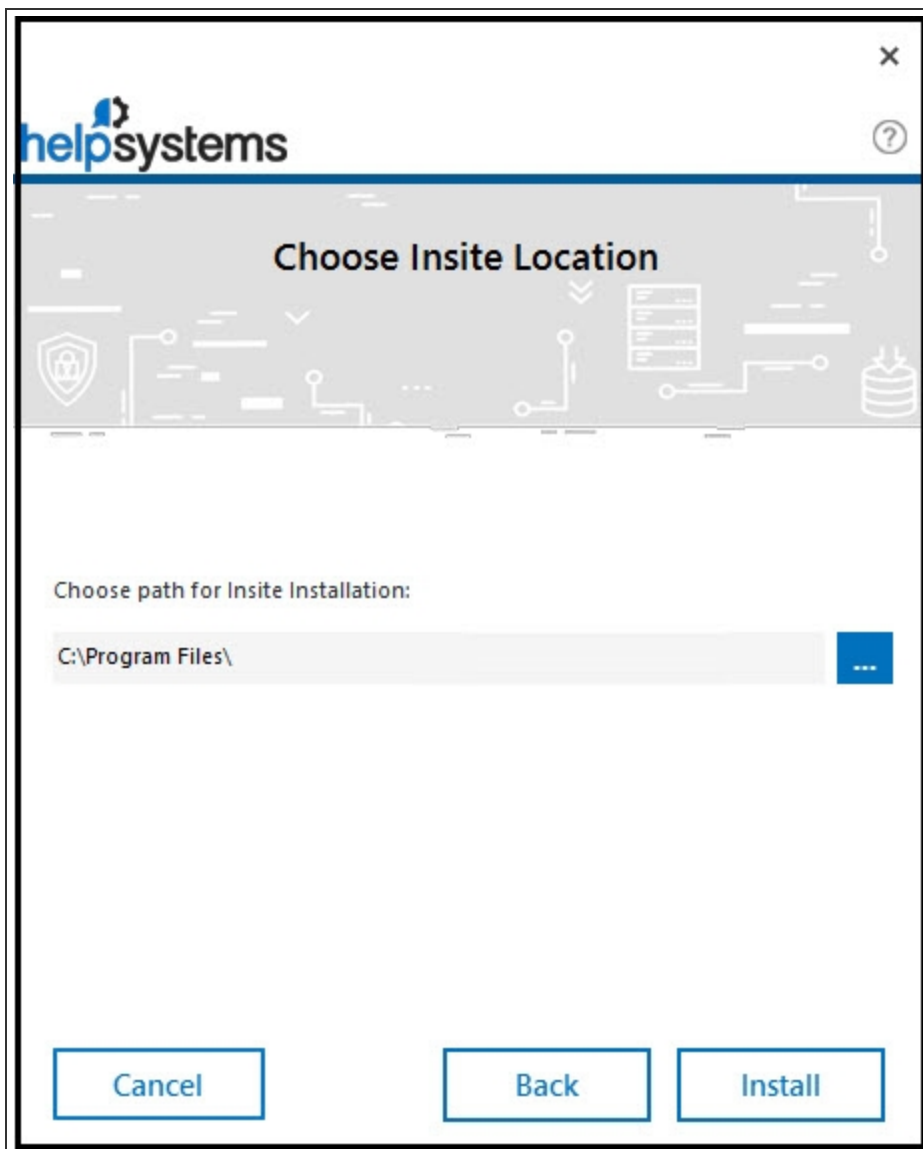
Insite Watch List is a component of Insite that will be installed and cannot be excluded with Quick Setup. The installation of Insite Watch List can add additional time to the installation process.

Quick Setup:

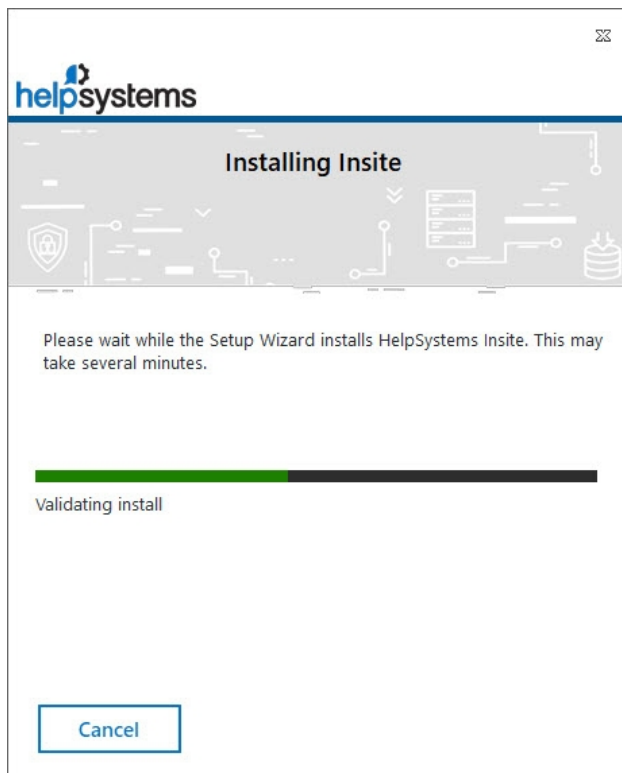
1. Click **Get Started** within the Quick Setup section of the installation window.



2. Choose the location where you would like to install Insite. You can change the default location.



3. Click **Install**.
4. The installation begins. The installer gives you a detailed view of the installation progress.



5. The Insite Server Configuration Manager window displays. You must set up ports for Insite. The installer lets you know if the default ports are available. If a port is unavailable, enter a new port number and click **Test** to see if it is available. Once all ports are available, click **OK**.

helpsystems Step 4 of 5

Configure Insite Ports

Server Address: Server2016.sysdev.com

Insite Server

Shutdown Port: 3029 ✓ Connector Port: 3030 ✓

Insite Database

Database Port: 5432 ✓

Integration Service

Server Port: 8998 ✓ Coordinator Port: 2181 ✓ Message Broker Port: 9092 ✓ Secure Storage Port: 8200 ✓

Insite Analytics Server

Shutdown Port: 9000 ✓ Connector Port: 9001 ✓

Revert to Defaults Test

Cancel Ok

- Follow the onscreen instructions to complete the installation. After the installation completes, a summary screen will open in your default browser.

After You Are Done

After installation of all components is complete, point a web browser to the following URL:

`http://xxx.xxx.xxx.xxx:nnnn/`

where `xxx.xxx.xxx.xxx` is the IP address of your server and `nnnn` is the connector port number you entered during installation.

NOTE: If you have updated from an earlier Insite version, reload your browser to ensure all services are visible in the Products list.

If this is a new installation, the [Startup Wizard](#) will display to help you configure your installation of Insite. That will help you start setting up the software.

Installing or Updating Insite on Your Windows Server - Single System

Make sure your system meets the [minimum requirements](#) before installing or updating Insite on your Microsoft Windows Server.

NOTE:

- You can download the installer from the customer portal. The installer is available whether you are requesting a free trial of our software, updating your software, or converting your software.
- If you are updating Insite and have specific configuration you would like to retain, we recommend backing up Insite prior to updating.

The Single System option is for users that are only installing or updating on a single system and want the ability to pick which products are installed as part of their Insite installation.

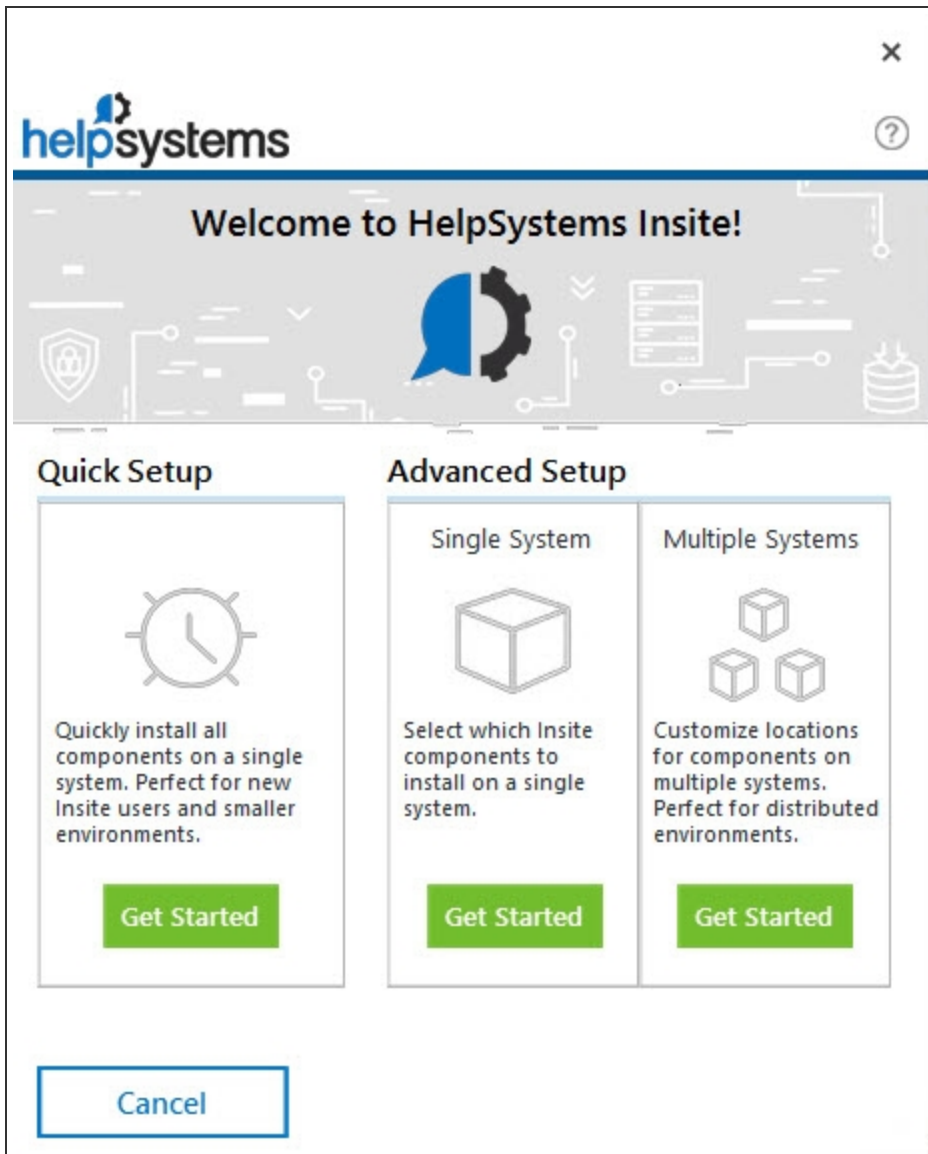
Installation on Windows requires a user account that is a member of the Administrators user group.

NOTE:

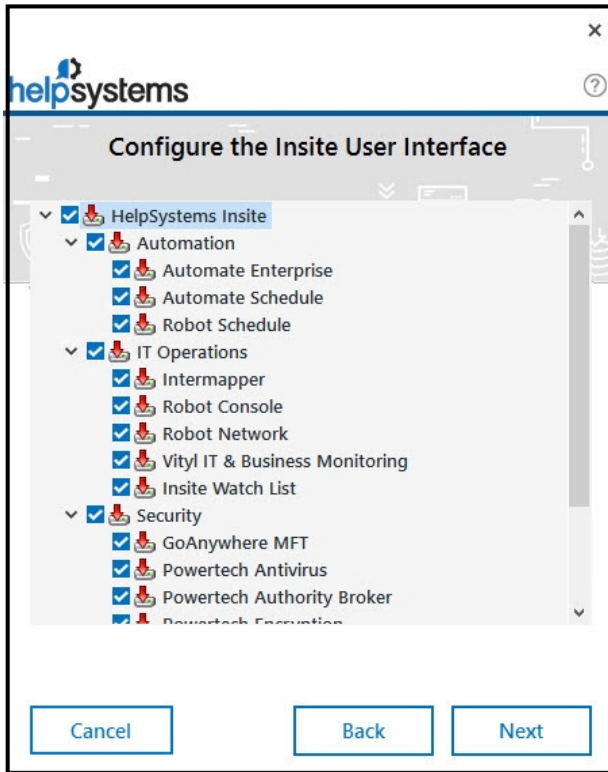
Insite Watch List is a component of Insite that can be installed during your Single System install. The installation of Insite Watch List can add additional time to the installation process.

