

IBM Sterling External Authentication Server

Installation Guide

Version 2.4



Copyright

This edition applies to the 2.4 version of IBM Sterling External Authentication Server and to all subsequent releases and modifications until otherwise indicated in new editions.

Before using this information and the product it supports, read the information in *Notices* on page 21.

Licensed Materials - Property of IBM

IBM Sterling External Authentication Server

© Copyright IBM Corp. 2005, 2010. All Rights Reserved.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1 Review Resources 5

Chapter 2 Install Sterling External Authentication Server on UNIX or Linux 7

Install Sterling External Authentication Server on UNIX or Linux	7
Start Sterling External Authentication Server on UNIX or Linux	8
Start the Sterling External Authentication Server on UNIX or Linux	8
Start the Sterling External Authentication Server on UNIX Using a Stored and Encrypted Passphrase	9
Start the Sterling External Authentication Server on UNIX and Require a Passphrase.	9
Restore the Stored Password File on UNIX	9
Start the Sterling External Authentication Server GUI On UNIX.	10
Start the Sterling External Authentication Server GUI From the Computer Where the Sterling External Authentication Server GUI Is Installed	10
Start the Sterling External Authentication Server GUI from a Remote Computer	11
Log Off Sterling External Authentication Server on UNIX or Linux	11
Shut Down Sterling External Authentication Server on UNIX.	11

Chapter 3 Install Sterling External Authentication Server on Microsoft Windows13

Install Sterling External Authentication Server on Microsoft Windows	13
Start Sterling External Authentication Server on Microsoft Windows	14
Start the Sterling External Authentication Server on Microsoft Windows	14
Start the Sterling External Authentication Server on Microsoft Windows Using a Stored and Encrypted Password	14
Start the Sterling External Authentication Server on Microsoft Windows And Require a Passphrase	15
Restore the Stored Password File on Microsoft Windows	15
Start the Sterling External Authentication Server GUI on Microsoft Windows	15
Start the GUI from the Local Microsoft Windows Computer.	16
Start the GUI from a Remote Computer.	16
Log Off Sterling External Authentication Server on Microsoft Windows	17
Shut Down Sterling External Authentication Server on Microsoft Windows	17

Shutdown the Sterling External Authentication Server from the Sterling External Authentication Server GUI 17
Shutdown the Sterling External Authentication Server from a Command Line 17

Chapter 4 Upgrade Sterling External Authentication Server **19**

Upgrade Sterling External Authentication Server 19

Notices **21**

Trademarks 23

Review Resources

Before you install Sterling External Authentication Server, review security configuration details that are relevant for Sterling External Authentication Server. You may need to consider details that are environment specific. Refer to the following resources as you plan network and security related resources for installing and configuring Sterling External Authentication Server:

Configuration Resource	Sterling External Authentication Server Usage
TCP Ports	Use available port numbers, in appropriate port ranges to set the secure and non-secure listener, and servlet port used to download the GUI.
Network Interface Addresses	Confirm the local bind address of a network interface for a connection.
LDAP Directory Information Tree	Apply related knowledge when selecting and specifying LDAP parameters for checking attributes in directory entries.
Requirements for data encryption	Set SSL/TLS-related parameters for connections between the server and GUI, between the Sterling External Authentication Server and client applications, and between Sterling External Authentication Server and LDAP directory servers.
Ciphers for data encryption	Apply knowledge of cipher selection and related requirements when configuring data encryption parameters.
Authentication mechanism use requirements	Choose the appropriate Simple Authentication and Security Layer (SASL) mechanism from those supported in authentication definitions.
Use of self-signed certificates	Allow self-signed certificate use as appropriate.
Use of certificates signed by Certificate Authorities (CAs)	Support use of certificates signed by selected CAs.
Length of public keys	Set the public key minimum length in certificate validation definitions.

Install Sterling External Authentication Server on UNIX or Linux

Install Sterling External Authentication Server on UNIX or Linux

During installation, define a passphrase. Be sure to write it down because you may need to provide it when you start the Sterling External Authentication Server.

