FORTRA

SIEM Agent 4.8 Installation 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.

202504080154

Installing SIEM Agent

Use the following instructions to install, update, or upgrade SIEM Agent.

Before You Begin

Read this section before you install SIEM Agent.

If you are installing in an HA environment, review Replication of Identity Manager, Exit Point Manager, SIEM Agent, and Central Administration in a High Availability Environment before installing Powertech SIEM Agent for IBM i.

Licensing

SIEM Agent for IBM i requires that you enter a valid license key. Contact keys@fortra.com if you need to request a new license key.

System Requirements

The following requirements are necessary in order to install and run SIEM Agent.

- IBM i 7.3 or higher
- 7.3: PTF SI62950
- Library QHTTPSVR (IBM HTTP Server for i) must be installed under license program 5770-DG1
- Java 8 is required to send Events from SIEM Agent to Apache Kafka
  Kafka 2.5 or higher is required

> **NOTE:** During installation an FTP connection is initiated. The FTP server responds with messages that prompt for FTP login credentials. The standard port reserved to establish an FTP connection to the IBM i is port 21. Consequently, it is required that this port is open and 'listening' on the server in order to establish a connection with the Installation Wizard and facilitate a successful installation. Any firewall or exit program technology on the PC or the IBM i system could potentially block the FTP file upload and remote commands running the installation. Ensure any such firewall or program is configured to permit an FTP connection on port 21. If standard FTP is not permitted, contact Technical Support for instructions on how to manually install the product without the installation wizard.

System Values

It is Fortra's goal not to change system values on customer systems because we recognize that security-conscious organizations have rigorous change control processes in place for even small changes to system values. Therefore, we ask you to make any system value changes that are needed. However, the SIEM Agent IBM agent installation process could change a system value to allow the install to proceed if a system value is not set as specified below. If the Installation Wizard changes a system value during install, it changes it back to its original value when the install completes.

To install the SIEM Agent IBM i agent on your system, the following system values that control object restores must be configured as shown.

- Set QALWOBJRST to *ALWPGMADP (at a minimum) to allow the system to restore programs that adopt authority. Many Powertech programs adopt the authority of the product owner, rather than forcing you to give authority directly to administrators and end users. (**Note:** For some system configurations, *ALL is required temporarily.)
- QALWUSRDMN controls which libraries on the system can contain certain types of user domain objects. You should set the system value to *ALL or include the name of the SIEM Agent install libraries (PTSALIB and PTPLLIB) for the product to function properly.
- Set QVFYOBJRST to 1, 2, or 3. This allows SIEM Agent to restore all objects regardless of their signature. (**Note:** If you normally check signatures, remember to check this system value after the SIEM Agent install process completes.)
- Set QFRCCVNRST (Force conversion on restore) to 0, Do not convert anything.

Before Starting an Upgrade

The automated process of upgrading your system (described in the next section) is the same as the installation procedure.

End the SIEM Agent for IBM i Monitor jobs by running the following commands:

ADDLIBLE PTSALIB
PSAENDMON

You can also use the product menu option to ‘End Interact Monitors’.

The license code is valid only on the registered system and partition. Contact keys@fortra.com if you need to request a new license key.

If you are upgrading SIEM Agent in a High Availability environment, see Replication of Identity Manager, Exit Point Manager, SIEM Agent, and Central Administration in a High Availability Environment.

Installing SIEM Agent

The following servers must be available and running prior to installation or upgrade:

- FTP Server
- Remote Command Server

Do the following to perform the installation or update:

1. Download the SIEM Agent installer (**setupSIEMAgent.exe**) to your PC from the SIEM Agent download page.
2. Double-click the .exe file to start the Installation Wizard.
3. On the Choose Components panel, select which components you to install. You can choose to install the Manuals and the Software for IBM i. Click **Next**.
4. If you are installing the Manuals only, the process completes and the installer closes. The Manuals have been installed. You can skip the rest of these steps.