Single System:

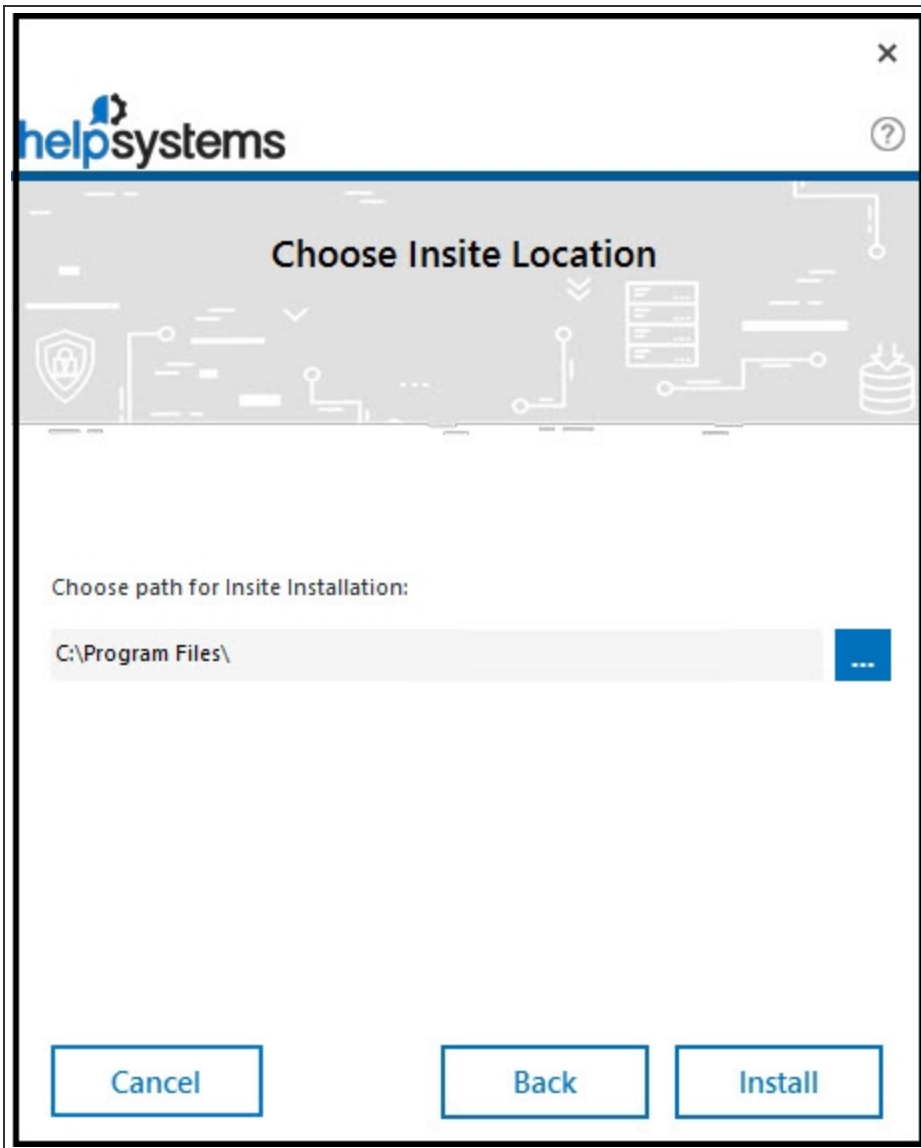
1. Click **Get Started** within the Single System section of the installation window.



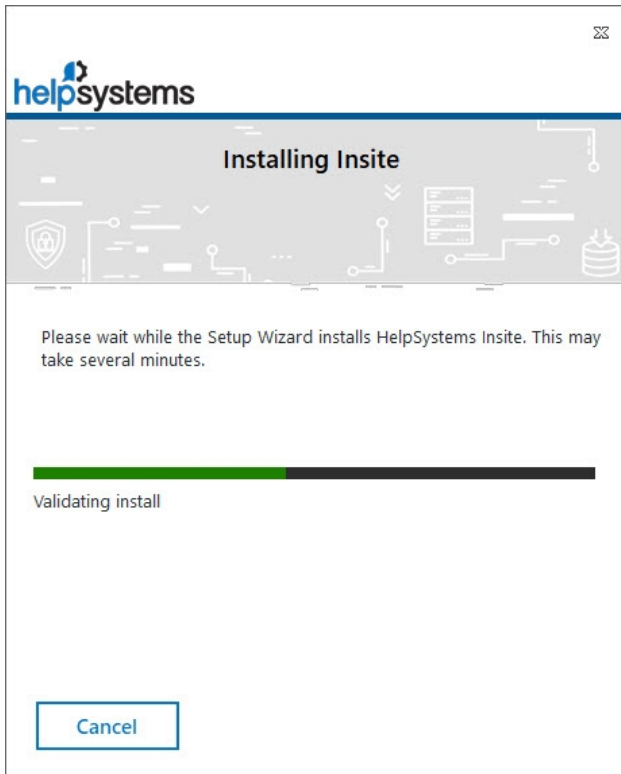
2. On the Configure the Insite User Interface Panel, select the products you want to install and click **Next**.



3. Choose the location where you would like to install Insite. You can change the default location.



4. Click **Install**.
5. The installation begins. The installer gives you a detailed view of the installation progress.



6. The Insite Server Configuration Manager window displays. You must set up ports for Insite. The installer lets you know if the default ports are available. If a port is unavailable, enter a new port number and click **Test** to see if it is available. Once all ports are available, click **OK**.

The screenshot shows the 'Configure Insite Ports' dialog box. At the top left is the 'helpsystems' logo and 'Step 4 of 5' at the top right. The title bar reads 'Configure Insite Ports'. Below the title bar, there are several sections for configuring ports:

- Server Address:** A dropdown menu showing 'Server2016.sysdev.com'.
- Insite Server:** 'Shutdown Port: 3029' and 'Connector Port: 3030', both with green checkmarks.
- Insite Database:** 'Database Port: 5432' with a green checkmark.
- Integration Service:** 'Server Port: 8998', 'Coordinator Port: 2181', 'Message Broker Port: 9092', and 'Secure Storage Port: 8200', all with green checkmarks.
- Insite Analytics Server:** 'Shutdown Port: 9000' and 'Connector Port: 9001', both with green checkmarks.

At the bottom, there are buttons for 'Cancel', 'Revert to Defaults', 'Test', and 'Ok'.

- Follow the onscreen instructions to complete the installation. After the installation completes, a summary screen will open in your default browser.

After You Are Done

After installation is complete, point a web browser to the following URL:

`http://xxx.xxx.xxx.xxx:nnnn/`

where `xxx.xxx.xxx.xxx` is the IP address of your server and `nnnn` is the connector port number you entered during installation.

If you have updated from an earlier Insite version, reload your browser to ensure all services are visible in the Products list.

If this is a new installation, the [Startup Wizard](#) will display to help you configure your installation of Insite. That will help you start setting up the software.

Installing or Updating Insite on Your Windows Server - Multiple Systems

Make sure your system meets the [minimum requirements](#) before installing or updating Insite on your Microsoft Windows Server.

NOTE:

- You can download the installer from the customer portal. The installer is available whether you are requesting a free trial of our software, updating your software, or converting your software.
- If you are updating Insite and have specific configuration you would like to retain, we recommend backing up Insite prior to updating.
- Before performing a multiple system install, ensure the following:
 - Each system is on the same domain and able to resolve the hostname by DNS.
 - Ports from the first system are opened prior to running the install on the second system.

The Multiple Systems option is for users that will be installing or updating components of Insite on multiple systems in a distributed environment. For example, you may want to install the [Insite Integration Service](#) and the Insite User Interface on separate servers.

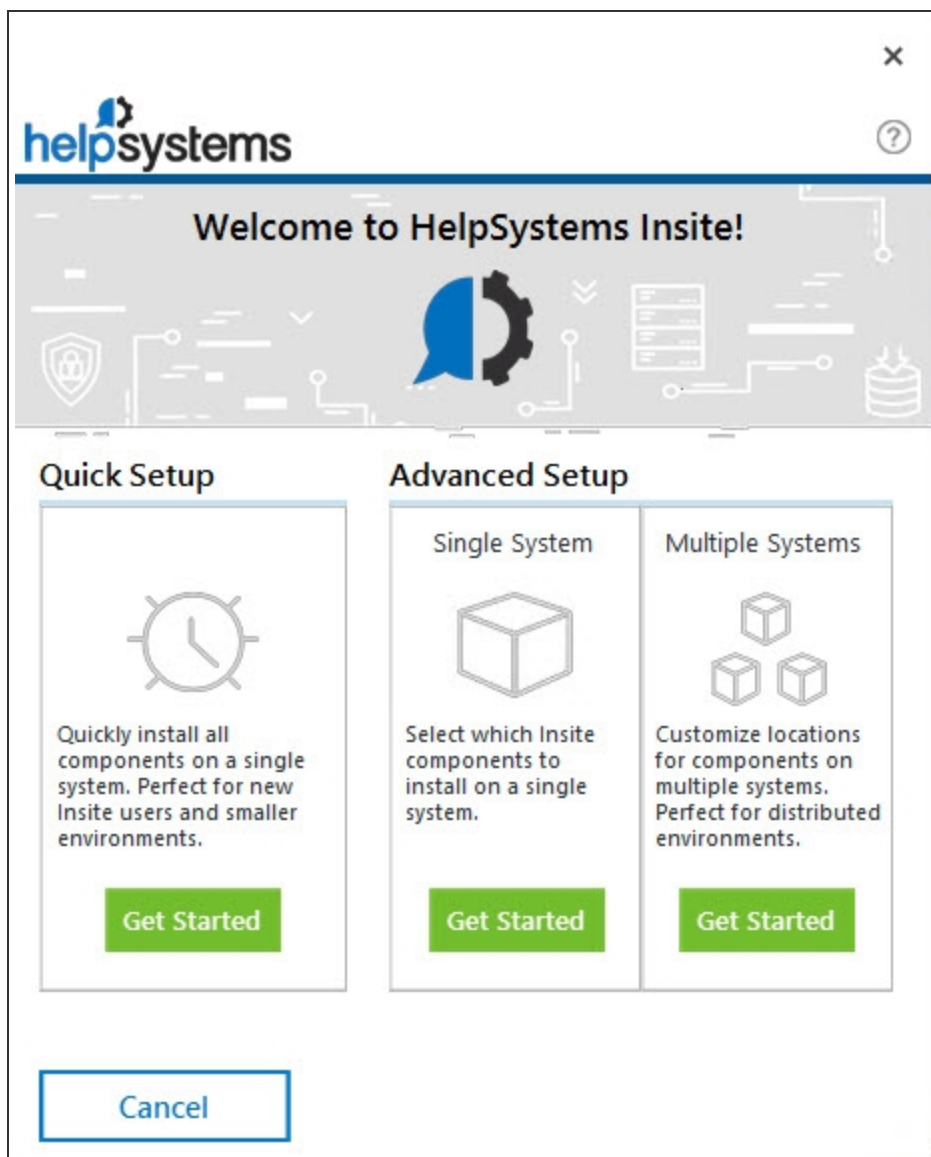
Installation on Windows requires a user account that is a member of the Administrators user group.

NOTE:

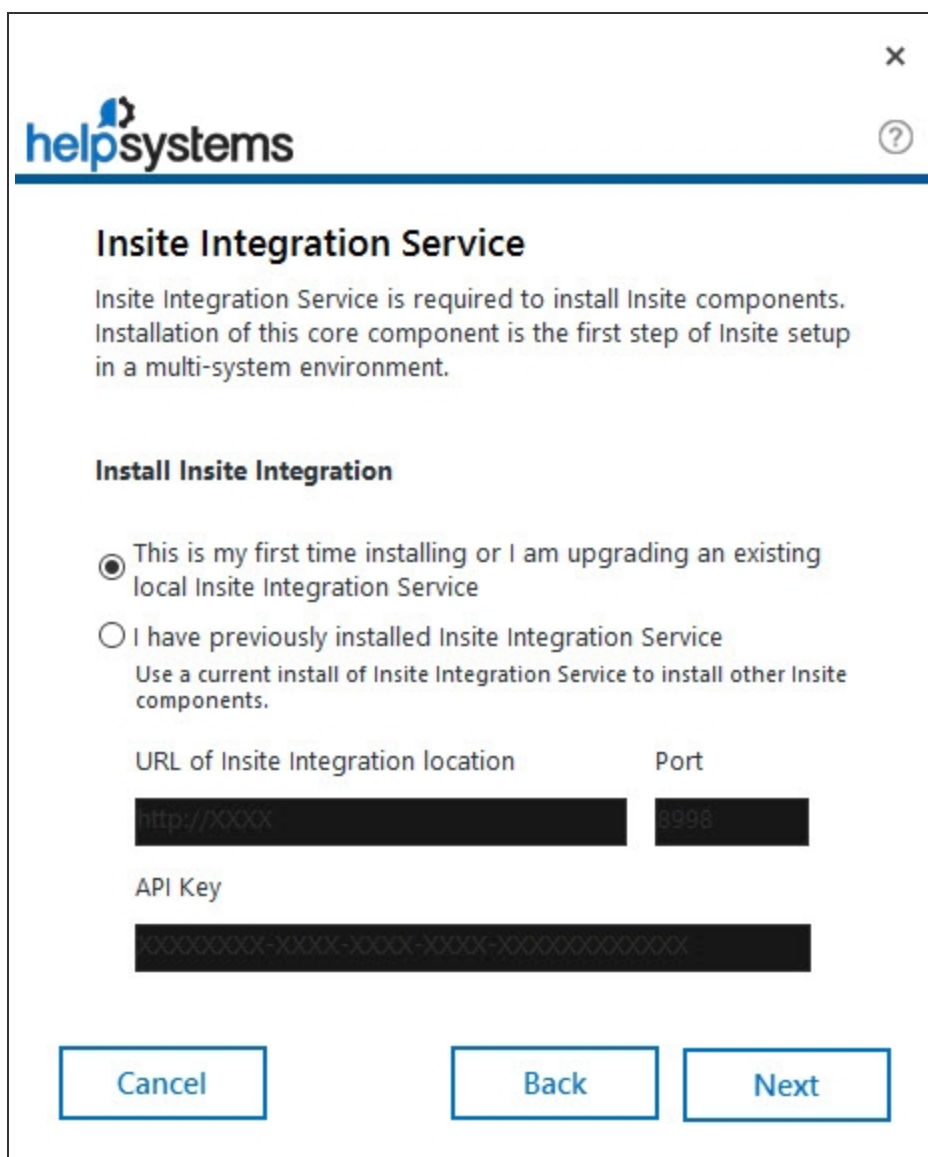
Insite Watch List is a component of Insite that can be installed on any of your multiple systems. The installation of Insite Watch List can add additional time to the installation process.

Multiple Systems:

1. Click **Get Started** within the Multiple Systems section of the installation window.



2. Select whether you have installed [Insite Integration Service](#) previously. If so, enter the **URL**, **Port**, and **API Key**, otherwise, leave the default of 'This is my first time installing Insite Integration Service'. Then, click **Next**.



The screenshot shows a window titled "Insite Integration Service" with the helpsystems logo in the top left. The window contains the following text and controls:

Insite Integration Service

Insite Integration Service is required to install Insite components. Installation of this core component is the first step of Insite setup in a multi-system environment.

Install Insite Integration

This is my first time installing or I am upgrading an existing local Insite Integration Service

I have previously installed Insite Integration Service
Use a current install of Insite Integration Service to install other Insite components.