To install Sterling External Authentication Server on UNIX:

1. Navigate to the directory where you downloaded the installation .tar file.
2. Type the following command to retrieve the files from the archive:

```
tar xvf ESD file name
```

The 32-bit Linux installation file is extracted to the /Linux_X86 directory and the 64-bit Linux installation file is extracted to the /Linux_X64 directory.

3. To start the installation, type the following command.

```
sh SEASInstall.bin
```

4. Accept the default installation directory or specify a different directory and press **Enter**.
5. Accept the default port for the nonsecure listener or specify a different port and press **Enter**. The default is 61365.
6. Type a passphrase that is 6 or more characters and press **Enter**. Write it down because you may need it to start the server.
7. To configure the servlet container:
 - a. Accept the default value for the port number or specify a value.
 - b. Accept the default or specify a value for the fully-qualified DNS name for the engine.
8. Review the installation details and press **Enter**. When the installation is complete, the command prompt is displayed.

Start Sterling External Authentication Server on UNIX or Linux

Use the procedures in this section to start Sterling External Authentication Server. Use the following checklist to ensure that you complete the tasks necessary to start Sterling External Authentication Server:

Installation Task	Procedure to Complete
Start the Sterling External Authentication Server	Use one of the following procedures: <ul style="list-style-type: none"> ◆ <i>Start the Sterling External Authentication Server on UNIX Using a Stored and Encrypted Passphrase</i> on page 9 ◆ <i>Start the Sterling External Authentication Server on UNIX and Require a Passphrase</i> on page 9
Start the Sterling External Authentication Server GUI	Use one of the following procedures: <ul style="list-style-type: none"> ◆ <i>Start the Sterling External Authentication Server GUI From the Computer Where the Sterling External Authentication Server GUI Is Installed</i> on page 10 ◆ <i>Start the Sterling External Authentication Server GUI from a Remote Computer</i> on page 11
Change admin password	<i>Change the Admin Password</i> on page 36
Log Off	<i>Log Off Sterling External Authentication Server on UNIX or Linux</i> on page 11
Shut down Sterling External Authentication Server	<i>Shut Down Sterling External Authentication Server on UNIX</i> on page 11

Start the Sterling External Authentication Server on UNIX or Linux

When you install Sterling External Authentication Server, you define a passphrase and it is required at startup. Use one of the following methods to start Sterling External Authentication Server:

- ◆ Start Sterling External Authentication Server automatically, without interaction from the user. The passphrase is read from an encrypted file.
- ◆ Start Sterling External Authentication Server and require that the user type a passphrase when prompted. The passphrase is masked and is not visible as the user types the characters.

With both methods, the server starts in the background. All log messages are sent to the bin/startSeas.out file.

Determine the method to use to start Sterling External Authentication Server and complete the procedure for the method you select.

Start the Sterling External Authentication Server on UNIX Using a Stored and Encrypted

Passphrase

This is the default startup method. It does not require that a user type a passphrase at startup because it is stored in an encrypted file. The server starts in the background without user interaction.

Note: If this is an upgrade and the passphrase file does not exist in the previous installation, it will not be created during the upgrade.

To start the Sterling External Authentication Server using a stored passphrase:

1. Navigate to *install_dir/bin*, where *install_dir* is the Sterling External Authentication Server installation. Type the following:

```
./startSeas.sh
```

2. Check status of the server startup by viewing the *bin/startSeas.out* file. If the startup completed successfully, the file contains the following message:

```
Sterling External Authentication Server is ready for Service.
```

Start the Sterling External Authentication Server on UNIX and Require a Passphrase

This method requires that you type a passphrase. When entered, it is masked and not visible.

To start Sterling External Authentication Server and require that a passphrase be provided at startup:

1. Delete the *sb.enc* file from the *install_dir/conf/system* directory.
2. Navigate to the *install_dir/bin* directory and type the following command:

```
./startSeas.sh
```

3. Type the passphrase and press **Enter**.
4. Check status of the server startup by viewing the *bin/startSeas.out* file. If the startup completed successfully, the file contains the following message:

```
Sterling External Authentication Server is ready for Service
```

Restore the Stored Password File on UNIX

If you use the method, *Start the Sterling External Authentication Server on UNIX and Require a Passphrase* on page 9, to start the Sterling External Authentication Server, it deletes the stored passphrase and requires that the user type a passphrase at startup.

