IBM RealSecure

Server Sensor Installation Guide

Version 7.0

IBM Internet Security Systems

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

Disclaimer: The information contained in this document may change without notice, and may have been altered or changed if you have received it from a source other than IBM Internet Security Systems (IBM ISS). Use of this information constitutes acceptance for use in an “AS IS” condition, without warranties of any kind, and any use of this information is at the user’s own risk. IBM Internet Security Systems disclaims all warranties, either expressed or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall IBM ISS be liable for any damages whatsoever, including direct, indirect, incidental, consequential or special damages, arising from the use or dissemination hereof, even if IBM Internet Security Systems has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages, so the foregoing limitation may not apply.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by IBM Internet Security Systems. The views and opinions of authors expressed herein do not necessarily state or reflect those of IBM Internet Security Systems, and shall not be used for advertising or product endorsement purposes.

Links and addresses to Internet resources are inspected thoroughly prior to release, but the ever-changing nature of the Internet prevents IBM Internet Security Systems, Inc. from guaranteeing the content or existence of the resource. When possible, the reference contains alternate sites or keywords that could be used to acquire the information by other methods. If you find a broken or inappropriate link, please send an email with the topic name, link, and its behavior to support@iss.net.

November 26, 2008

Contents

Preface

Chapter 1: Introduction to RealSecure Server Sensor

Chapter 2: Upgrading RealSecure Server Sensor

Chapter 3: Before You Install RealSecure Server Sensor

Chapter 4: Installing on a Windows Platform

Chapter 5: Installing on a Solaris Platform

Chapter 6: Installing on an AIX Platform

Chapter 7: Installing on an HP-UX Platform

Chapter 8: After You Install RealSecure Server Sensor

Chapter 9: Uninstalling a Sensor

Chapter 10: Troubleshooting

Preface

Overview

Purpose

This guide describes the requirements and procedures for installing and preparing your IBM RealSecure Server Sensor version 7.0 for configuration. This guide also gives procedures for upgrading sensors.

Audience

This guide is intended for system administrators responsible for installing RealSecure Server Sensor.

What's new in this guide

This guide was updated for RealSecure Server Sensor for AIX, Service Release 4.2 and includes new or revised information about the following topics:

- for installations on AIX version 6.1, the installation package supports installation on system workload partitions. See "Installation Options for Workload Partition Environments" on page 85.
- uninstalling from AIX systems. See "Uninstalling a Sensor from an AIX Platform" on page 119.

Note

The installation packages for each version of server sensor include all enhancements released with the latest Service Release. When you install a sensor, the sensor will show as a version 7.0 sensor with the appropriate Service Release applied.

How to Use RealSecure Server Sensor Documentation

Using this guide

Refer to this guide as you install or update a RealSecure Server Sensor.

Related publications

For additional information, see the following publications:

- *RealSecure Server Sensor Policy Guide*
- *RealSecure Server Sensor System Requirements*
- *SiteProtector Installation Guide*
- *SiteProtector Help*

License agreement

For licensing information on IBM Internet Security Systems products, download the IBM Licensing Agreement from:

http://www-935.ibm.com/services/us/iss/html/contracts_landing.html

Getting Technical Support

Introduction

IBM Internet Security Systems provides technical support through its Web site and by email or telephone.

The IBM ISS Web site

The Customer Support Web page (http://www-935.ibm.com/services/us/index.wss/offerfamily/iss/a1029129) provides direct access to online user documentation, current versions listings, detailed product literature, white papers, and the Technical Support Knowledgebase.

Hours of support

The following table provides hours for Technical Support at the Americas and other locations:

Location	Hours
Americas	24 hours a day
All other locations	Monday through Friday, 9:00 A.M. to 6:00 P.M. during their local time, excluding IBM ISS published holidays **Note:** If your local support office is located outside the Americas, you may call or send an email to the Americas office for help during off-hours.

Table 1: *Hours for technical support*

Contact information

For contact information, go to the Contact Technical Support Web page at http://www-935.ibm.com/services/us/index.wss/offering/iss/a1029178.

Chapter 1

Introduction to RealSecure Server Sensor

Overview

Introduction

This chapter describes RealSecure Server Sensor. This chapter contains useful information to help you as you deploy and install your sensor.

In this chapter

This chapter contains the following topics:

About RealSecure Server Sensor

Introduction

RealSecure Server Sensor monitors traffic to and from a single server. In addition to detecting intrusions, the sensor can also prevent intrusions by blocking network packets. The sensor can also identify attacks destined for active services on the protected host.

Management

Manage RealSecure Server Sensor with SiteProtector Version 2.0, Service Pack 5.2 or later.

Server sensor overview

RealSecure Server Sensor has the following attributes:

- detects both network and system events
- detects events at the application layer
- detects events before they reach the IP stack
- monitors traffic to and from the host it is installed on
- prevents intrusions
- extends validation and response options with Fusion Scripting

Reference

For more information about sensor features and how to configure them to optimize the protection the sensor offers, see the *IBM RealSecure Server Sensor Policy Guide, Version 7.0*.

Installation Programs and Utilities

Introduction

You can obtain the RealSecure Server Sensor installation program from the IBM Internet Security Systems Web site or from the IBM Internet Security Systems CD.

System requirements

The System Requirements document contains the most current information about memory, processor speed, hard drive space, and other hardware and software requirements. The System Requirements document is located on the IBM ISS Web site at: http://documents.iss.net/literature/RealSecure/Server_Sensor_System_Requirements.pdf

Installation programs

RealSecure server sensor has installation programs for the following operating systems:

- Windows
- Solaris
- HP-UX
- AIX

Utility programs

RealSecure Server Sensor also uses utilities that run like installation programs to serve the following purposes:

- distribute public cryptographic keys
- restore archived private cryptographic keys
- select cryptographic authentication keys

Note: For information about installing these utilities, contact Technical Support.