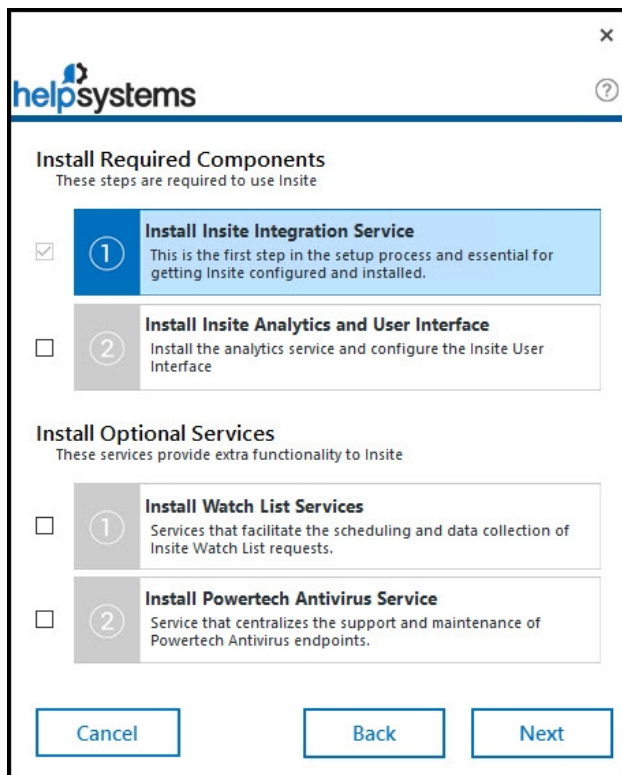
URL of Insite Integration location Port

API Key

At the bottom of the window are three buttons: "Cancel", "Back", and "Next".

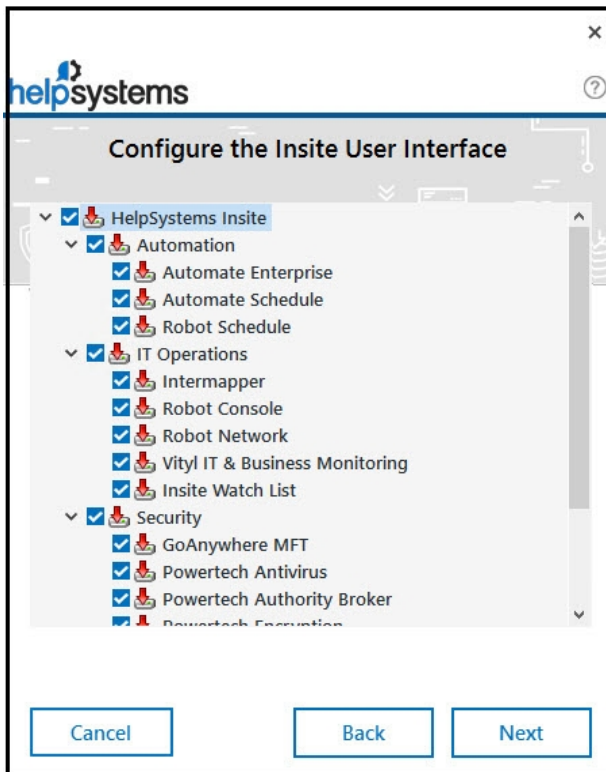
NOTE: If you are entering data for an existing Insite Integration Service installation, be sure to verify its correctness before continuing.

3. On the Install Required Components Panel, select which components you want to install on this system and click **Next**.

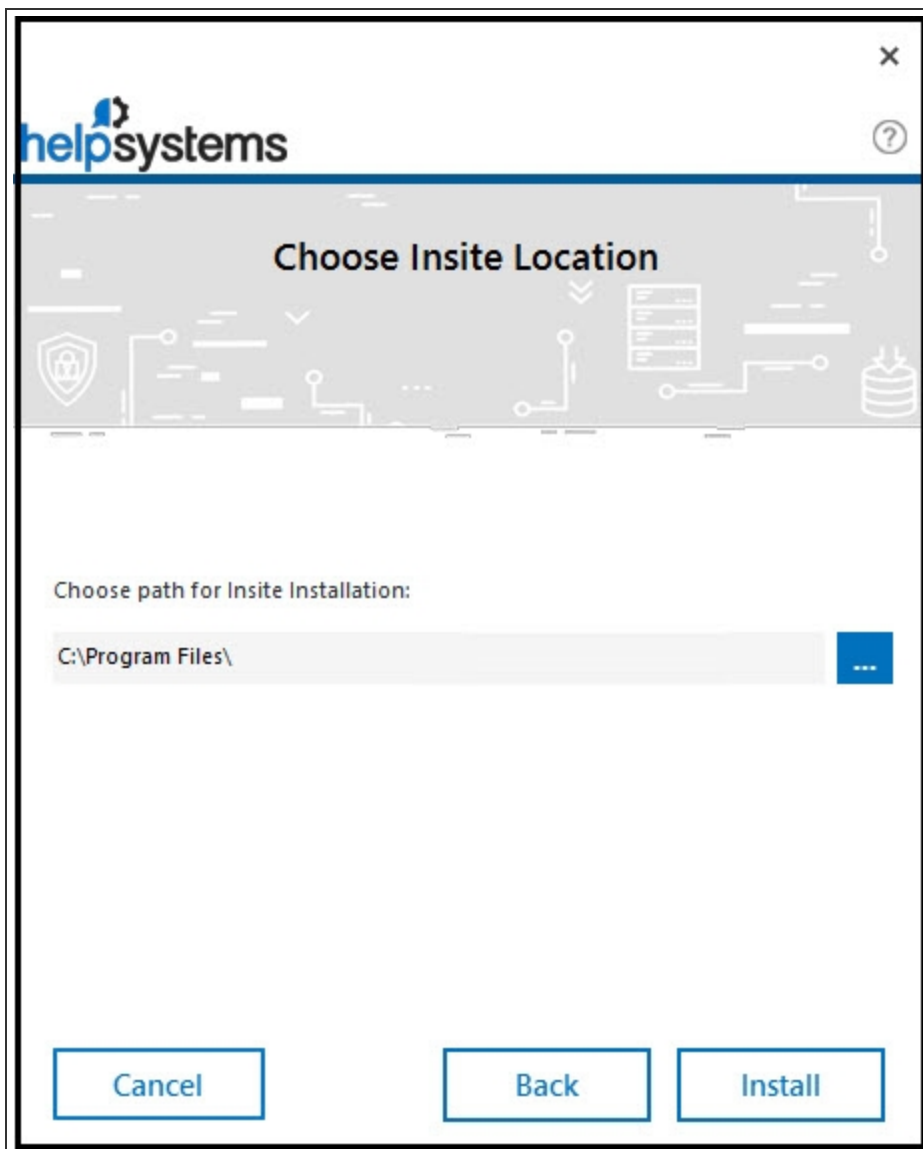


NOTE: If you entered an Insite Integration Service on the previous panel, the Install Insite Integration Service option will be disabled. The installer will use your previous installation of Insite Integration Service to install Insite.

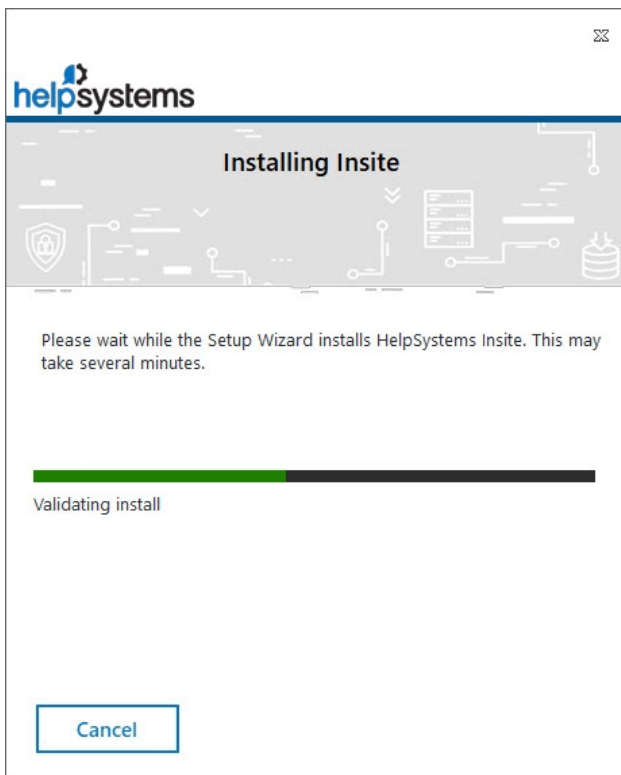
4. If you chose to install Insite Analytics and User Interface, select the products you want and click **Next**.



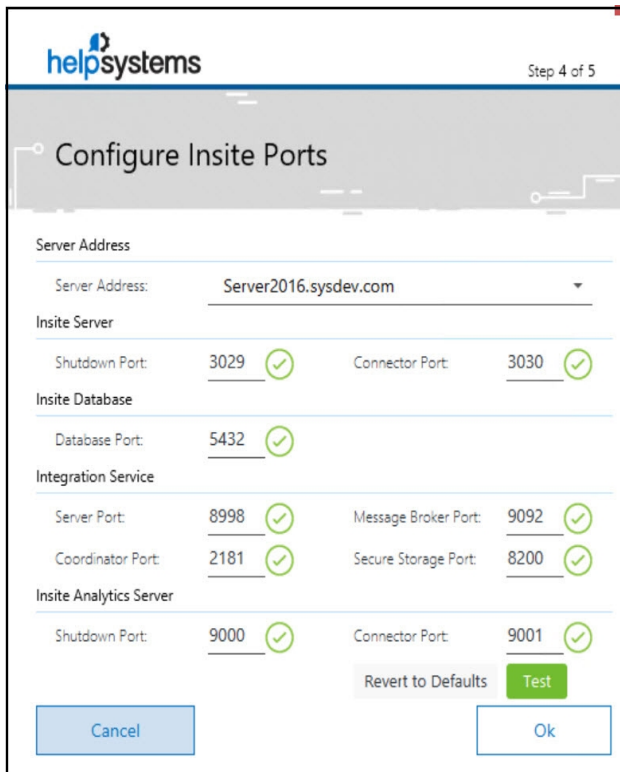
5. Choose the location where you would like to install the Insite components. You can change the default location.



6. Click **Install**.
7. The installation begins. The installer gives you a detailed view of the installation progress.



8. The Insite Server Configuration Manager window displays. You must set up ports for Insite. The installer lets you know if the default ports are available. If a port is unavailable, enter a new port number and click **Test** to see if it is available. Once all ports are available, click **OK**.



9. Follow the onscreen instructions to complete the installation. After the installation completes, a summary screen will open in your default browser.

Installation Summary

Integration Service	Insite Server	Analytics Service	Watch List Coordinator Service
HTTP Port: 8998	HTTP Port: 3030	HTTP Port: 9001	Database Port: 9042
Messenger Port: 9092	Shutdown Port: 3029	Shutdown Port: 9000	
Coordinator Port: 2181			
Secure Storage Port: 8200			
Database Port: 5432			

You've installed the following module(s):

- Insite Web Server
 - Authority Broker
 - Automate
 - Automate Schedule
 - Crypto Complete
 - Deployment Manager
 - GoAnywhere MFT
 - HelpSystems Insite
 - Insite Analytics
 - Insite Integration
 - Insite Watch List
 - Intermapper
 - Password Self Help
 - Powertech Antivirus
 - Powertech Event Manager
 - Powertech Multi-Factor Authentication
 - Powertech Network Security
 - Robot Console
 - Robot Network
 - Robot Schedule
 - Vityl IT & Business Monitoring
- Insite Analytics Server
- Insite Integration Service
- Insite Watch List Coordinator Service
- Insite Watch List Collector Service
- Insite Authorization Service

Ready to install other required components on different systems?

Use the Insite installer to configure the other components on any other system(s). When you have the installer open, choose the "Multiple Install" option and enter the Insite Integration URL and API key below.

You will need to provide this URL when installing the other required components on other systems.

Insite Integration Service can be found at this URL:
http://Server2016-sysdev.com:8998

You will need your API Key to use Insite:
502b5f6f-c701-200c4efd90cc

Insite can be found at this URL:
http://Server2016.sysdev.com:3030

NOTE: If you will be installing other components on other servers, be sure to save the resulting **URL, API Key**, and port information from the summary screen. You will need this data to install other components on other servers. If you lose or forget this information, you can always find it on the **installer-summary.htm** file located in the Help Systems directory on your system. (example - C:\Program Files\Help Systems\HelpSystems\Insite)

After You Are Done

After installation of all components is complete, point a web browser to the following URL:

`http://xxx.xxx.xxx.xxx:nnnn/`

where *xxx.xxx.xxx.xxx* is the IP address of your server and *nnnn* is the connector port number you entered during installation.

If you have updated from an earlier Insite version, reload your browser to ensure all services are visible in the Products list.

If this is a new installation, the [Startup Wizard](#) will display to help you configure your installation of Insite. That will help you start setting up the software.

Installing or Updating Insite on Linux or Power Linux Servers

Installing Insite allows you to access your Fortra products through a web browser interface.

Currently, Insite allows you to access the following products:

- Automate BPA Server 10.5 or higher
- Automate Schedule 4.3 or higher
- Insite Analytics 1.0 or higher
- Insite Watch List 1.0 or higher
- Powertech Antivirus 5.0 or higher
- Powertech Event Manager 6.1 or higher
- Powertech Exit Point Manager for IBM i R7M04 or higher
- Powertech Multi-Factor Authentication 1.0 or higher
- Powertech Password Self Help 3.001 or higher
- Robot Console 7.03 or higher
- Robot Network 11.00 or higher
- Robot Reports 7.70 or higher
- Robot Schedule 10.30 or higher
- Vityl IT & Business Monitoring 1.0 or higher

Make sure your system meets the [minimum requirements](#) before installing or updating Insite on your Linux or Power Linux servers.