If you want to restore the default start up method, you must restore the saved passphrase. This procedure restores the passphrase to the *conf/system/sb.enc* file.

To restore the stored password file on UNIX:

1. From the `install_dir/bin` directory, type the following command:

```
enableBootstrap.sh
```

2. At the prompt, type the passphrase defined for Sterling External Authentication Server and press **Enter**.

Complete the procedure *Start the Sterling External Authentication Server on UNIX Using a Stored and Encrypted Passphrase* on page 9 to start Sterling External Authentication Server and use the stored passphrase.

Start the Sterling External Authentication Server GUI On UNIX

When you start the GUI and connect to the server for the first time, you must use the nonsecure port. To connect to the server using the secure listener port, you set up the certificates on the server and on the GUI and enable the secure listener port in the server. Refer to *Create and Manage System Certificates* on page 43.

You can start the GUI from the computer where it is installed or from a remote connection.

Start the Sterling External Authentication Server GUI From the Computer Where the Sterling External Authentication Server GUI Is Installed

To start the GUI on the computer where Sterling External Authentication Server is installed, X Windows must be running.

To start the Sterling External Authentication Server GUI:

1. Navigate to the `install_dir/bin` directory. Type the following command:

```
./startGUI.sh
```

2. On the Login screen, provide the following information:

- ◆ Host
- ◆ Port
- ◆ User
- ◆ Password

Note: The default user is **admin** and password is **admin**. Use them the first time you logon. Then, change the password.

3. Click **Login**.

Start the Sterling External Authentication Server GUI from a Remote Computer

You can run the Sterling External Authentication Server GUI on any remote computer that can connect to the Sterling External Authentication Server.

To run the Sterling External Authentication Server GUI from a remote computer:

1. Open an Internet browser.
2. In the **Address** field, type **http://SEAS_host:port**, where *SEAS_host* is the host name of the Sterling External Authentication Server, and *port* is the port for the servlet container, defined at installation. Default=9080.
3. Click **Launch GUI**. The first time you run Sterling External Authentication Server from a browser, you receive messages about the launch and any security issues.
4. Accept the certificate to start the GUI from the browser for the first time.
5. Provide the following information:
 - ◆ Host
 - ◆ Port
 - ◆ User
 - ◆ Password
 - ◆ SSL/TLS

Note: The default user is **admin** and the password is **admin**. Use these values the first time you logon. Then, change the password.

6. Click **Login**.

Log Off Sterling External Authentication Server on UNIX or Linux

To log off of Sterling External Authentication Server, select **Exit** from the **File** menu.

Shut Down Sterling External Authentication Server on UNIX

If you close the Sterling External Authentication Server GUI, the Sterling External Authentication Server continues to run. Keep the Sterling External Authentication Server running when client applications need to connect. To shut down the server, close all open GUI Windows and complete the one of the following procedures.

To shut down the server from the Sterling External Authentication Server GUI:

1. From the **File** menu, select **Shutdown Server**.
2. Type the passphrase created at installation and click **OK**. The Sterling External Authentication Server shuts down and the GUI closes.

To shut down the Sterling External Authentication Server from a command line:

1. From a command prompt, navigate to the *install_dir/bin* directory.
2. Type the following command.

```
./stopSeas.sh
```

3. When prompted, type the passphrase, defined at installation.
4. When prompted, type the administrator ID and administrator password.

A message is displayed indicating the server is shutting down.

Install Sterling External Authentication Server on Microsoft Windows

Install Sterling External Authentication Server on Microsoft Windows

At installation, you define a passphrase, a six or more character password that contains any combination of characters. Write it down because you may need it when you start the server.

To install Sterling External Authentication Server on Microsoft Windows:

1. Navigate to the directory where the Sterling External Authentication Server installation archive file is downloaded.
2. Extract the files to the download directory or to another location by double-clicking the Sterling External Authentication Server installation archive file icon.