Deployment Suggestions

Introduction

Install a sensor on any file server that contains critical data. Common locations for sensors are as follows:

- on Internet Information Server (IIS) or Apache Web servers
- on important Windows or Unix servers
- on Windows domain servers or Unix NIS servers
- on host systems with critical data
- on hosts to monitor remote Unix syslogs or Windows event logs

On important servers

When installed on important servers associated with vital applications or data files, the sensor monitors security-sensitive activities on the critical hosts.

On Windows domain or Unix NIS servers

Windows domain servers and Unix NIS servers are typically the repository for important user account files and other important configuration data. The sensor monitors activity on these critical data stores.

On host systems with critical data

When installed on systems with sensitive data, you can use the sensor to detect changes in host configuration, unusual administrator activity, or attempts to access important files.

On hosts to monitor remote logs

RealSecure Server Sensor can run on Windows hosts and on Unix hosts. To monitor Unix hosts where the sensors cannot run locally, you can either forward the host’s syslog files to a Windows agent or use the remote monitoring feature built into the Unix subsystem on a host running a sensor.

⚠ **Caution:** When you forward syslogs or read them remotely, the syslog information is sent in clear text. Use an encrypted VPN tunnel or a secure channel if you plan to forward syslogs or read syslogs remotely.

Chapter 2

Upgrading RealSecure Server Sensor

Overview

Introduction

If you have an earlier version of RealSecure Server Sensor installed, you can upgrade to a version 7.0 sensor. This chapter provides the procedures for how to upgrade sensors and policies to version 7.0.

Note: You cannot upgrade earlier versions of server sensor to version 7.0 for the HP-UX platform or for the AIX platform. RealSecure Server Sensor version 7.0 is the first server sensor designed to run on the HP-UX and AIX platforms.

In this chapter

This chapter contains the following topics:

Upgrading Sensors Remotely

Introduction

This topic describes the prerequisites to upgrading an earlier version sensor. This topic also describes where to find upgrade packages and how to upgrade a sensor remotely.

Upgrading with management components

If you have version 6.5 sensors installed, you can use SiteProtector to remotely upgrade your sensors to version 7.0. If you have a sensor version earlier than 6.5 installed, you must upgrade your sensor to version 6.5 before you can use SiteProtector to upgrade to version 7.0.

Reference: For information about remotely upgrading sensors using SiteProtector, see the SiteProtector Help.

Prerequisites for 6.x sensors

If you are upgrading a 6.x sensor remotely, you must do the following:

- upgrade SiteProtector to version 2.0, Service Pack 5.2 or later

  Reference: For more information, see the *SiteProtector Installation Guide*.
- upgrade version 6.0 and 6.0.1 sensors to version 6.5
- locate the upgrade package as follows:
  - from the SiteProtector Deployment Manager
  - from the IBM ISS Web site at the following location:

    http://www.iss.net/download/
  - on the IBM Internet Security Systems Product CD in the **`/updates/RealSecure`** directory

Prerequisite for Solaris server sensors

When you upgrade RealSecure Server Sensor for Solaris you must stop and then restart the server to complete the upgrade. Before you begin the upgrade, choose a time when it is most convenient to stop and restart the server.

Upgrades and Web server components

If you are using the Web server monitoring component of server sensor, and the Web server is not installed in the default location, then the upgrade process cannot configure the monitoring component during the upgrade. You must manually configure the monitoring component after the upgrade is complete. For more information on how to manually configure the Web server monitoring component, see the *IBM RealSecure Server Sensor Policy Guide*.

Procedure

To remotely upgrade a sensor:

1. Manage the sensor you want to upgrade.

   Reference: For information about how to manage a sensor, look up "managing, sensors" in the Help.

2. Right-click the sensor.

   A pop-up menu lists command options.

3. Select **X-Press or product update**.

   The Update Installer window opens.

4. Select the location of the upgrade package.
5. Select **Upgrade or Service Release**.
6. Click **Next**.

   The Available updates box lists the updates available for this sensor.

7. Select the update you want, and then click **Next**.

   The Strong Encryption Export Agreement window opens.

8. Read the agreement, select **Yes**, and then click **OK**.

   The update program downloads the update, and then prompts you to continue.

9. Click **Continue**.
10. Click **Yes**.

    After a few seconds, the component status changes to "Unknown." When the upgrade is complete, the component status changes to Active.

    Solaris sensors: If you are upgrading a RealSecure Server Sensor for Solaris, the system must shut down and restart before the installation can be completed.

Upgrading Sensors Manually

Introduction

If you chose not to use the remote upgrade feature, you can upgrade a sensor manually.

Upgrading sensors

To manually upgrade sensors to version 7.0, you must uninstall any previous versions of the sensor, and then install the new version.

References: For instructions on uninstalling a sensor, see Chapter 9, "Uninstalling a Sensor". For installation instructions, see the appropriate installation chapter in this guide.

Upgrading Policies

Introduction

This topic describes the following:

- policy versions that are compatible with 7.0 server sensors
- policy upgrade issues

Note: You cannot upgrade earlier version policies for use with RealSecure Server Sensor version 7.0 on the HP-UX or AIX platforms.

Policy compatibility

Table 2 defines sensor and policy compatibility.

Important: If you apply a later version of a policy to an earlier version of a sensor (for example, a 7.0 policy to a 6.5 sensor), then the 6.5 sensor cannot use new signatures contained in the 7.0 policy, and the sensor will generate errors that notify you of the discrepancy.