NOTE:

- You can download the installer from the customer portal. The installer is available whether you are requesting a free trial of our software, updating your software, or converting your software.
- The installer uses the default values for all ports (assuming none are already in use, in which case it decrements the port's value until an open port is found). You can manually override these port assignments.
- Before installing, be sure you are using the GNU Tar. That is the version supported by Insite.
- Root or sudo access is required in order to install.
- The ports that Insite uses must be open on all servers that Insite components will be installed. See [Ports and URLs Used by Insite](#) for a listing of these ports.
- If Insite is at 2.00 to 2.04, Insite will need to be updated to 2.08 prior to updating to 3.x or above. If you are running Insite 1.x, contact support for assistance on the upgrade process.
- If you are using Multifactor Authentication 1.4 or below with Insite, please contact Multifactor Authentication support for assistance on the upgrade process for both products.
- If you are using Multi-Factor Authentication, end it before updating Insite by ending the processes in this order: the Message Broker, the Database server, the Authentication Manager service. Contact support if needed.
- We always recommend backing up Insite before updating.
- When performing a multiple system installation, the installer needs to be run on each system.

You have two options when installing or updating Insite. You can choose to install Insite on a single system or multiple systems. The multiple systems option allows you to install components of Insite on multiple systems in a distributed environment. For example, you may want to install the [Insite Integration Service](#) and the Insite User Interface on separate servers. Because of the expanded footprint of Insite with the addition of Integration Services, installing on separate servers improves performance and allows for scalability in an enterprise level environment. Root or sudo access is required in order to install or update.

[Installing or Updating Insite on Your Linux Server - Single System](#)

[Installing or Updating Insite on Your Linux Server - Multiple Systems](#)

Installing or Updating Insite on Your Linux Server - Single System

Complete the following steps to download and install Insite on your Linux server. Root or sudo access is required in order to install.

1. Download the **insite_install.tgz** file to a temporary directory on your system (/tmp). The directory where you put **insite_install.tgz** must have read+execute (5) permissions for all.
2. Use the following command to extract the contents of the file:
tar -xzf insite_install.tgz
Extracted files will be put in a new directory named insite_install (/tmp/insite_install).
3. Use the following command to start the installer:
insite_install/serverInstall
4. The installer displays the actions it is going to perform, and asks for your permission to proceed.

NOTE: A user, 'helpsys' will be created to be used during the installation.

5. At the prompt, 'Would you like to perform a single system install?' enter **y** and press enter.
6. At the prompt, 'Would you like to install all Insite modules?' enter **y** to install all of the Insite modules. Enter **n** to choose the modules you would like from a list.
 - a. If choosing modules from the list, separate the numbers with spaces. Press enter to continue.
 - b. Enter **y** to confirm your selected modules or **n** to change your selection.

EXAMPLE:

```
Would you like to perform a single system install? [y]
Would you like to install all Insite modules? [y] n
Please select which Insite Web Server modules to install:
1 - Automate
2 - Automate Schedule
3 - Event Manager
5 - Insite Analytics
6 - Insite Watch List
7 - Powertech Antivirus
8 - Powertech Exit Point Manager
9 - Powertech Multi-Factor Authentication
10 - Powertech Password Self Help
11 - Robot Console
12 - Robot Network
13 - Robot Reports
14 - Robot Schedule
15 - Vityl IT & Business Monitoring
```

```
Please enter the number for all options you want installed
(1 2 3) (Then hit enter):1 2 3
You selected the following:
Automate
Automate Schedule
Event Manager

Is this correct? [y]
```

7. At the prompt, "Select the fully qualified domain name you would like to use for this server:' enter **1** to accept the domain name provided or **2** to enter a custom domain name.
8. The default port numbers for Insite Integration components are listed. To change these settings, enter **c** and press Enter. Or, enter **y** or press enter to begin the Insite Integration installation.
9. When the Insite Integration installer has completed, the **Integration Server url**, **Integration Server port**, and the **Integration Server API Key** appears. Make note of this data. You will need this data if you want to install Insite components on a different system in the future.
10. The default port numbers for Insite Core components are listed. To change these settings, enter **c** and press Enter. Or, enter **y** or press Enter to begin the Insite Core installation.
11. When the Insite Core installer has completed, it displays the URL to access Insite and a list of used ports. Ensure that those ports are open.

After You Are Done

After installation is complete, point a web browser to the following URL:

`http://xxx.xxx.xxx.xxx:nnnn/`

where `xxx.xxx.xxx.xxx` is the IP address of your server and `nnnn` is the connector port number you entered during installation.

If you have updated from an earlier Insite version, reload your browser to ensure all services are visible in the Products list.

If you are the first person to log in, you are asked to change the 'admin' password. Then, you will see the Server Settings page which has a Getting Started section on it. That will help you start setting up the software.

Installing or Updating Insite on Your Linux Server - Multiple Systems

Use the following procedure to install or update Insite Integration on the first system and all other Insite components, including Insite product modules, on the second system.

Root or sudo access is required in order to install.

NOTE: Before performing a multiple system install, ensure the following:

- Each system is on the same domain and able to resolve the hostname by DNS.
- Ports from the first system are opened prior to running the install on the second system.

On the first system:

1. Download the **insite_install.tgz** file to a temporary directory on your system (/tmp). The directory where you put **insite_install.tgz** must have read+execute (5) permissions for all.
2. Use the following command to extract the contents of the file:
tar -xzf insite_install.tgz
Extracted files will be put in a new directory named insite_install (/tmp/insite_install).
3. Use the following command to start the installer:
insite_install/serverInstall
4. The installer displays the actions it is going to perform, and asks for your permission to proceed.
5. At the prompt, 'Would you like to perform a single system install?' enter n and press enter.
6. At the prompt 'Please select which components to install' enter 1 for Insite Integration. Then enter y to confirm or n to change your selection.

```
Would you like to perform a single system install? [y] n
```

```
*****  
*****
```

```
Please select which components to install:
```

- ```
1 - Insite Integration
2 - Insite Web Server
3 - Insite WatchList Coordinator
4 - Insite WatchList Collector
```

```
5 - Insite Powertech Antivirus Insite Service
Please enter the number for all options you want installed (1 2
4 5) (Then hit enter):1
You selected the following:
 Insite Integration
Is this correct? [y]
```

**NOTE:** You could additionally select other components by entering their component numbers separated by spaces. Then enter y to confirm or n to change your selection.

If you have selected option 2 - Insite Web Server, in step 6, you will receive the prompt 'Would you like to install all Insite modules?' enter y to install all of the Insite modules. Enter n to choose the modules you would like from a list.

7. At the prompt, 'Select the fully qualified domain name you would like to use for this server:' enter 1 to accept the domain name provided or 2 to enter a custom domain name.
8. The default port numbers for Insite Integration components are listed. To change these settings, enter C and press Enter. Or, enter y or press enter to begin the Insite Integration installation
9. When the Insite Integration installer has completed, the **Integration Server url**, **Integration Server port**, and the **Integration Server API Key** will display. Make note of this data. You will need this data when installing on the other server in your multiple system setup. If you lose or forget this information, you can always find it on the **installer\_summary.txt** file located in the /opt/insite/ directory on your system with IIS installed.

On the second system:

1. Download the **insite\_install.tgz** file to a temporary directory on your system (/tmp). The directory where you put **insite\_install.tgz** must have read+execute (5) permissions for all.
2. Use the following command to extract the contents of the file:  
**tar -xzf insite\_install.tgz**  
Extracted files will be put in a new directory named insite\_install (/tmp/insite\_install).
3. Use the following command to start the installer:  
**insite\_install/serverInstall**
4. The installer displays the actions it is going to perform, and asks for your permission to proceed.

5. At the prompt, 'Would you like to perform a single system install?' enter n and press enter.
6. At the prompt 'Please select which components to install' choose 2 (and optionally 3, 4, and 5).

**NOTE:**

Insite Integration (1) only needs to be installed on the first system.

Enter y to confirm or n to change your selection.

```
Would you like to perform a single system install? [y] n
```

```

```

```

```

```
Please select which components to install:
```

- 1 - Insite Integration
- 2 - Insite Web Server
- 3 - Insite WatchList Coordinator
- 4 - Insite WatchList Collector
- 5 - Insite Powertech Antivirus Insite Service

```
Please enter the number for all options you want installed (1 2 4 5) (Then hit enter):2,3,4,5
```

```
You selected the following:
```

- Insite Web Server
- Insite WatchList Coordinator
- Insite WatchList Collector
- Insite Powertech Antivirus Insite Service

```
Is this correct? [y]
```

7. You will then be prompted, one at a time, to enter the domain name, port, and API key that you took note of earlier.
8. At the prompt, 'Would you like to install all Insite modules?' enter y to install all of the Insite modules. Enter n to choose the modules you would like from a list.
  - a. If choosing modules from the list, separate the numbers with spaces. Press enter to continue.
  - b. Enter y to confirm your selected modules or n to change your selection.

**EXAMPLE:**

```
Would you like to install all Insite modules? [y] n
```

```
Please select which Insite Web Server modules to install:
```

- 1 - Automate
- 2 - Automate Schedule

```

4 - Event Manager
5 - Insite Analytics
6 - Insite Watch List
7 - Powertech Antivirus
8 - Powertech Exit Point Manager
9 - Powertech Multi-Factor Authentication
10 - Powertech Password Self Help
11 - Robot Console
12 - Robot Network
13 - Robot Reports
14 - Robot Schedule
15 - Vityl IT & Business Monitoring

```

```

Please enter the number for all options you want installed
(1 2) (Then hit enter):1 2
You selected the following:
Automate
Automate Schedule

Is this correct? [y]

```

9. At the prompt, 'Select the fully qualified domain name you would like to use for this server:' enter 1 to accept the domain name provided or 2 to enter a custom domain name.
10. The default port numbers for selected components are listed. To change these settings, enter C and press Enter. Or, enter y or press enter to begin the installation
11. When the Insite Installer is complete, it displays the url to access Insite.

## After You Are Done

After installation is complete, point a web browser to the following URL:

**`http://xxx.xxx.xxx.xxx:nnnn/`**

where `xxx.xxx.xxx.xxx` is the IP address of your server and `nnnn` is the connector port number you entered during installation.

If you have updated from an earlier Insite version, reload your browser to ensure all services are visible in the Products list.

If you are the first person to log in, you are asked to change the 'admin' password. Then, you will see the Server Settings page which has a Getting Started section on it. That will help you start setting up the software.

# Insite Integration Service

The Insite Integration Service improves data flow and security in Insites by providing secure communication channels using TLS certificates for the following products:

- Insite services
- Insite Watch List
- Powertech Antivirus

These TLS channels provides transmission of requests/events that is secured and encrypted, optimizing Insite security on an enterprise level. The inclusion of Insite Integration Services today to your Insite installation provides the future capability to adapt these secure communication channels to all of your product connections. **The goal:** fast, reliable communications without web servers and a universally secure Fortra product line within Insite.

Important usability changes in Insite introduced with Insite Integration Services:

- **Multiple System installation** - Installation has been updated and improved to allow you to install Insite on two separate servers if desired. Because of the expanded footprint of Insite with the addition of Insite Integration Services, installing on separate servers will improve performance and allow for scalability in an enterprise level environment.
- **Product Instances** - The Product Instances page lists all products that are connected to your installation of Insite. The list is made up of two types of objects: legacy Product Connections, which you can also view and edit on the Product Connections page, and Product Instances, which are instances of Insite's new and more streamlined way to connect and communicate with an installed product. You cannot add a Product Instance, as they are added upon installation of compatible products, but you can view and edit properties and remove them. Be aware that within the Product Instance list you can add, edit, and remove legacy Product Connections as well.
- **Integration Service Administration** - The Integration Service Administration page is only accessible to a user with Integration Service administrative permissions. It allows you to copy the API key, enable/disable the API key, and Regenerate the API key needed for TLS authentication.

## Important Notes

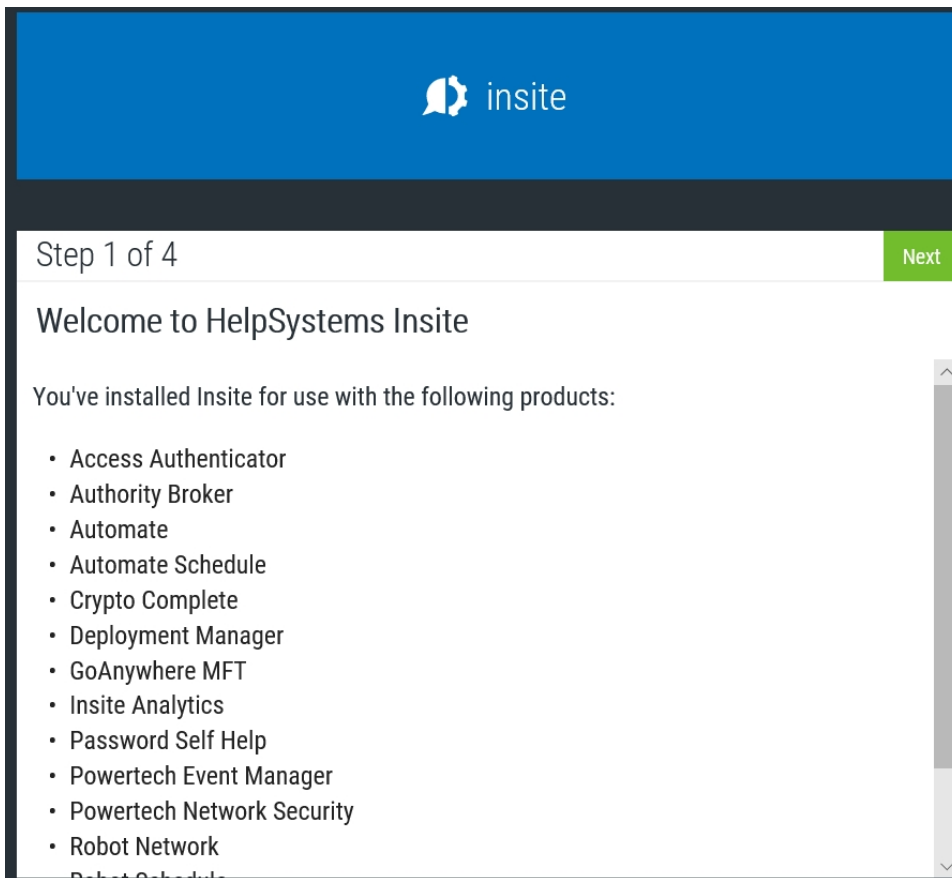
- Currently, only the product modules referenced above are using Insite Integration Services and are displayed as Product Instances within Insite. Future releases of Insite will introduce more products to this list.
- When installing Insite, it is recommended to do a multiple system install on two systems to take advantage of the performance benefits inherent in the multi-system approach.
- Product instances outside of Insite, including Insite Watch List and Powertech Antivirus, are not automatically allowed. You must allow them within the Product Instances screen before you can use these products within Insite.