The Microsoft Windows Server 2003 32-bit installation file is extracted to the \Windows_X86 directory and the Microsoft Windows Server 2008 64-bit installation file is extracted to the \Windows_X64 directory.

3. Double-click the SEASInstall.exe file.
4. Read the introductory information and click **Next**.
5. Accept the installation directory or click **Choose** to select another directory. Click **Next**.
6. Accept the default for the listener or specify a different port. Click **Next**. Default=61365.
7. Type a passphrase, in the **Passphrase** and **re-enter passphrase** fields. Click **Next**.
8. To configure the servlet container:
 - a. Accept the default value for the port of the servlet container or specify a value.
 - b. Accept the default for the fully-qualified DNS name for the engine or specify a value.
 - c. Click **Next**.
9. Review the installation details and click **Install**.
10. Click **Done**.

Start Sterling External Authentication Server on Microsoft Windows

Use the following checklist to ensure that you complete tasks to start Sterling External Authentication Server.

Installation Task	Procedure to Complete
Start the Sterling External Authentication Server	Use one of the following procedures: <ul style="list-style-type: none"> ◆ <i>Start the Sterling External Authentication Server on Microsoft Windows Using a Stored and Encrypted Password</i> on page 14 ◆ <i>Start the Sterling External Authentication Server on Microsoft Windows And Require a Passphrase</i> on page 15
Start the Sterling External Authentication Server GUI	Use one of the following procedures: <ul style="list-style-type: none"> ◆ <i>Start the GUI from the Local Microsoft Windows Computer</i> on page 16 ◆ <i>Start the GUI from a Remote Computer</i> on page 16
Change the password for the admin user	<i>Change the Admin Password</i> on page 36

Start the Sterling External Authentication Server on Microsoft Windows

When you install the Sterling External Authentication Server, you define a passphrase. It is required to start the server. Start Sterling External Authentication Server as a Microsoft Windows service or require that a passphrase be typed at startup.

Start the Sterling External Authentication Server on Microsoft Windows Using a Stored and Encrypted Password

This startup method is enabled when you install Sterling External Authentication Server. The user is not required to type a passphrase at startup because it is stored in a file. The server starts in the background, as a Microsoft Windows service without user interaction.

To start the Sterling External Authentication Server using a stored passphrase:

1. From **Control Panel**, double-click **Administrative Tools**.
2. Double-click **Services**.
3. Double-click the **Sterling External Authentication Server V2.4.00** service.
4. To configure the service to start automatically every time the computer is started, set **Startup type** to **Automatic**.
5. Under **Service status**, click **Start**.

Start the Sterling External Authentication Server on Microsoft Windows And Require a Passphrase

To start the Sterling External Authentication Server and require that a passphrase be provided:

1. Delete the `sb.enc` file from the `install_dir/conf/system` directory, where `install_dir` is the directory where Sterling External Authentication Server is installed.
2. From a command prompt, navigate to `install_dir/bin` and type the following command:

```
startSeas.bat
```

3. When prompted for a passphrase, type the passphrase defined at installation. The following message is displayed when the startup is successfully.

```
The Sterling External Authentication Server V2.4.00 service was started successfully.
```

The Sterling External Authentication Server runs as a Microsoft Windows Service when the startup is complete.

Restore the Stored Password File on Microsoft Windows

If you use the method, *Start the Sterling External Authentication Server on Microsoft Windows And Require a Passphrase* on page 15, to start the Sterling External Authentication Server, it deletes the stored passphrase and requires that the user type a passphrase at startup.

To restore the default start up method, you must restore the saved passphrase.

To restore the passphrase to the `conf\system\sb.enc` file:

1. From the `install_dir/bin` directory, type the following command:

```
enableBootstrap.bat
```

2. At the prompt, type the passphrase defined for Sterling External Authentication Server and press **Enter**.

Complete the procedure *Start the Sterling External Authentication Server on Microsoft Windows And Require a Passphrase* on page 15 to start Sterling External Authentication Server and use the stored passphrase.

Start the Sterling External Authentication Server GUI on Microsoft Windows

When you start the GUI the first time, you must use the nonsecure port. To prepare for secure connection, set up certificates on the server and GUI and enable the secure listener port. See *Create and Manage System Certificates* on page 43.