Sensor version...	accepts policy versions...
5.5	5.5
5.5.1	5.5.1
5.5.2	5.5.1, 5.5.2, 5.5
6.0	5.5, 6.0
6.0.1 (Windows only)	6.0.1 (Windows only)
6.5	5.5, 5.5.1, 5.5.2, 6.0.1, 6.5
7.0	6.5, 7.0

Table 2: *Policies and sensor compatibility*

Upgrading a custom version 6.5 policy

Use the policy editor to import a version 6.5 custom policy to a version 7.0 server sensor.

Solaris policies: For existing signatures, the sensor preserves any dynamic block settings. New signatures use a default setting of 1800 seconds.

Windows policies: In server sensor version 6.5, you configured dynamic blocking at the signature level. In server sensor version 7.0, you can configure dynamic blocking at the sensor level or at the signature level. When you import a version 6.5 policy to a version 7.0 sensor, the signature level dynamic block configuration is imported as a signature level dynamic block configuration.

Note: If dynamic blocking is enabled at the sensor level in the version 7.0 sensor, the sensor level setting overrides the signature level setting.

Reference

For information about importing policies, see the SiteProtector Help.

Chapter 3

Before You Install RealSecure Server Sensor

Overview

Introduction

This chapter provides important information you should know before you install RealSecure Server Sensor.

In this chapter

This chapter contains the following topics:

Prerequisite Checklist

Introduction

This topic provides a checklist of prerequisites you should consider before you install RealSecure Server Sensor.

Prerequisites table

The following table describes the prerequisite tasks you must perform before you install a server sensor:

Task	Description	Reference
❑	Obtain a license file	*SiteProtector Installation Guide*
❑	Create a naming convention for sensors	“Sensor Naming Conventions” on page 25
❑	Unharden the operating system	“Unhardening the Operating System” on page 26
❑	Uninstall any previously installed versions of server sensor	Chapter 9, "Uninstalling a Sensor"
❑	Decide if you will automatically import authentication keys	“Automatically Importing Authentication Keys” on page 29
❑	Install new encryption software, if needed	“Customizing Encryption” on page 31
❑	Verify that the latest encryption Service Pack is installed	“Customizing Encryption” on page 31
❑	Determine public key administrators	“Administering Public Authentication Keys” on page 35
❑	Configure the system appropriately for use with non-English characters or a non-English Windows operating system	“Support for Non-English Windows Applications and Characters” on page 36
❑	Review the requirements for installing multiple sensors on one system	“Installing Multiple Sensors on a System” on page 39

Table 3: *Prerequisites to installing server sensor*

Task	Description	Reference
❑	Enable C2Audit (AIX and HP-UX platforms only)	“Enabling C2 Audit for AIX Platforms” on page 40 “Enabling C2 Audit for HP-UX Platforms” on page 41
❑	Increase memory (HP-UX platforms only)	“Increasing the Size Limits for Per Process Memory on HP-UX Platforms” on page 42
❑	Enable the Basic Security Module (Solaris platforms only)	“Enabling the Basic Security Module (BSM) on Solaris Platforms” on page 43
❑	Gather information required to complete the installation if you plan to protect an Apache Web Server	“Protecting an Apache Web Server” on page 44
❑	Plan your installation for a time when it is convenient to restart your system (certain installation options may not require a system restart, but most do).	

Table 3: *Prerequisites to installing server sensor (Continued)*

Sensor Naming Conventions

Introduction

A sensor naming convention helps you to identify sensors on the Console. For example, you may want a sensor name to indicate whether a sensor is inside or outside the firewall, or to indicate that it is located in a specific department.

⚠ **Caution:** Sensor names can contain only alphanumeric characters and underscores; they must also not exceed 100 characters in length.

Naming a sensor

Assign a name to the sensor or accept the default name when you are installing the sensor. You cannot rename a sensor after you install it, so it is important to establish a logical naming convention before you deploy your sensors. To rename a sensor, you must uninstall, and then reinstall the sensor.

Example: The following naming convention categorizes sensors by physical and geographical location and also identifies their host name:

- nyc_dmz_hostname1
- nyc_int_hostname2
- atl_dmz_hostname3
- atl_int_hostname4

Unhardening the Operating System

Introduction

The installation program cannot write critical files and registry keys to a hardened or locked-down operating system because you cannot write to locked files and registry keys.

Action

Before you install the sensor, IBM ISS recommends that you unharden the operating system and then reharden the system after the installation completes.

Using Authentication

Introduction

Authentication is a process by which one component proves its identity to another component. Authentication occurs when components establish communication connections. Authentication uses a public/private key pair created by a cryptographic provider. This method of authentication is secure because each component must identify itself to the other components before sensitive security data is sent. The authentication process does not negatively impact the performance of your system.

Authentication and public/private keys

For authentication, event collectors must have the public authentication key of the Console, and sensors must have the public authentication keys of Consoles and event collectors. You send the public keys to each component's system in one of the following ways:

- using the automatic key import option

  Reference: For more information, see "Automatically Importing Authentication Keys" on page 29.
- manually copying them

  Reference: For more information, see "Configuring Authentication Manually" on page 101.

Private keys are stored securely on the system where the key pairs were generated.

Reference: For more information about key management, see "Administering Public Authentication Keys" on page 35.

Key names

The installation program saves public keys in the `Keys` subdirectory of each component. Console keys start with `sp_con`. Sensor and event collector keys start with `rs_eng`.

Cryptographic providers

Cryptographic providers provide the means for creating the public/private key pairs. When you install a sensor, you should select a cryptographic provider and use authentication.

Changing cryptographic providers

If you want to change the cryptographic provider after you install the sensor, uninstall and then reinstall the sensor with the new settings.

Note: If an event collector and a sensor reside on the same computer, you must uninstall and then reinstall both components. You only need to uninstall the SiteProtector Console if you need to change the cryptographic providers for the Console.