# Startup Wizard

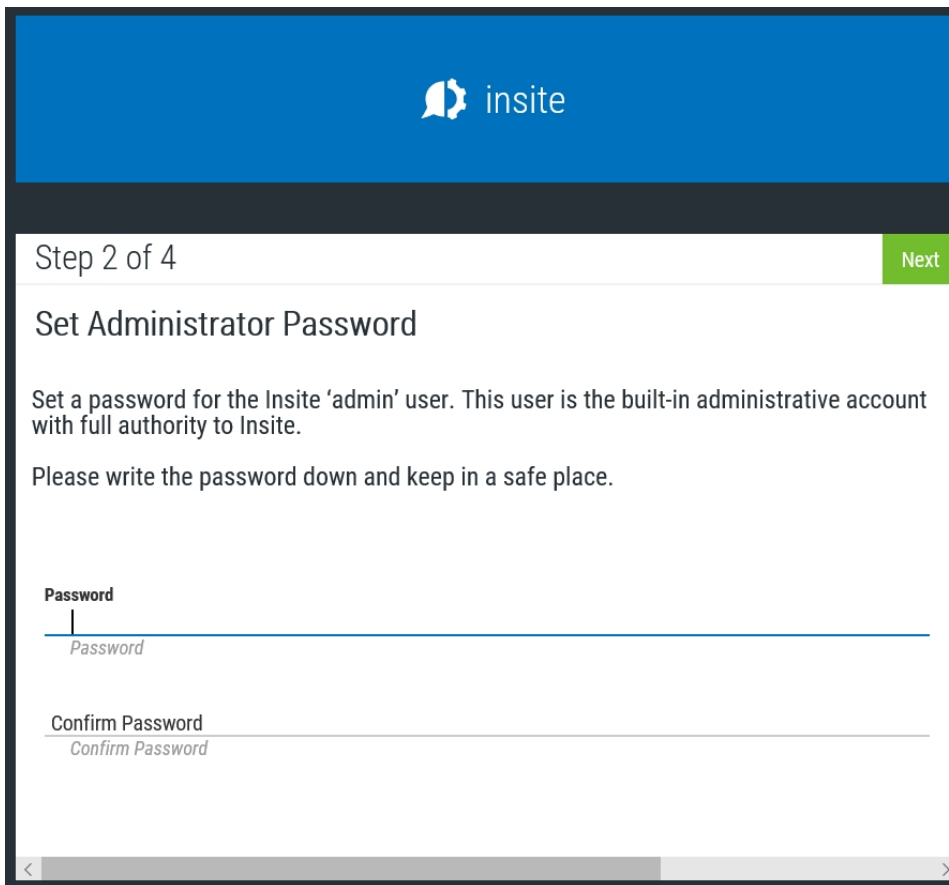
The Insite Startup Wizard displays after a successful initial installation to guide you through Insite's basic configuration steps. The wizard will help you complete these steps to ensure that you are immediately ready to enjoy the benefits of Insite.

To navigate through the wizard:

1. The **Getting Started** step displays the products you had chosen to install. Click **Next** to proceed to the next step.



2. The **Admin Password** step allows you to create a password for build-in 'Admin' user. This administrator account has full authority to Insite. Ensure that you enter a strong password. Click **Next** to continue.



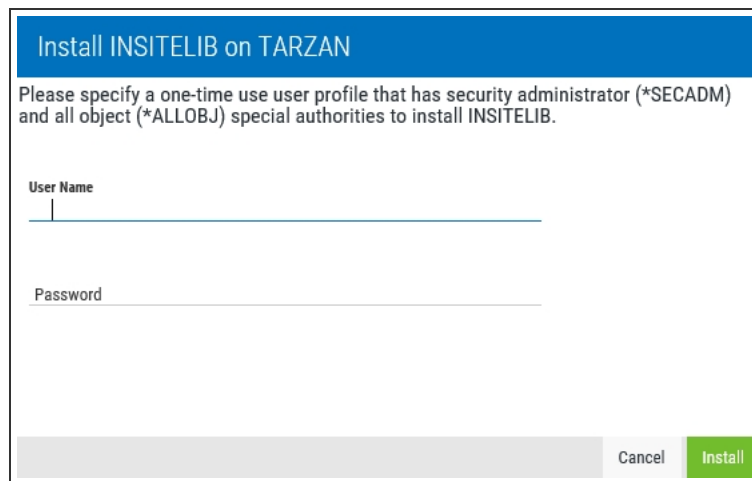
The screenshot shows a web-based wizard interface for Insite. At the top, there is a blue header with the Insite logo. Below the header, the page is titled "Step 2 of 4" with a "Next" button. The main heading is "Set Administrator Password". The instructions state: "Set a password for the Insite 'admin' user. This user is the built-in administrative account with full authority to Insite. Please write the password down and keep in a safe place." There are two input fields: "Password" and "Confirm Password", both with placeholder text "Password" and "Confirm Password" respectively. A scrollbar is visible at the bottom of the form area.

3. The **Connections** step allows you to setup an initial product connection for one of the products you chose to install. See [Adding a new Product Connection](#) for instructions on how to fill out this form for your selected product.

#### IBM i connection considerations:

- New library 'INSITELIB' will be added to all IBM i systems that Insite is connected to. Upon initial IBM i connection creation, you will be required to provide a login with security administrator (\*SECADM) permissions and all object (\*ALLOBJ) special authorities, but this login will not be saved. It will only serve to allow Insite to install the INSITELIB library.





**Install INSITELIB on TARZAN**

Please specify a one-time use user profile that has security administrator (\*SECADM) and all object (\*ALLOBJ) special authorities to install INSITELIB.

User Name

Password

Cancel Install

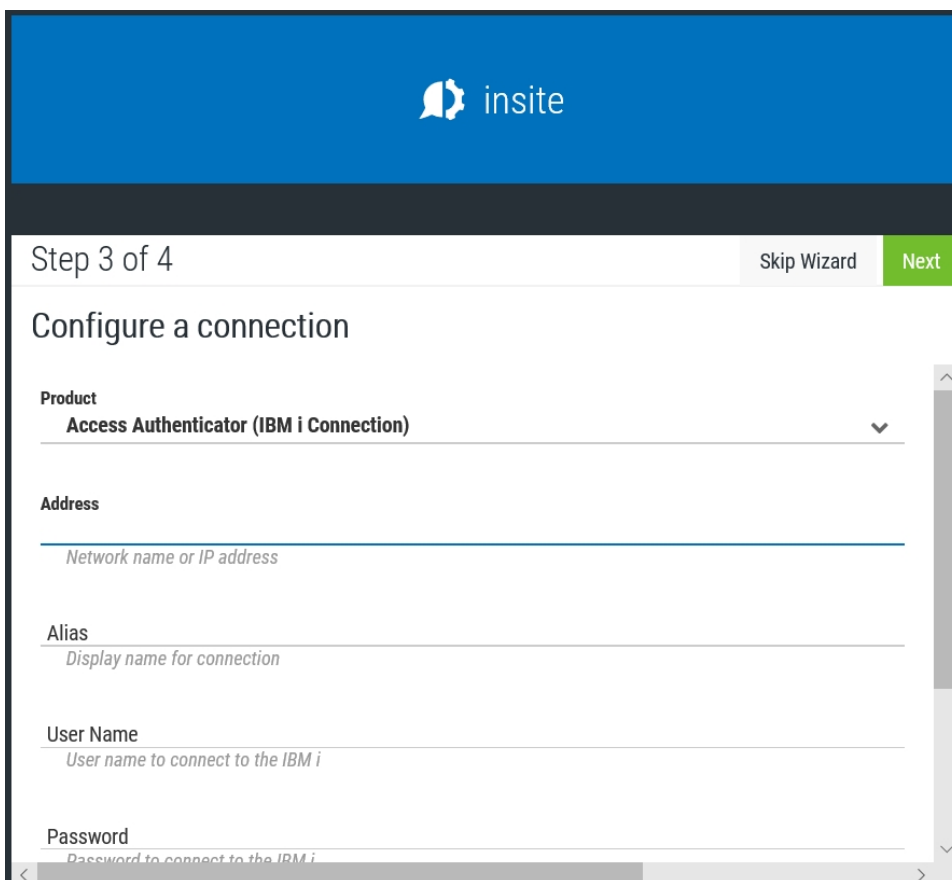
- Two new users will be added as well:  
INSITEUSR and INSITEADM - These users function similarly to how RBTADMIN, PTADMIN and RBTUSER, PTUSER behave upon installation of Robot and Powertech products. They are designed to own all connected product objects so that you are not required to create a profile in Insite with \*SECOFR permissions to interact with your IBM i.
- If necessary, you can fix the installation of INSITELIB through the Product Connections view or the Alerts view.

**NOTE:** For Network Security users, in order to have \*USER on the profile connection and use Powertech products, the profile with the connection MUST be added to the PTADMIN authorization list.

**NOTE:** IBM i systems that will be connecting to your Insite Server must be at V7R2 or higher.

When finished, click **Next** to continue.

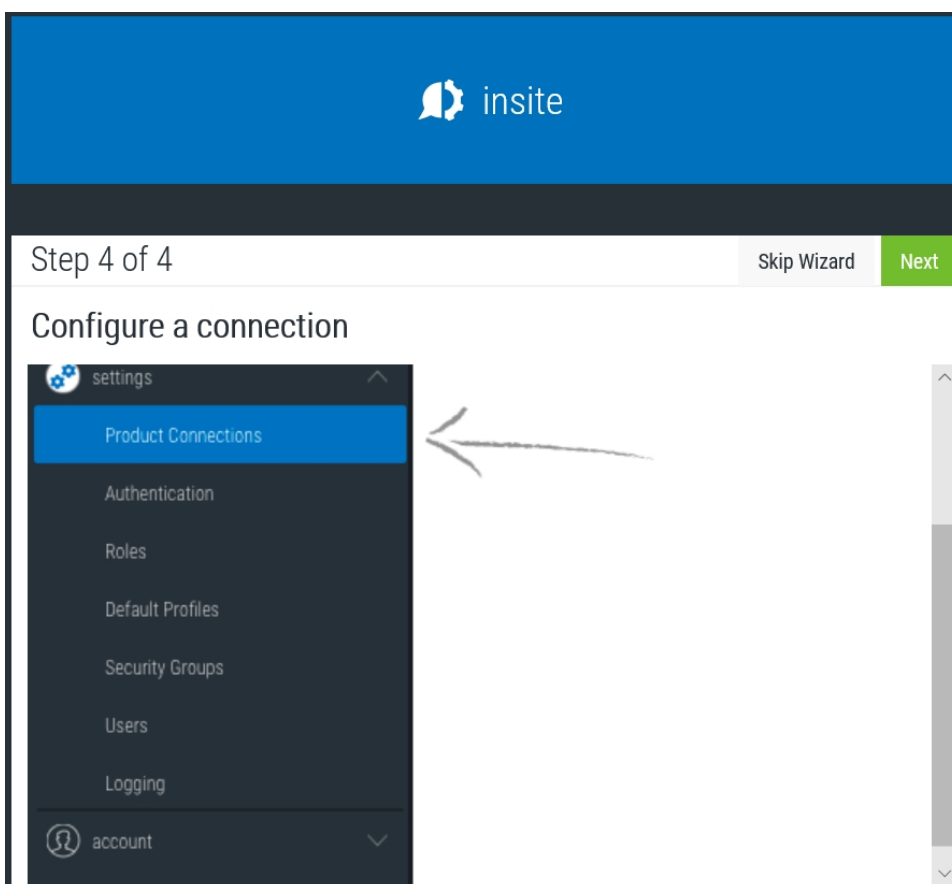
**NOTE:** You can click the **Skip Wizard** button to exit the Startup Wizard and enter Insite.