You can logon from the computer where Sterling External Authentication Server is running or from a remote computer.

Start the GUI from the Local Microsoft Windows Computer

To start the GUI on the computer where Sterling External Authentication Server is running:

1. From the **Start** menu, click **Programs > Sterling External Authentication Server V2.4.00>Sterling External Authentication GUI**.
2. Provide the following information:
 - ◆ Host
 - ◆ Port
 - ◆ User
 - ◆ Password
 - ◆ SSL/TLS

Note: The default user is **admin** and the default password is **admin**. Use the default values the first time you logon. Then, change the password to maintain security.

3. Click **Login**.

Start the GUI from a Remote Computer

You can download and run the GUI on any remote computer that can connect to the Sterling External Authentication Server.

To start the GUI on a remote computer:

1. Open an Internet browser.
2. In the **Address** field, type **http://SEAS_host:port**, where *SEAS_host* is the Sterling External Authentication Server host name, and *port* is the port number for the servlet container, specified during installation. Default=9080.
3. Click **Launch GUI**. The first time you run Sterling External Authentication Server from a browser, messages are displayed about the launch and any potential security issues.
4. Accept the certificate to start the GUI from the browser for the first time.
5. Provide the following information:
 - ◆ Host
 - ◆ Port
 - ◆ User
 - ◆ Password
 - ◆ SSL/TLS

Note: The default user is **admin** and the default password is **admin**. Use the default values the first time you logon. Then, change the password to maintain security.

6. Click **Login**.

Log Off Sterling External Authentication Server on Microsoft Windows

To log off of Sterling External Authentication Server, select **Exit** from the **File** menu.

Shut Down Sterling External Authentication Server on Microsoft Windows

If you close the Sterling External Authentication Server GUI, the server continues to run. Keep the server running when applications need to connect.

Shutdown the Sterling External Authentication Server from the Sterling External Authentication Server GUI

To shut down the Sterling External Authentication Server from the Sterling External Authentication Server GUI:

1. Select **File>Shutdown Server**.
2. Type the passphrase created at installation and click **OK**. The Sterling External Authentication Server shuts down and the GUI closes.

Shutdown the Sterling External Authentication Server from a Command Line

To shut down the Sterling External Authentication Server from a command line:

1. From a Microsoft Windows command prompt, navigate to the *install_dir/bin* directory.
2. Type the following command.

```
stopSeas.bat
```

3. When prompted, type the passphrase, defined at installation.
4. When prompted, type the administrator ID and administrator password.
A message is displayed indicating the server is shutting down.

Upgrade Sterling External Authentication Server

Upgrade Sterling External Authentication Server

If you upgrade an installation, configuration files located in the conf directory and log files located in the logs directory are not overwritten. Configuration files that are new to version 2.4.00 are installed and encrypted with a passphrase. If you removed any files from an installation, such as removing the sb.enc file to require that a passphrase be provided at startup, these files will not be replaced during an upgrade.

To upgrade Sterling External Authentication Server to version 2.4.00:

1. Shut down the Sterling External Authentication Server and confirm that no application is accessing Sterling External Authentication Server files.
2. Make a backup of the existing installation. These files are used only if the upgrade is unsuccessful.
3. Install Sterling External Authentication Server version 2.4.00.
4. Specify the directory where the existing version is installed.
The installation program detects the existing installation and gives you the opportunity to install over the existing files or specify an alternate directory.
5. If the file conf/system/sb.enc does not exist in the existing installation, you are prompted for a passphrase. Specify the passphrase from the original installation.

The original port of the non-secure listener and the Servlet container from the original installation are used.

After you review the information displayed in the Pre-Installation Summary, the upgrade updates any new and modified files.

When the upgrade is complete, you may start the Sterling External Authentication Server.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual

Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do

not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA__95141-1003
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available. This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2010. Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. 2010.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both: <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft Windows, Microsoft Windows NT, and the Microsoft Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center®, Connect:Direct®, Connect:Enterprise, Gentran®, Gentran:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker®, and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce, Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.