Connections that are not authenticated

If you do not use authentication, any device that uses the IBM ISS protocol can monitor a component. The Console or event collector uses the public/private key pair that was created when you installed them, and they send the public key to any component they communicate with; however, the component does not verify the identity of the Console or event collector. The sensor automatically accepts the public keys on a per-session basis.

Automatically Importing Authentication Keys

Automatic authentication key import

When you install a component you can automatically import an authentication key from the Console. When you select the auto-import option, the sensor receives the initial authentication key over a standard network connection initiated from the Console. The installation program imports only the Console's public keys. Unless you use the Deployment Manager to automatically distribute authentication keys, you must manually copy the public keys of other components, such as event collectors, to the sensors.

⚠ **Caution:** If you use the automatic key import option and the sensor receives its first connection from an unknown user, then the public key from the unknown user's Console is copied to the sensor. When a known user tries to copy public keys to the sensor, a warning message indicates that a key already exists, and the known user's keys are not copied to the sensor.

Auto-import and multiple components

When an event collector and a sensor reside on the same computer, the auto-import feature is enabled for both components.

Requirements

For auto-import to work correctly, you must do the following:

- If you are installing the event collector on the same system as SiteProtector, then you must install SiteProtector, and then enable the Automatic Key Import option.
- Install all the sensors or event collectors on the computer and enable the Automatic Key Import option during the installation.
- Install all the components that will reside on a single computer before you connect to any of the sensors, event collectors, or other components.
- After the installation is complete, connect to any sensor or event collector on the computer that uses the Deployment Manager.

Installing components after first connection

If you install a component with the auto-import option, connect to the component, and then later install a second component, you must manually copy the authentication keys to the second component before you can manage or monitor it.

Reference: For more information about manually copying keys, see "Configuring Authentication Manually" on page 101.

Recommendation

IBM ISS recommends that you configure the sensor on a network segment that is protected from unauthorized network access until the initial public key has been imported by the Console. After you connect to the sensor for the first time, verify that only the appropriate users have access to the sensor.

Customizing Encryption

Introduction

IBM ISS software uses a proprietary communication protocol to secure the information passed among components (Consoles, event collectors, and sensors). This protocol relies on encryption provided through one or more built-in providers or external Cryptographic Service Providers (CSPs), such as Microsoft RSA. During the installation process, you make choices that concern cryptographic providers and how the encryption algorithms are configured. You can change these settings at any time after you install the IBM ISS software.

Reference: For more information, see “Changing Encryption Providers” on page 105.

Encryption custom options

During the installation, you can customize the encryption settings in the following ways:

- Choose (from a list of available providers on your system) the provider that you want a particular component to use.
- Arrange the providers in order of preference. This determines which provider the sensor attempts to use first.
- Customize any default encryption algorithms or key strengths.

  Important: You must select common encryption algorithms and keys for the Console and for each sensor and event collector. If you do not, the components will not be able to communicate with each other. If you make a change in the default settings, make a note of it so that you can apply the same algorithms or keys to the other components.

Encryption keys

At the end of the installation process, the program generates a public/private encryption key pair for each provider you selected. These keys are used to encrypt and decrypt a symmetric encryption key passed between components, and to let other components authenticate the one you just installed, if you authenticated the new one.

Reference: For more information about setting up authentication using these public keys, see “Using Authentication” on page 27.

Rules for configuring encryption during installation

The following rules apply to configuring cryptographic providers during the installation:

- The option to customize cryptographic providers is available only in the custom sensor installation program.
- The option to configure cryptographic providers is always available during the Console installation.
- The first time you install a sensor or an event collector, you have the option to enable automatic import of the authentication key and select cryptographic providers and the authentication strength.
- After you install the first sensor or event collector, all other sensors or event collectors have the same authentication strength, cryptographic providers, and auto import setting as the first sensor or event collector that you installed.

Microsoft RSA encryption

SiteProtector supports the Microsoft RSA Base, Strong, or Enhanced Cryptographic Providers to encrypt communication between components (Console, sensors, and event collectors). The providers typically offer RSA public/private key encryption at 512, 1024, 1536, or 2048 bit strengths.

These providers may also offer symmetric encryption using DES, DESX, 2-key Triple DES, Triple DES, RC2, and RC4 algorithms. The RC2 and RC4 algorithms typically support 40, 56, or 128 bit key strengths. Cryptographic hash algorithms typically include MD2, MD4, MD5, and SHA-1. The choices that appear depend on your operating system level, service pack, and browser installation.

Enabling RSA authentication

IBM ISS recommends using RSA authentication for configurations that include version 7.0 server sensors. If RSA 1536 authentication is not enabled on the Console, the system prompts you to add an RSA provider. If you are installing the Console or the event collector for the first time, you should install at least one RSA provider when you install the Console so that the Console can communicate with the sensor.

Preferred cryptographic provider

Although Certicom encryption is available for earlier versions of components, RSA is the preferred cryptographic provider for components and for version 7.0 server sensor configurations. **Certicom encryption will not be available in future releases of the software**.

Note: Starting with server sensor version 7.0, Service Release 4.1 for HP-UX platforms, Service Release 4.4 for Windows platforms, Service Release 4.3 for Solaris platforms, and Service Release 4.1 for AIX platforms only RSA authentication is supported.

Reference: For more information about provider availability and capability, see the Microsoft Web site. You must complete any provider upgrades or installations before you install the server sensor software.

Encryption and US laws

Encryption technologies are restricted by U.S. export laws. These technologies cannot be exported or re-exported to certain countries.