   > **NOTE:** The manuals are installed to the following location:
   > C:\Program Files\PowerTech\SIEM Agent for IBM i\manuals

5. On the IBM i Details panel:
   a. Select or enter the IBM i system.
   b. Enter a user profile and password that is a member of the user class *SECOFR and has at least the following special authorities: *ALLOBJ, *SECADM, *JOBCTL, *IOSYSCFG, *SERVICE, *SPLCTL, and *AUDIT. The user profile should have Limit capabilities set to *NO.
   c. (Optional) In the Advanced Settings section:
      - Enter a port number or use the arrows if you want to change the FTP port number to something other than the default of 21.
      - Select **Secure File Transfer** if you want to use FTPS during the file transfer. The default FTPS secure port is 990, but it can be changed to the required secure port for your environment.
      - In the **Timeout (seconds)** field, enter the number of seconds the session should be kept active during an FTP transfer. You can choose anywhere between 25 and 1800 seconds (30 minutes).

> **NOTE:** If the transfer takes longer than the amount of time specified, the session will expire.

d. Click **Next**.

6. You have two options on the Product Load Options panel:
   a. Click **Immediate Load** if you'd like to load the product on the IBM i now.
   b. Click **Staged Load** if you'd like to transfer the objects now and load them on the IBM i at a later time.

   > **NOTE:** See "Loading Staged Objects on the IBM i" (below) for instructions on how to load the staged objects on your selected IBM i system.

7. The Product Load Progress panel for SIEM Agent launches.

   If the Product Load Progress panel ends with an overall Failed message, the product upload could not complete properly. To find the reason the upload failed, click **View Logs** and review your logs. You can also use **Download** at the top of the logs to save the information for future review.

   When the processing is complete, you have two choices:

   - If this is the only installation or update of SIEM Agent that you're doing, click **Finish**.
   - If you have installs or updates to do on other IBM i systems, click **Restart**. Then, return to step 4.

Loading staged objects on the IBM i

If you chose to stage your objects during step 5b of the installation or update process, do the following to manually load them on the IBM i you identified above.

1. On the IBM i, execute the following command to display the Work with Loads panel:

   HSLOADMGR/HSWRKLOAD

2. Enter option **1**, Load, next to the Load Name for SIEM Agent and press Enter.

   The installation program installs SIEM Agent, including the required user profiles and libraries (see table below for details).

The installation process displays the job log name, user, and job log number. Use the WRKSPLF command to display the job log for complete information on the SIEM Agent install.

After You Are Done

Congratulations! Powertech SIEM Agent is now installed. Read the following for additional information, including additional steps for upgrading users.

Objects Installed on System

Installed on System	Description
Product Library	PTSALIB PTWRKMGT PTPLLIB
User Profiles	PTADMIN PTUSER
Authorization List	PTADMIN - SIEM Agent Administrators
Subsystem	PTWRKMGT *The subsystem is created at install if it doesn't already exist on the system.*
Commands in QGPL	**Object** **Type** **Library** **Attribute** POWERTECH *CMD QGPL PRX POWERTECH *MENU QGPL PGM WRKPTSA *CMD QGPL *CMD
Job Queue Entries	PSAJOBQ - In PTSALIB with 1000 max active jobs.
IFS directory	/Powertech/SIEMAgent
kafka-clients-2.5.0.jar	Installed to /Powertech/SIEMAgent
slf4j-api-1.7.30.jar	Installed to /Powertech/SIEMAgent
ReleaseNotes.html	Installed to /Powertech/SIEMAgent

See Implementing SIEM Agent for information on starting and using the product.

After You Upgrade

To convert and import version 3 settings to SIEM Agent 4:

Prompt (F4) the following command:

PTSALIB/PSACVTINT

Set Processing Option to *CONVERT to convert the existing data on your system to SIEM Agent 4. Note that you can also choose *RPTONLY to create a report instead if, for example, you would like to test the conversion.

Press Enter. A log file is created for review after the conversion: **PTSALIB/PSACVTLOG**.

After conversion has completed, if you wish to continue to use the prior version, be sure to start the SIEM Agent 3/Interact monitor jobs by submitting the command:

PTINTERACT/STRPLIAMON

If you run the prior version and new version concurrently with the same configuration, the same event transmissions to your SYSLOG server will be duplicated. Once you are content the new version is fully operational, the old version is no longer necessary and can be shut down.

> **NOTE:** In SIEM Agent 4, the app-name value included in syslog messages has been changed from "Interact" to "SIEM Agent", to reflect the product name (updated in 2018). If you have created rules in your SIEM that use the app-name value as a condition, you will need to update those rules to check for app-name = "SIEM Agent" instead of app-name="Interact".

Contacting Fortra

Please contact Fortra for questions or to receive information about SIEM Agent. 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.