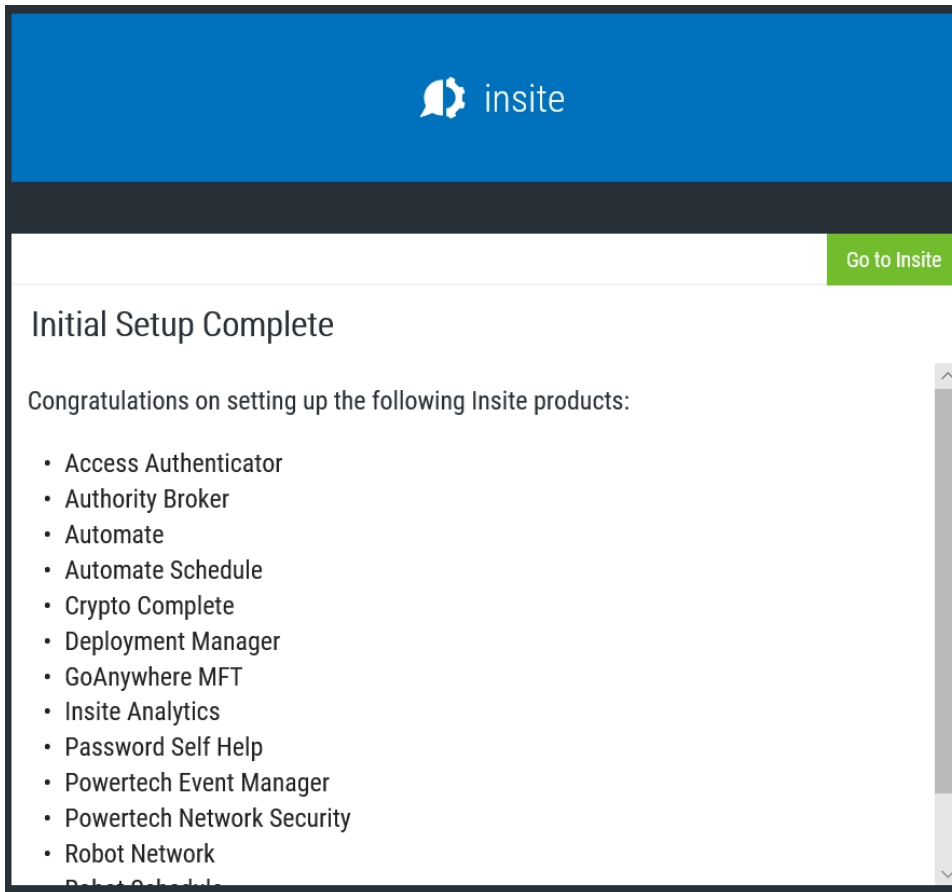
The screenshot shows the 'Configure a connection' step of the Insite Startup Wizard. The interface features a blue header with the 'insite' logo. Below the header, the progress is indicated as 'Step 3 of 4'. Two buttons are present: 'Skip Wizard' and 'Next'. The main content area contains several form fields: a dropdown menu for 'Product' set to 'Access Authenticator (IBM i Connection)', an 'Address' field with the placeholder 'Network name or IP address', an 'Alias' field with the placeholder 'Display name for connection', a 'User Name' field with the placeholder 'User name to connect to the IBM i', and a 'Password' field with the placeholder 'Password to connect to the IBM i'. A vertical scrollbar is visible on the right side of the form area.

4. The **Connections** step continues with an image showing you where in the Insite menu you can find the Product Connections screen to add more product connections. Click **Next** to continue.

**NOTE:** You can click the **Skip Wizard** button to exit the Startup Wizard and enter Insite.



5. The initial setup is complete. Click **Go to Insite** to enter Insite and begin working.



The screenshot shows a web interface for the Insite startup wizard. At the top, there is a blue header with the Insite logo and the word "insite" in white. Below the header is a dark grey bar with a green button labeled "Go to Insite". The main content area has a white background and features the heading "Initial Setup Complete". Below this heading, there is a message: "Congratulations on setting up the following Insite products:". This is followed by a bulleted list of products: Access Authenticator, Authority Broker, Automate, Automate Schedule, Crypto Complete, Deployment Manager, GoAnywhere MFT, Insite Analytics, Password Self Help, Powertech Event Manager, Powertech Network Security, and Robot Network. A vertical scrollbar is visible on the right side of the list.

insite

Go to Insite

## Initial Setup Complete

Congratulations on setting up the following Insite products:

- Access Authenticator
- Authority Broker
- Automate
- Automate Schedule
- Crypto Complete
- Deployment Manager
- GoAnywhere MFT
- Insite Analytics
- Password Self Help
- Powertech Event Manager
- Powertech Network Security
- Robot Network

# Adding a New Product Connection

In order to use the Insite modules, you must connect Insite to one or more of your systems. For a list of the available modules, see [Welcome to Insite](#).

**TIP:** You can import a list of IBM i connections from a CSV file. For details, see [Importing IBM i Product Connections](#)

**NOTE:** In order to use TLS security to encrypt an IBM i Product Connection you must first configure a digital certificate, which contains the server's public encryption key. See [Securing an IBM i Product Connection](#).

Follow these steps to define a connection:

1. In the Navigation Panel, click **Settings**.
2. Click **Products**.
3. Click **Add**.
4. Select a **Connection Type**.
5. **If you chose an Automate Enterprise server connection:**

- a. Enter the IP **Address** (or network name) of the Automate Enterprise server you want to connect to.

**New Product Connection** help ?

Cancel Save

**Connection Type**  
Automate

**Address**  
*Network name or IP address*

**Port**  
9608

**Alias**  
*Display name for connection*

**User Name for Guest Access:**  
*User name to connect to Automate when a guest*

**Password for Guest Access**  
*Password to connect to Automate when a guest*

**Confirm Password**  
*Confirm the password*

- b. Enter the **Port** number for the server.
- c. Enter an **Alias** for the server. This is what displays throughout Insite.
- d. Enter a **User Name for Guest Access** and **Password for Guest Access** (and **Confirm Password**) for a user who would log on as a guest on the system you entered above.

**NOTE:** You will not necessarily log on to Insite as this user (unless you choose to). This is just the user that allows the connection to be made to the Automate Enterprise server.

## 6. If you chose an Automate Schedule server connection:

- a. Enter the IP **Address** (or network name) of the Automate Schedule server you want to connect to.

Cancel Save

**Connection Type**  
**Automate Schedule** ⌵

---

**Address**  
  
*Network name or IP address*

**Port**  
**8008**

---

**Alias**  
  
*Display name for connection*

**User Name**  
  
*User name to connect to Automate Schedule*

**Password**  
  
*Password to connect to Automate Schedule*

**Confirm Password**  
  
*Confirm the password*

**Database Port**  
**7432**

---

**Database User Name**  
  
*User name to connect to Automate Schedule database*

**Database Password**  
  
*Password to connect to Automate Schedule database*

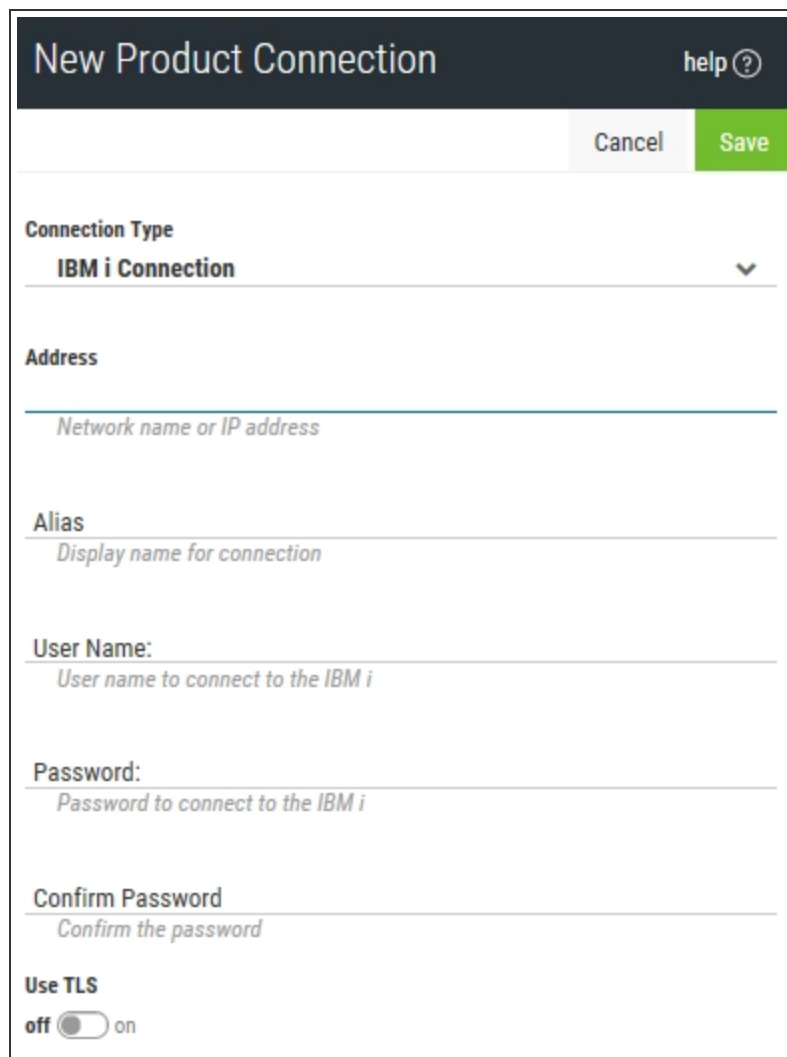
**Confirm Database Password**  
  
*Confirm the database password*

**Use HTTPS**  
off  on

- b. Enter the **Port** number for the server.
- c. Enter an **Alias** for the server. This is what displays throughout Insite.
- d. Enter a **User Name** and **Password** (and **Confirm Password**) for the user of the system you entered above.
- e. Enter the **Database Port** number.
- f. Enter a **User Name** and **Password** (and **Confirm Password**) for the database user of the database you entered above.
- g. Toggle **Use HTTPS** to 'on' to use a secure connection, or leave 'off' to use HTTP.

7. If you chose an **IBM i** connection:

- a. Enter the **IP Address** (or network name) of the IBM i system you want to connect to.



The screenshot shows a dialog box titled "New Product Connection" with a "help" icon in the top right corner. Below the title bar are "Cancel" and "Save" buttons. The main content area contains the following fields and controls:

- Connection Type:** A dropdown menu currently set to "IBM i Connection".
- Address:** A text input field with the placeholder text "Network name or IP address".
- Alias:** A text input field with the placeholder text "Display name for connection".
- User Name:** A text input field with the placeholder text "User name to connect to the IBM i".
- Password:** A text input field with the placeholder text "Password to connect to the IBM i".
- Confirm Password:** A text input field with the placeholder text "Confirm the password".
- Use TLS:** A toggle switch currently set to "off".



- b. Enter an **Alias** for the IBM i system. This is what displays throughout Insite.
- c. Enter the **User Name** and **Password** (and **Confirm Password**) for a user on the system you entered above.

**NOTE:** See the **IBM i connection considerations** section below.

- d. Toggle **Use TLS** to 'on' to use TLS security to encrypt the connection.

### IBM i connection considerations:

- New library 'INSITELIB' will be added to all IBM i systems that Insite is connected to. Upon initial IBM i connection creation, you will be required to provide a login with security administrator (\*SECADM) permissions and all object (\*ALLOBJ) special authorities, but this login will not be saved. It will only serve to allow Insite to install the INSITELIB library.

Install INSITELIB on TARZAN

Please specify a one-time use user profile that has security administrator (\*SECADM) and all object (\*ALLOBJ) special authorities to install INSITELIB.

User Name

Password

Cancel Install

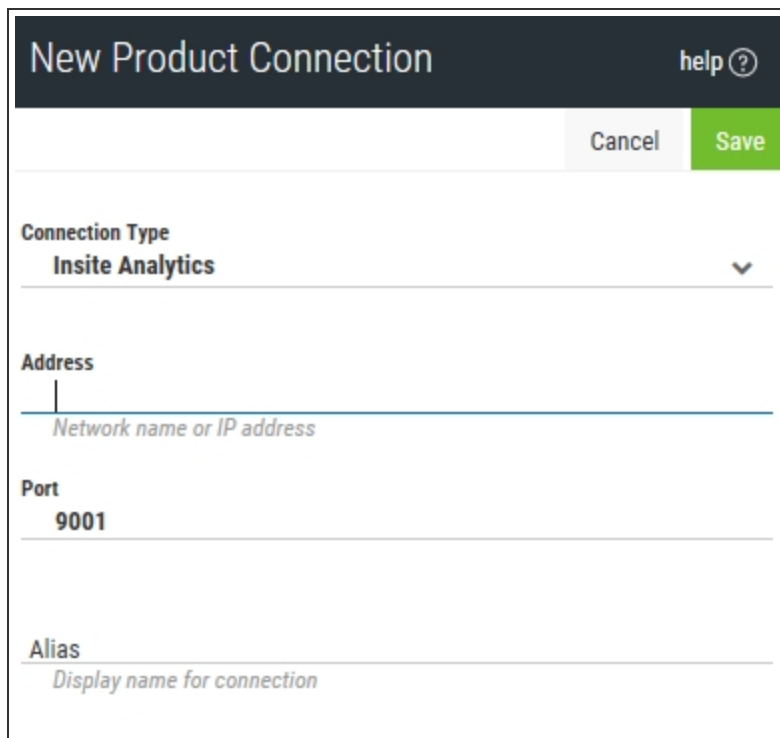
- Two new users will be added as well:
  - INSITEUSR and INSITEADM - These users function similarly to how RBTADMIN, PTADMIN and RBTUSER, PTUSER behave upon installation of Robot and Powertech products. They are designed to own all connected product objects so that you are not required to create a profile in Insite with \*SECOFR permissions to interact with your IBM i.
- If necessary, you can fix the installation of INSITELIB through the Product Connections view or the Alerts view.

**NOTE:** For Powertech Network Security users, in order to have \*USER on the profile connection and use Powertech products, the profile with the connection **MUST** be added to the PTADMIN authorization list.

**NOTE:** IBM i systems that will be connecting to your Insite Server must be at V7R2 or higher.

8. If you chose an Insite Analytics connection:

- a. Enter the IP **Address** (or network name) of the Insite Analytics system you want to connect to.



The screenshot shows a dialog box titled "New Product Connection" with a "help ?" icon in the top right corner. Below the title bar are "Cancel" and "Save" buttons. The form contains the following fields:

- Connection Type:** A dropdown menu with "Insite Analytics" selected and a downward arrow.
- Address:** A text input field with a vertical cursor. Below the field is the placeholder text "Network name or IP address".
- Port:** A text input field containing the value "9001".
- Alias:** A text input field with the placeholder text "Display name for connection".

- b. Enter a **Port** number.
- c. Enter an **Alias** for the Insite Analytics system. This is what displays throughout Insite.

9. If you chose a Powertech Event Manager connection:

- a. Enter the IP **Address** (or network name) of the Powertech Event Manager system you want to connect to.