Reference: For more information about U.S. export laws, see the Commercial Encryption section of the Bureau of Export Administration's Web site at:

http://www.bis.doc.gov

Archiving Private Keys

Introduction

If the cryptographic provider's private key is damaged or destroyed, and you have an archived copy, use the Restore Cryptographic Private Keys utility to retrieve the archived copy.

Important: The installation program can only archive private keys when it creates them; it cannot archive existing private keys. The option to archive private keys is not available with the automated installation.

If you do not have an archived copy of the key

If the private key becomes damaged or destroyed, and you do not have an archived copy of the key, IBM ISS recommends that you reinstall the component that has the damaged key to create a new private/public key pair. Then, before authenticated communication can occur, you must copy the new public key to other components.

Reference: For more information, see “Restoring Archived Private Keys” on page 103.

Administering Public Authentication Keys

Introduction

Key management allows you to manage and distribute public authentication keys. Using key management, you can specify one or more users as key administrators. A key administrator is a user who has rights to manage public authentication keys remotely from the Console.

Important: At least one user must have key administrator rights to use the Deployment Manager.

Key administrators

A key administrator can maintain daemon roles, which is an access list of users with special privileges that the issDaemon maintains. The list identifies users as computername_username. Daemon roles include Key Administrator.

Setting up a key administrator (Windows)

For a Windows sensor, you must set up at least one key administrator during the installation process or enable auto-import during the installation process (the first person to connect to the sensor gains key administrator rights).

Reference: For more information about using the automatic key import option, see “Automatically Importing Authentication Keys” on page 29.

Setting up a key administrator (Unix)

For a Unix sensor, you should set up a key administrator during the installation process, if this option is available for the installation option you chose. If you do not set up a key administrator during the installation process, you can add an administrator from the command line.

Support for Non-English Windows Applications and Characters

Non-English versions of Windows

RealSecure Server Sensor has been tested on non-English versions of Windows, including French, Japanese, German, and Spanish. However, the software is most thoroughly tested on English versions of Windows, and IBM ISS recommends that you use the English version of Windows.

Foreign characters for other programs

If you need to use foreign characters for other applications on the computer that is running a sensor, IBM ISS recommends that you configure Windows to support your location and language instead of installing the non-English version of Windows.

Foreign characters

If you change your locale settings, sensor names, directories, or user names, any other character-based name must use English characters or numbers.

⚠ **Caution:** Using foreign characters can cause sensors or other components to malfunction.

Reference

For more information about system locales, see the Microsoft Web site at: http://msdn.microsoft.com/library/

Localizing the US English version of Windows NT 4.0

To configure the US English version of Windows NT 4.0 to support your system locale:

1. From the taskbar, select **Start→Settings→Control Panel**.

   The Control Panel window appears.

2. Double-click the **Regional Settings** icon.

   The Regional Settings Properties window appears.

3. From the **Regional Settings** tab, select a language from the list.
4. Select the **Set as system default locale** check box, and then click **Apply**.
5. Click **OK**.

   The system applies the language's default code page and associated fonts to your system.

6. Do the display settings need to be adjusted?
   - If *yes*, go to Step 7.
   - If *no*, go to Step 11.
7. From the **Control Panel** window, double-click the **Display** icon.

   The Display Properties window opens.
8. Select the **Appearance** tab, and then select a font size.
9. Click **Apply**.
10. Click **OK** to quit the **Display Properties** window.
11. From the **Regional Setting Properties** window, select the **Input Locales** tab.
12. Click **Add**.

    The **Add Input Locale** window appears.
13. Select the language from the list, and then click **OK**.
    The **Input Locales** tab appears.
14. In the **Default input locale** field, click **Set as Default**.

    The system sets the language as the default input locale.
15. In the **Switch Locales** field, select the shortcut key combinations for switching between input locales.
16. Select the **Enable indicator on taskbar** check box, and then click **OK**.
17. Click **Apply**.

    The **Regional Properties** window closes.
18. Restart the system.

    The system locale changes take effect.

Localizing the US English version of Windows 2000 and 2003

To configure the US English version of Windows 2000 to support your system locale:

1. From the taskbar, select **Start→Settings→Control Panel**.

   The Control Panel window appears.
2. Double-click **Regional Options**.

   The Regional Options Properties window appears.
3. From the **Regional Options** tab, select a language from the list.

4. Select the **Set default** check box.

   The Select System Locale window appears.

5. Click **OK**, and then click **Apply**.

6. Click **OK**.

   The system applies the language's default code page and associated fonts to your system.

7. Do the display settings need to be adjusted?

   ■ If *yes*, go to Step Step 8.

   ■ If *no*, go to Step 12.

8. From the **Control Panel** window, double-click the **Display** icon.

   The Display Properties window opens.

9. Select the **Appearance** tab, and then select a font size.

10. Click **Apply**.

11. Click **OK** to quit the **Display Properties** window.

12. From the **Regional Setting Properties** window, select the **Input Locales** tab.

13. Click **Add**.

    The **Add Input Locale** window opens.

14. Select the language from the list, and then click **OK**.

    The **Input Locales** tab appears.

15. In the **Installed input locales** field, click **Set as Default**.

    The system sets the language as the default input locale.

16. In the **Hot keys for input locales** field, select the shortcut key combinations for switching between input locales.

17. Select the **Enable indicator on taskbar** check box, and then click **OK**.

18. Click **Apply**.

    The **Regional Properties** window closes.

19. Restart the system.

    The system locale changes take effect.

Installing Multiple Sensors on a System

Introduction

You should install RealSecure Server Sensor on all your important servers, including computers that are running network sensors.

Server sensor installation configuration

If you install a RealSecure Server Sensor and a RealSecure Network sensor on the same computer, you must install server sensor using the custom installation option and you must disable the network monitoring component of the server sensor.

Enabling C2 Audit for AIX Platforms

Introduction

Before you can use the C2 auditing feature for sensors running on an AIX operating system, you must enable C2 auditing on the system.

Enabling C2 audit

To enable C2 audit:

1. Log on using a superuser account, such as **`root`**.
2. Type the following command:

   ```
   audit start
   ```

Disabling C2 audit

To disable C2 audit:

1. Log on using a superuser account, such as **`root`**.
2. Type the following command:

   ```
   audit shutdown
   ```

Enabling C2 Audit for HP-UX Platforms

Introduction

Before you can use the C2 auditing feature for sensors running on an HP-UX operating system, you must enable C2 auditing on the system.

Procedure

To enable C2 audit:

1. Log on using a superuser account, such as **`root`**.
2. Type the following command:

```
/usr/lbin/tsconvert
vi /etc/rc.config.d/auditing
```

3. Assign the following values to the listed variables:

Variable	Value	Example
AUDITING	1	
PRI_AUDFILE	<primary audit log file name>	/.secure/etc/audfile1
PRI_SWITCH	<max log file size in KB>	1000
SEC_AUDFILE	<secondary audit log file name>	/.secure/etc/audfile2
SEC_SWITCH	<max log file size in KB>	1000

4. Restart the auditing service.

Increasing the Size Limits for Per Process Memory on HP-UX Platforms

Introduction

You must increase the size limits for per process memory so that the sensor operates correctly.

Kernel parameters to configure

Increase per process memory size limits by configuring the following kernel parameters:

- `maxdsiz`
- `maxssiz`
- `maxtsiz`

Procedure

To configure the kernel parameters:

1. Log on using a superuser account, such as **`root`**.
2. Type the appropriate command for each kernel parameter listed above, as follows:
   - for HP-UX versions earlier than 11.23, type:
     ```
     usr/sbin/kmtune -s <parameter_name>=0x10000000
     ```
   - for HP-UX version 11.23, type:
     ```
     usr/sbin/kctune -s <parameter_name>=0x10000000
     ```

Enabling the Basic Security Module (BSM) on Solaris Platforms

Introduction

The Solaris BSM provides additional security features that are not supplied in standard UNIX. RealSecure Server Sensor can use information gathered by the BSM to ensure system integrity and security policy compliance. Without the BSM enabled, the sensor cannot detect certain security events.

Enabling the Basic Security Module (BSM)

To enable the BSM:

1. Log on using a superuser account, such as **root**.
2. Type the following command to run the BSM script and enable the BSM at startup:

   ```
   /etc/security/bsmconv
   ```

3. Type the following command:

   ```
   /etc/telinit 6
   ```

   The system goes into multi-user mode.
4. Restart the system.

   Note: You must restart the system before the changes to the BSM configuration take effect. Running the bsmconv script disables the Volume Manager, so after you have enabled the BSM, you must manually re-enable the Volume Manager or have the sensor installation script do it for you.

Reference: See the *SunSHIELD Basic Security Module Guide* for more information about the BSM. You can access this guide on the Sun Web site at the following location:

http://docs.sun.com/app/docs/doc/805-2635/6j2hbn761?l=en&a=view

Protecting an Apache Web Server

Introduction

If you plan to protect an Apache Web Server, you must know the following information to complete the installation process:

- name and location of the httpd executable and the httpd.conf file
- whether the modssl module is enabled

Note: RealSecure Server Sensor for HP-UX platforms does not inspect SSL-encrypted HTTP traffic.

Location of files

For more information about the location of the httpd executable and the httpd.conf file, see your Apache user documentation.

Modssl module

For more information about the modssl module, see your Apache user documentation.

Additional requirement

The Apache Web Server must support Dynamic Shared Object (DSO).

Chapter 4

Installing on a Windows Platform

Overview

Introduction

This chapter describes the sensor installation procedures for Windows environments.

Important

Before you install the sensor, be sure you read Chapter 3, "Before You Install RealSecure Server Sensor", which starts on page 21. Chapter 3 identifies prerequisites you *must* meet to ensure a successful installation.

In this chapter

This chapter contains the following topics:

Installation Options

Installation methods

Install the sensor for Windows platforms using one of the following methods:

- typical installation
- custom installation
- automated installation

Typical installation

If you do not plan to do any advanced configuration during the sensor installation process, use the typical installation option.

A typical installation uses the following default settings:

Option	Default Setting
Network monitoring component	Enabled
Enforce audit policy	Disabled When enabled, and audit-related signatures are enabled in the sensor policy, enforces the default audit policy, which provides the best protection for your system using recommendations from IBM ISS.
Blocking	Disabled When enabled, and you apply a predefined policy other than Blank_Windows.policy, blocks suspicious traffic using recommendations from IBM ISS.
Sensor name	server_sensor_1
Server sensor directory	C:\Program Files\ISS\issSensors\server_sensor_1
ISSDaemon directory	C:\Program Files\ISS\issDaemon
Key management	No key administrators
Cryptographic provider	RSA Built-In Provider, Strong Encryption Version
Automatic key import	Disabled
SSL monitoring	Enabled

Table 4: *Default installation settings*

Option	Default Setting
Restart WWW Publishing Service	Enabled

Table 4: *Default installation settings (Continued)*

Custom installation

If the settings for the typical installation do not meet your needs, use the Custom installation option.

Automated installation

If you intend to install RealSecure Server Sensor on more than one computer and all the sensors will have the same settings, use the Automated installation option. With this option, you respond to installation questions, save these responses to a response file, and then use the response file when you install other sensors. The Automated installation option allows you to install many sensors without having to monitor the each installation.

Silent installation

You can suppress the display of the installation prompts when you install server sensor. With this option, you use a response file in silent mode to specify the responses to installation questions as the sensor is installed.