The screenshot shows a 'New Product Connection' dialog box. At the top, there is a dark header with the title 'New Product Connection' and a 'help ?' icon. Below the header, there are two buttons: 'Cancel' and 'Save'. The main content area is divided into three sections. The first section is 'Connection Type' with a dropdown menu showing 'Powertech Event Manager'. The second section is 'Address' with a red error message 'This value is required.' below the input field. The third section is 'Port' with the value '19180' entered. The fourth section is 'Alias' with the value 'Powertech Event Manager' and a subtitle 'Display name for connection'.

- b. Enter a **Port** number.
- c. Enter an **Alias** for the Powertech Event Manager system. This is what displays throughout Insite.

10. If you chose a Vityl IT & Business Monitoring connection:

- a. Enter the IP **Address** (or network name) of the Vityl IT & Business Monitoring system you want to connect to.

The screenshot shows a 'New Product Connection' dialog box. At the top, there is a title bar with the text 'New Product Connection' and a 'help ?' icon. Below the title bar, there are two buttons: 'Cancel' and 'Save'. The main area of the dialog contains four input fields:

- Connection Type**: A dropdown menu with the selected value 'Vityl IT & Business Monitoring' and a downward arrow.
- Address**: A text input field with the placeholder text 'Network name or IP address'.
- Port**: A text input field with the value '19180'.
- Alias**: A text input field with the value 'Vityl IT & Business Monitoring' and the placeholder text 'Display name for connection'.

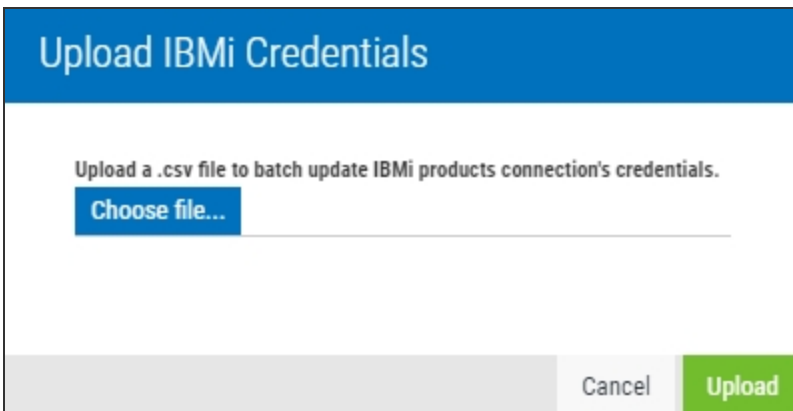
- b. Enter a **Port** number.
  - c. Enter an **Alias** for the Vityl IT & Business Monitoring system. This is what displays throughout Insite
11. If you are configuring an IBM i connection, turn Use TLS on to use TLS security to encrypt the connection. If you do this, you will first need to have configured a Certificate. See [Securing an IBM i Product Connection](#) for details.
  12. Click **Save**.

# Importing IBM i Product Connections

You can create IBM i product connections by importing the details, including the credentials, from a CSV file.

Follow these steps to import IBM i product connections:

1. In the Navigation Panel, click **Settings**.
2. Click **Products**.
3. Click **Upload IBMiConnections** in the upper right corner.
4. Click **Upload IBMi Connections** in the upper right corner.
5. Click **Choose file....** Select the .csv file to import.



**NOTE:**

The .csv file must have the following information in it: address, alias, user name (for general connection), password (for general connection), user name (for INSITELIB updates), password (for INSITELIB updates).

You do not need header information in the .csv file. Use one row for each IBM server. Each piece of information should be in a separate cell.

6. Click **Upload**.

# Securing an IBM i Product Connection

In order to use TLS security to encrypt an IBM i Product Connection from Insite, you must create and configure a Digital Certificate (also called a *Certificate Authority*). To do so requires the following steps:

- **Create a Certificate.** Use IBM's Digital Certificate Manager to create the Certificate.
- **Export the Certificate.** Export the Certificate from the Digital Certificate Manager.
- **Import the Certificate.** Import the Certificate into your Java Runtime Environment.

## Creating a Certificate

1. Open the Digital Certificate Manager by going to `http://your server name:2001/QIBM/ICSS/Cert/admin/qycucm1.ndm/main0`.

### EXAMPLE:

`http://myservername:2001/QIBM/ICSS/Cert/admin/qycucm1.ndm/main0`

### NOTE:

To open this URL, the http server must be running on your IBM i system. To start the http server, use the following command:

```
STRTCPSVR SERVER(*HTTP) HTTPSVR(*admin)
```

2. Click **Create a Certificate Authority (CA)** on the left side menu.
3. Enter the requested information and click **Continue**.
4. For 'Install Local CA Certificate,' review the text and click **Continue**.
5. For 'Certificate Authority (CA) Policy Data,' verify information and click **Continue**.
6. On the 'Policy Data Accepted' screen, click **Continue** again.
7. On the Create a Server or Client Certificate screen, you are prompted to create the Certificate store \*SYSTEM. Enter the requested information and click **Continue**.
8. Select applications that should trust the Certificate Authority and click **Continue**.
9. Continue to create an Object Signing Certificate if desired (not required).

## Exporting the Certificate from the Digital Certificate Manager

1. Open the Digital Certificate Manager by going to `http://your server name:2001/QIBM/ICSS/Cert/admin/qycucm1.ndm/main0`.
2. Click **Select Certificate Store**.
3. Select **\*SYSTEM** and click **Continue**.
4. Enter the Certificate store password and click **Continue**.
5. Select **Manage Certificate** on the left, and then **Export Certificate**.
6. Select **Certificate Authority**, then click **Continue**.
7. Select the Certificate Authority you created and click **Export**.
8. Select File and click **Continue**.
9. Enter a file path for the IBM i IFS and click **Continue**.
10. Download the file from the IBM i onto the system running Insite (e.g. via FTP).
  - a. Using a command prompt, open an FTP connection to the IBM i system using 'ftp systemname' (cmd (Windows) or bash/shell (Linux)).
  - b. Enter credentials to login if prompted.
  - c. Once logged in, enter `quote site namefmt 1`.
  - d. To copy the file, enter `GET /path/to/file/system.crt`. The file will be copied to the folder you are in within the command prompt.

## Importing the Certificate Authority into Java Runtime Environment (Windows)

1. Open a command prompt in java 'bin' folder.
 

```
cd "c:\Program Files (x86)\Help Systems\HelpSystems
Insite\jvm\bin"
```
2. Run
 

```
keytool -import -alias Server Alias -file Certificate
Path -keystore Keystore Path
```

### EXAMPLE:

```
keytool -import -alias HS55 -file
c:\helpsys\insitecert_HS55 -keystore "C:\Program Files
(x86)\Help Systems\HelpSystems
Insite\jvm\lib\security\cacerts"
```

3. Enter the keystore password, "changeit" by default.
4. Type `yes` and press **Enter**.
5. Restart the Insite server

After completing these steps, see [Adding a New Product Connection](#) in order to add a new connection in Insite.

**NOTE:** For more information regarding the IBM Digital Certificate Manager, see [Digital Certificate Manager \(DCM\) - Frequently Asked Questions and Common Tasks](#).



# Authentication

The Authentication page is only accessible to a user with administrative permissions. It allows you to set the session timeout, define the authentication method, and enable guest logins.

**Getting There:** In the Navigation Panel, click **Authentication** under Settings. If the menu is hidden, click .

You can do the following:

## Set the session timeout limit

You can set the number of minutes a session can remain inactive before timing out.

**NOTE:** If the timeout limit set here is greater than what a user sets for the auto-refresh intervals for dashboard widgets or in their preferences (for items such as Schedule Activity or the Status Center), it will prevent the user's session from timing out if they are on one of those pages.

## Select the authentication method you want to use and set it up

Before any of your users can log on to Insite, you must specify how to authenticate users. If authentication is not set up or the authentication server is down, only the 'Admin' user will be able to log in to Insite.

## Enable a guest login

A guest profile allows you to give people access to the dashboards that are marked as Guest. The Guest profile is for people who normally do not log onto the product and who may not even have an IBM i, Automate Enterprise server, or Webdocs IBM i profile. Guest users can only access the Dashboard area and view only those dashboards designated as Guest. They cannot access any other part of Insite, see any other dashboards, or make any changes.

The default Guest profile credentials are: User Name = guest, Password = guest. However, you can change it, if necessary. All guests use the same guest profile.

To complete the above tasks:

1. In the Navigation Panel, click **Authentication** under Settings. If the menu is hidden, click .

2. Enter the **Session Timeout** in minutes.

**NOTE:** If the timeout limit set here is greater than what a user sets for the auto-refresh intervals for dashboard widgets or in their preferences (for items such as Automate Activity, Schedule Activity, or the Status Center), it will prevent the user's session from timing out if they are on one of those pages.

3. Click in the authentication method field and select **LDAP**, **IBM i**, **Automate**, or **Webdocs for i**.

If you chose **LDAP**:

- a. Enter the name or address of the **LDAP Host** server.

**NOTE:**

- These settings are specific to the Insite module, and do not pertain to Multi-Factor Authentication's LDAP settings configured on Access Authenticator's LDAP Settings page.
- LDAP authentication can be used with Active Directory.

Select the method of authentication you want to use:

LDAP Host:

LDAP Port:

Use SSL with LDAP:  Off

LDAP Administrator:

Administrator Password:

Confirm Password:

Default Context:

User ID Field Name:

LDAP Field to Match:

- b. Enter the **LDAP Port** used by the LDAP server.
- c. Switch **Use SSL with LDAP** to On if a secure sockets layer (SSL) is used with your LDAP server. You must first import the root certificate from the LDAP Host.

### To import the root certificate from the LDAP Host:

1. Get the CA certificate from the LDAP host you want to connect to and move it to your Insite machine file system.
2. Import the certificate into javas cacert.

- Run (Windows)

```
keytool -import -alias Server Alias -file Certificate Path -keystore Keystore Path
```

**EXAMPLE:**

```
C:\Program Files (x86)\Help
Systems\HelpSystems
Insite\jvm\bin\keytool -import -
file c:\PATHTOCERT\insitecert.cert
-keystore "C:\Program Files
(x86)\Help Systems\HelpSystems
Insite\jvm\lib\security\cacerts"
```

- Run (Linux)

**EXAMPLE:**

```
/opt/insite/jvm/bin/keytool -import
-file /PATHTOCERT.insitecert.cert -
keystore
"/opt/insite/jvm/lib/security/cacerts"
```

3. Enter the keystore password, "changeit" by default.

**NOTE:** The default password for cacerts is "changeit". You should consider changing this for security reasons.

4. Type yes and press Enter.
5. Restart the Insite Server service.

- d. Enter the name of your **LDAP Administrator**. This administrator must be able to read the LDAP tree.

**NOTE:** Distinguished Name format is acceptable. For more on Distinguished Names, go to the [Microsoft Developer Network website](#).

- e. Enter the **Administrator Password** (and **Confirm Password**) for the administrator you entered above.
- f. Enter the **Default Context** for the LDAP server. This is the location to search for users in Distinguished Name format.
- g. Enter the **User ID Field Name** for the LDAP server. This is the Attribute Name to search in for the username.
- h. Enter the **LDAP Field to Match**. This is the value that matches the "samaccountname" listed for the user on the LDAP server.

- i. Click **Validate LDAP Connection** to test the information you entered above.

### If you chose IBM i:

- a. Enter the name or **Address** of the IBM i server you want to use for authentication.

**NOTE:** This does not have to be one of the IBM i systems that you are connecting Insite to.

Select the method of authentication you want to use: IBM i

Address:

Alias:

Port:

- b. Enter an **Alias** for the server you specified above.

**NOTE:** The alias you enter here is displayed on the Log In page as the server that is providing authentication.

- c. Enter the **Port** the server uses.

4. To enable guest logins and define the guest profile:

- a. Click **On** to Allow Guest Login. Click **Off** to disable it.

Allow Guest Login:  On

Guest User Name:

Guest Password:

Confirm Guest Password:

- b. Enter the **Guest User Name**. The default is 'Guest'.
- c. Enter the **Guest Password**. Enter it again to confirm it. The default is 'guest'.

5. Click **Save**.

## Auto Login

If authentication has been successfully set up on your Insite server, you can use the Auto Login feature to provide access to users with non-interactive computers. To use Auto Login:

1. Identify the user name and password you would like to use for this feature. You can use the guest login or specify a particular user.

**NOTE:** Use caution when selecting the user. Ensure that the user name only has authority to the parts of Insite you would like. Use Roles to set authority.

2. Identify the route to the specific Insite page for which you would like to provide access. Everything after the # in your Insite URL is considered the route. The route is bolded in the example below.

**EXAMPLE:**

`http://xx.xx.xx.xx:3030/HelpSystems/#HelpSystems/ AdvDashboard/ 2`

3. Provide the link to those who need access. The link format is as follows:

**`http://Insite IP Address:port/HelpSystems/#Login/ {user name}/ {password}/ {route}`**


**EXAMPLE:**

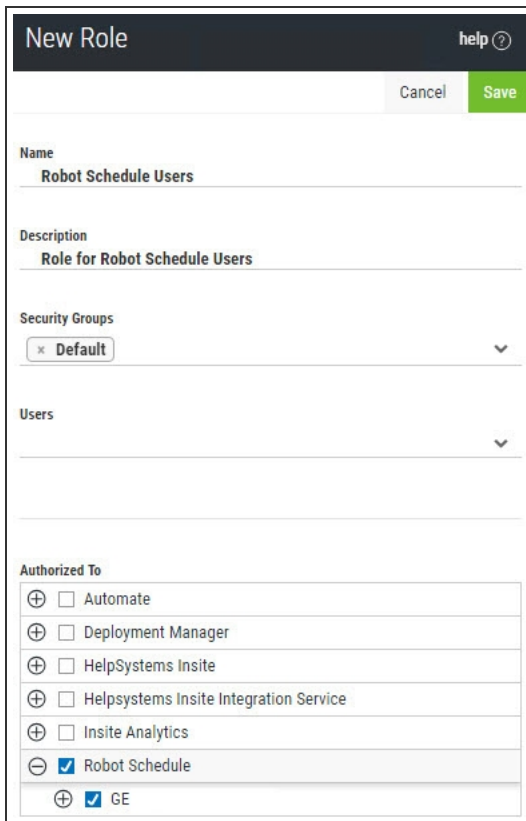
`http://  
xx.xx.xx.xx  
:3030/HelpSystems/#Login/ Guest/ GuestPswd/HelpSystems/ AdvDashboard/2`

# Adding a Role

To ensure your users only access the areas of Insite they are authorized to, you can create and assign them to roles.