Unpackaging the Installation Files

Introduction

If you download the installation package from the Web site, you must unpackage the files before you can install the sensor.

Unpackaging options

The following table lists the ways to unpackage the installation files:

For this type of installation...	To unpackage to...	Reference
Typical or Custom	a temporary directory and install the sensor immediately	See "Unpackaging files to temporary directory and installing the sensor immediately" on page 48.
Typical or Custom	a custom directory and install the sensor immediately	See "Unpackaging files to specific directory and installing the sensor immediately" on page 48.
Automated or Silent	a custom directory and install the sensor at a later time	See "Unpackaging files to specific directory without installing the sensor" on page 49.

Table 5: *Options for unpackaging installation files*

Unpackaging files to temporary directory and installing the sensor immediately

To unpackage the server sensor installation files:

1. Download the packaged file.
2. Double-click the packaged file.

   Note: This will extract the files and begin the installation process.

   Reference: See "Typical Installation" on page 50 or "Custom Installation" on page 52.

Unpackaging files to specific directory and installing the sensor immediately

To unpackage the server sensor installation files:

1. Select **Start→Run**.
2. In the **Run** window, change the command line in the **Open** box to:

   ```
   "full_path_to_installation_package" -p
   ```
3. Click **OK**.

4. Type the path or browse to the directory where the installation package should be unpackaged to.
5. Click **Next**.

   Note: This will extract the files and begin the installation process.

   Reference: See "Typical Installation" on page 50 or "Custom Installation" on page 52.

Unpackaging files to specific directory without installing the sensor

To unpackage the server sensor installation files:

1. Select **Start→Run**.
2. In the **Run** window, change the command line in the **Open** box to:

   "*full_path_to_installation_package***" -p**
3. Click **OK**.
4. Type the path or browse to the directory where the installation package should be unpackaged to.
5. Click **Next**.
6. Click **Cancel**.

   The installation files are unpackaged to the location you specified without installing the sensor.

   Reference: See "Automated Installation" on page 56 or "Silent Installation" on page 58.

Typical Installation

Introduction

The typical installation option uses default settings to quickly install the sensor.

Reference: For a list of the default settings, see Table 4, “Default installation settings” on page 46.

Procedure

To install a sensor on a Windows platform:

Important: The Typical installation option installs the SSL traffic monitoring component. As part of the installation process, the WWWPublishing Service is restarted.

1. Run the `RealSecureServerSensor70_SR4_4.exe` file.

   The Welcome window opens.
2. Click **Next**.

   The License Agreement window opens.
3. Read the text, and then click **I Accept**.

   The Readme window opens.
4. Read the text, and then click **Next**.

   The Setup Types window opens.
5. Click **Typical**.
6. If you are notified of pending file operations, do one of the following:
   - Click **Yes** to abort the installation, restart the system, and then resume the installation.
   - Click **No** to continue the installation process.

     Note: If you continue the installation process while there are pending file operations, the installation will continue but files with pending operations may be renamed or deleted when the system is next restarted due to the pending operation.

7. Continue through the installation questions. Use the following table as a guide:

Setting	Option
Automatic Key Import	Select **Allow Auto-Import** to send the initial authentication key from the Console over a standard network connection. **Important:** You must select this option if SiteProtector is using authentication. **Reference:** For more information, see “Automatically Importing Authentication Keys” on page 29.
Public Key Administrators	Do one of the following: • Type the IP address of the Console computer, and then click **Add**. • Type the name for the Console computer’s Public Key Administrator, and then click **Add**. Use the format `computername_username` **Important:** IBM ISS recommends that you add at least one key administrator at this time. If you do not add an administrator now, you must reinstall the component to set up a key administrator.

8. Click **Finish**.

Custom Installation

Introduction

Use the custom installation option to install specific components and to change default settings.

Procedure

To install a sensor using a custom configuration:

1. Run the `RealSecureServerSensor70_SR4_4.exe` file.

   The Welcome window opens.
2. Click **Next**.

   The License Agreement window opens.
3. Read the text, and then click **I Accept**.

   The Readme window opens.
4. Read the text, and then click **Next**.

   The Setup Types window opens.
5. Click **Custom**.

   The Select Components window opens.
6. Continue through the installation questions. Use the following table as a guide:

Setting	Option
Network monitoring component	Click **Next** to install the network monitoring component of the sensor.
Pending file operations	If you are notified of pending file operations, do one of the following: • Click **Yes** to abort the installation, restart the system, and then resume the installation. • Click **No** to continue the installation process. **Note:** If you continue the installation process while there are pending file operations, the installation will continue but files with pending operations may be renamed or deleted when the system is next restarted due to the pending operation.

Setting	Option
Enforce Audit Policy	Select the **Enforce Audit Policy** check box. **Important:** If you do not enforce an audit policy, the sensor will not monitor the system for important events such as login, startup, shutdown, registry access, and file access events. **Note:** When you enable EAP and apply a policy that has audit-related signatures enabled, the sensor provides the best protection for your system using recommendations from IBM ISS.
Blocking	Select the **Enable Blocking** check box to have the sensor block suspicious traffic immediately after the installation ends. **Note:** This option is only available if you are using the network monitoring capabilities of the server sensor. If you select this option, the sensor blocks suspicious traffic immediately upon installation using recommendations from IBM ISS.
Sensor name	Type a custom name for the sensor. **Note:** Use only alphanumeric characters with underscores for sensor names.
Installation directory (sensor)	Select an installation directory. **Important:** IBM ISS recommends that you accept the default location so that the setup program can locate important files that may have been installed previously. The default location is `C:\Program Files\ISS\issSensors\`*`sensor_name`*
Installation directory (daemon)	Select an installation directory. **Important:** IBM ISS recommends that you accept the default location `C:\Program Files\ISS\issDaemon`
Authentication Mode	Select **Next** to use authentication to secure communication between the sensor and the Console. **Important:** IBM ISS recommends that you use authentication to prevent unauthorized users from controlling and potentially hiding attacker activity. **Reference:** For information about authentication, see “Using Authentication” on page 27.