Follow these steps to create a role:

1. In the Navigation Panel, click **Roles** under Settings. If the menu is hidden, click .
2. Click **Add**.



The screenshot shows the 'New Role' configuration window. The 'Name' field is filled with 'Robot Schedule Users'. The 'Description' field contains 'Role for Robot Schedule Users'. Under 'Security Groups', the 'Default' group is selected. The 'Authorized To' section lists several permissions, with 'Robot Schedule' and 'GE' checked. The 'Save' button is highlighted in green.

3. Enter a **Name** for the role you want to create.
4. Enter a **Description** for the role.
5. Select any security groups you want to add the role to. For example, if you create a role with permissions to the Robot Schedule production system (like in the image above), you could add a security group for all Robot Schedule users to it.

**NOTE:** If you haven't created any security groups yet, see Security Groups.

6. If you want to add users to the role (outside of users who are assigned to any security groups this role is a part of, as they will get this role's permissions automatically), type their username into the field or select them drop the drop-down.
7. Click the products and areas of Insite you want to apply to this role. The current products and areas available are the following:

### Multi-Factor Authentication

These are the areas of the product that can be chosen when defining a role.

- Agents
- Managers
- Product Settings
- Reports
- Users and Groups

### Automate

These are the areas of the product that can be chosen when defining a role.

- Insite - Automate Licensing

### Deployment Manager

These are the areas of the product that can be chosen when defining a role.

- Enterprise License Agreement
- <active product connections>
  - Licensing Products
  - Installing Products

### Insite

These are the areas of the product that can be chosen when defining a role.

- Authentication
- Dashboards
- Logging
- Product Connections
- Role Based Security

### Insite Integration Service

These are the areas of the product that can be chosen when defining a role.

- Change and Remove Product Instances
- Enable Disable Healthcheck
- Renew Certificates



- View All Product Instances
- Allowed and Blocked Products

### Insite Analytics

These are the areas of the product that can be chosen when defining a role.

- Data Connections
- Licensing
- Query Builder

### Password Self Help

These are the areas of the product that can be chosen when defining a role.

- All Product Functions

### Powertech Event Manager

These are the areas of the product that can be chosen when defining a role.

- Event Analysis

### Powertech Network Security

These are the areas of the product that can be chosen when defining a role.

- <active product connections>
  - All Product Functions

### Robot Network

These are the areas of the product that can be chosen when defining a role.

- <active product connections>
  - All Product Functions

### Robot Schedule

These are the areas of the product that can be chosen when defining a role.

- <active product connections>
  - All Product Functions

### Vityl IT & Business Monitoring

These are the areas of the product that can be chosen when defining a role.

- All Product Functions

**NOTE:** Some products will only display in the **Authorized To** list if there is an active Product Connection.


8. Click **Save**.

When you are finished, the new role will show up on the Roles page.

# Adding a Default Profile

Default profiles allow you to connect to a role or system without needing to create a user. This is useful in the event that someone on your team cannot be validated through LDAP or an IBM i connection but still needs access to the various areas in Insite.

Follow these steps to create a default profile:

1. In the Navigation Panel, click **Default Profiles** under Settings. If the menu is hidden, click .
2. Click **Add**.
3. Enter a name for the default profile you want to create.
4. Enter a user name.
5. Enter a password. Confirm the password.
6. Click **Save**.

When you are finished, the new default profile will show up on the Default Profiles page.

# Adding a Security Group

Before you can assign users and Roles to a Security Group, you need to create one. Insite comes with a default Security Group, but it has no basic authorization added and should only be used to catch users that aren't assigned to a Security Group (or Role).

Follow these steps to create a Security Group:

1. In the Navigation Panel, click **Settings > Security Groups**. If the menu is hidden, click .
2. Click **Add**.

New Security Group
help ?

Cancel
Save

**Name**

**Description**

**LDAP Group**

**Roles**

**Users**

**Automatically Assigned Users**

**Authorized To**

|   |                                               |
|---|-----------------------------------------------|
| ⊕ | <input type="checkbox"/> Access Authenticator |
| ⊕ | <input type="checkbox"/> Automate             |
| ⊕ | <input type="checkbox"/> Deployment Manager   |
| ⊕ | <input type="checkbox"/> HelpSystems Insite   |
| ⊕ | <input type="checkbox"/> Password Self Help   |
| ⊕ | <input type="checkbox"/> Robot Network        |
| ⊕ | <input type="checkbox"/> Robot Schedule       |

3. Enter the **Name** and **Description** of the Security Group you want to create.
4. If you are using LDAP as your [Authentication](#) method, enter the distinguished name (DN) for your **LDAP Group**. This DN is used to search for users in your LDAP server and add them (if they match) to this Security Group when they first log on to Insite. *This field does not appear if you are not authenticating with LDAP.*
5. Select the Role you want to add to the Security Group.

**NOTE:** If you haven't created any Roles yet, see [Roles](#).

6. If you want to add specific users to the Security Group, select them from the drop-down.
7. Ensure the Security Group is authorized to the correct Insite areas and products. These boxes will be automatically checked with whatever authorities the Roles and Security Groups you have selected are assigned to.

**NOTE:** You can only add authorities through a Role. Permissions are additive if multiple Roles are assigned to the Security Group.


8. Click **Save**.

When you are finished, the new Security Group will show up on the Security Groups page.

# Adding a User

Users are created in two ways: when a user logs on to Insite using an approved method of [Authentication](#), such as LDAP, or when an administrator manually creates (pre-registers) a user.

You can use the following steps to manually create (pre-register) a user:

1. In the Navigation Panel, click **Settings > Users**. If the menu is hidden, click .
2. Click **Add**. The New User screen appears.

New User
help ?

Cancel
Save

**Username**  
newuser

---

**Description**

---

**LDAP Value to Match**  
*Enter the user's value to match for the LDAP field: samaccountname*

---

**Roles**

x Admin
v

---

**Security Groups**

---

**Automatically Assigned Security Groups**

---

**Authorized To**

|   |                                     |                      |
|---|-------------------------------------|----------------------|
| + | <input checked="" type="checkbox"/> | Access Authenticator |
| + | <input checked="" type="checkbox"/> | Automate             |
| + | <input checked="" type="checkbox"/> | Deployment Manager   |
| + | <input checked="" type="checkbox"/> | HelpSystems Insite   |
| + | <input checked="" type="checkbox"/> | Password Self Help   |
| + | <input checked="" type="checkbox"/> | Robot Network        |
| + | <input checked="" type="checkbox"/> | Robot Schedule       |

3. Enter the **Username** of the user you want to create. If IBM i authentication is being used, the username you choose must match the user's IBM i profile on the authenticated IBM i system. If LDAP is the authentication method being used, Insite uses the **LDAP Value to Match** value for authentication.
4. Enter a description for the user.

5. If LDAP is being used for authentication, enter the value of the LDAP field being used for authentication (specified in the Authentication screen's "LDAP Field to Match" field). By default, the samaccountname field is used. See [Authentication](#) for more details.
6. Select the Role(s) you want to assign to the user. See [Roles](#) for more details.
7. If you want to add the user to a Security Group, select one from the drop-down. See [Security Groups](#) for more details.

**NOTE:** Roles can also be applied to Security Groups. Users inherit Roles of the Security Group they are assigned to.

8. Ensure the user is authorized to the correct Insite areas and products. These boxes will be automatically checked with whatever authorities the roles and security groups you have selected are assigned to.

**NOTE:** You can only add authorities through a role. Permissions are additive if a user is assigned to multiple roles or a security group composed of multiple roles.

9. Click **Save**.

When you are finished, the new user will show up on the Users page.



# Securing Insite

Insite supports TLS/SSL (Transport Layer Security/ Secure Sockets Layer) communications to and from both your web browser and Product Connections. Steps include:

- **Generating a Certificate.** If your organization already has a signed Certificate Authority (CA), these steps are not required and will be skipped. If not, you can use these instructions to generate a self-signed certificate.
- **Enabling the Certificate** on Windows or Linux.
- **Accessing the Insite server** with your browser.
- **Troubleshooting**

**NOTE:** Additional information is available on the [Apache Tomcat website](#).

## Generating a Self-Signed Certificate

**NOTE:** If your organization already has a signed Certificate Authority (CA), skip to the **Enabling the Certificate** section below.

You must first generate a .keystore file. Make sure to note the password you enter, as you will need this later.

### For Windows

Insite comes packaged with its own JVM. To generate the .keystore file on Windows, do the following:

1. Open the Command Prompt and go to the following directory:  
`C:\Program Files (x86)\Help Systems\HelpSystems Insite\jvm\bin`
2. Enter the following command to generate the key using the keytool:  
`keytool -keysize 2048 -genkey -alias tomcat -keyalg RSA -keystore hsinsite.keystore`
3. After creating a password, you will be prompted for your organization's information. When asked for your first and last name, specify the domain name of the server that users will enter in order to connect to Insite (e.g. 10.60.152.64) to help ensure that their certificates are valid when connecting to the server.

4. After you have filled the requested fields, press Enter. The resulting **hsinsite.keystore** file is located in your working directory (C:\Program Files (x86)\Help Systems\HelpSystems Insite\jvm\bin).

## For Linux:

1. Enter the following command:
 

```
"$JAVA_HOME/bin/keytool" -keysize 2048 -genkey -alias tomcat -keyalg RSA -keystore hsinsite.keystore
```
2. After creating a password, you will be prompted for your organization's information. When asked for your first and last name, specify the domain name of the server that users will enter in order to connect to Insite. For your first and last name if you do not have a DNS entry for the Insite server you are going to connect to you can use the IP address (e.g. 10.60.152.64). This helps ensure that their certificates are valid when connecting to the server.
3. The resulting **hsinsite.keystore** file is located in your working directory.

## Enabling the Certificate

1. Stop the Insite Server service.
  - **Windows**
    - On Windows, run **services.msc** to open the Services Manager.
    - Right-click Insite Server and choose **Stop**.
  - **Linux**
    - Run the script: /opt/insite/stopInsite.pl
2. Copy the Certificate Authority file into the installation:
  - **Windows:** C:\Program Files(x86)\Help Systems\HelpSystems Insite\conf\
  - **Linux:** /opt/insite/conf
3. Open and edit the **server.xml** file as follows. This file's location depends on the directory where the Insite server is installed (see step 2). **Note:** You can edit the server.xml file with any text editor. Be sure to create a backup a copy of the original file before editing. If you are not familiar with the XML format, we recommend using an XML-aware editor such as XML Notepad or Notepad++.
  - a. Comment out the code block for protocol="HTTP/1.1":
 

```
Connector SSLEnabled="false" compression="force"
connectionTimeout="20000" port="3040"
protocol="HTTP/1.1" scheme="http" secure="false"/
```

- b. Add the following code block, replacing the italicized text with information specific to your configuration:

```
Connector SSLEnabled="true" clientAuth="false"
compression="force" keystoreFile="your-ca-
path/filename" keystorePass="your-ca-password"
keystoreType="your-keystore-type"
maxHttpHeaderSize="32768" port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
scheme="https" secure="true"
sslEnabledProtocols="TLSv1, TLSv1.1, TLSv1.2"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_
ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_
256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_
RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_
SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_
256_CBC_SHA"
```

- c. Uncomment and change `redirectPort="8009"` to `redirectPort="8443"` in the Connector for `protocol="AJP/1.3"`.

**NOTE:** Make sure the port 8009 is available and not being used by another process on the system. You can submit the command from a DOS prompt to view the assigned ports to verify:

**For Windows:** `netstat -a | find "8009"`

**For Linux:** `netstat -an | grep "8009"`

If port 8009 is already in use and 'listening', change 8009 to a different port like 8008:

4. Save your changes to **server.xml**.
5. Start the Insite Server to complete the configuration process.
  - Windows
    - Run `services.msc` to open the Services Manager.
    - Right-click the Insite Server and choose Start.
  - Linux
    - Run the script: `/opt/insite/startInsite.pl`

## Accessing the Page

- Change your browser links to use https (instead of http) and the correct port (8443).
- `https://insite-server-ip-address:8443/HelpSystems/#HelpSystems/Home`
- `https://insite-server-domain-name:8443/HelpSystems/#HelpSystems/Home` (depending on the criteria required by your Certificate Authority).

**NOTE:** If you are using a self-signed certificate, your browser will warn you the certificate is invalid, indicate the page is a possible security threat, and may ask you to define an exception in order to access the page.

## Troubleshooting

Should you run into issues, see the below for possible solutions:

- Check the firewall configuration on the server to make sure the Insite https port is allowed incoming connections (port 8443 in example server.xml).
- On the Insite server system, check that "nslookup myserver.<domainname>.com" returns the correct IP address.
  - If it does not, then do A or B:
    - Have your server added to DNS by I.T.
    - Add the appropriate entry to the server's hosts file.
- If the Insite server is hosted on a Windows system that is joined to <domainname>.com:
  - On \*client\* system check that "nslookup myserver.<domainname>.com" returns the correct IP address
- If Insite server is not joined to the <domainname> domain then on browser client systems the "hosts" file needs to be modified to include an entry for myserver.<domainname>.com
  - Windows hosts file located at: `c:\Windows\system32\Drivers\etc\hosts`
  - \*nix hosts file located at: `/etc/hosts`
  - Example entry for "myserver":
    - `10.60.10.56 myserver.<domainname>.com`
- After ensuring the above, navigate in browser to `https://myserver.<domainname>:8443` and the connection should be secure without any browser warnings or adding certs to the client system.