Setting	Option
Automatic Key Import	Select **Allow Auto-Import** to send the initial authentication key from the Console over a standard network connection. **Important:** You must select this option if SiteProtector is using authentication. **Reference:** For more information, see “Automatically Importing Authentication Keys” on page 29.
Public Key Administrators	Do one of the following: • Type the IP address of the Console computer, and then click **Add**. • Type the name for the Console computer’s Public Key Administrator, and then click **Add**. Use the format `computername_username` **Important:** IBM ISS recommends that you add at least one key administrator at this time. If you do not add an administrator now, you must reinstall the component to set up a key administrator.
Cryptographic providers	Add, change, or delete cryptographic providers. **References:** For more information, see “Customizing Encryption” on page 31 and “Working with Cryptographic Providers During a Windows Installation” on page 62.
Monitoring SSL traffic	Select **Install SSL traffic monitoring component** to have server sensor monitor traffic directed through SSL-encrypted HTTP streams on systems running Internet Information Services. **Note:** This option is only available if you are using the network monitoring capabilities of the sensor. **Important:** You must restart the WWW Publishing Service before this component can protect your system. Restart the service automatically as part of the installation process by selecting the **Restart the WWW Publishing Service** check box, or restart the service manually at a later time.

Setting	Option
Archive private keys	To archive a copy of the cryptographic provider's private key for this installation, specify the location for the archive copy and a passphrase to encrypt the copy. **Note:** The passphrase must be a minimum of seven characters in length. **Reference:** For more information, see "Archiving Private Keys" on page 64.

7. Click **Finish**.

Automated Installation

Introduction

You can use the Autorecord and Autoinstall features to automatically install a sensor.

Important: The automated installation does not provide the option to archive private keys.

Benefits

The Autorecord and Autoinstall features are useful when you want to install RealSecure Server Sensor on multiple systems.

Autorecord

In Autorecord mode, you can save your responses to the installation program prompts in a response file as you install a sensor. You can edit the response file as desired for use on systems configured differently from the original system. You can also manually create a response file that includes the desired responses.

Autoinstall

In Autoinstall mode, you can use the response file you created in Autorecord mode to install sensors on other systems. The Autoinstall feature reads your responses to installation prompts from the response file instead of requiring you to respond to the installation prompts.

Process overview

To install a sensor using the automated installation feature, you must do the following:

Task	Operation	Reference
1	Obtain the installation package	See “Unpackaging the Installation Files” on page 48.
2	Unpackage the installation package	See “Unpackaging files to specific directory without installing the sensor” on page 49.
3	Create an automated installation response file	See “Generating a response file” on page 57.
4	Install the sensor	See “Installing sensor with an automated installation response file” on page 57.

Table 6: *Tasks in the silent installation process*

Generating a response file

To generate a response file:

1. Locate the installation file `Setup.exe` in the directory where you unpackaged the installation files.
2. From the Start menu, select **Start**→**Run**.
3. In the **Run** window, change the command in the **Open** box to:

   ```
   "full_path_to_file\Setup.exe" -p
   full_path_to_response_file\response_file_name.rsp
   ```

   Example: `"d:\ServerSensor\Windows\Setup.exe" -p c:\temp\my_auto_inst_file.rsp`
4. Click **OK**.
5. Respond to the installation prompts.

   Reference: See "Typical Installation" on page 50 or "Custom Installation" on page 52.

Installing sensor with an automated installation response file

To install a sensor with an automated installation response file:

1. Locate the installation file `Setup.exe` in the directory where you unpackaged the installation files.
2. From the Start menu, select **Start**→**Run**.
3. In the **Run** window, change the command line in the **Open** box to:

   ```
   "full_path_to_file\Setup.exe" -g
   full_path_to_response_file\response_file_name.rsp
   ```

   Example: `"d:\ServerSensor\Windows\Setup.exe" -g c:\temp\my_auto_inst_file.rsp`
4. Click **OK**.
5. Check the autoinstall log to ensure the installation was successful.

Autoinstall log file

The installation program generates a log file in the Windows directory that contains error and other messages related to the automated installation. Always check this file for error messages after you complete an automated installation. The default log file name indicates the date and time of the installation and follows the following format:

```
RealSecure_Server_Sensor_7.0_SR4.4_xx-xx-
  2006_xx_xx_xx_install.xml
```

Silent Installation

Introduction

You can use the automated installation feature with InstallShield's Silent Install feature to suppress the display of the installation prompts when you install a sensor.

Process overview

To install a sensor using the silent installation feature, you must do the following:

Task	Operation	Reference
1	Obtain the installation package	See "Unpackaging the Installation Files" on page 48.
2	Unpackage the installation package	See "Unpackaging files to specific directory without installing the sensor" on page 49.
3	Create an automated installation response file **Note:** IBM ISS provides a response file, `server_sensor_typical.rsp`, for a Typical installation on English versions of Windows.	See "Generating a response file" on page 57.
4	**Note:** Only complete this task if you want to configure a key administrator before you use the `server_sensor_typical.rsp` response file to install a sensor. Configure communication with SiteProtector, before silent installation of the sensor, by defining a key administrator.	See "Task 4: Configuring communication with SiteProtector before silent installation" on page 59.
5	Install a sensor using the Silent Install feature	See "Task 5: Installing server sensor non-interactively" on page 59.

Table 7: *Tasks in the silent installation process*

Task	Operation	Reference
6	**Note:** Only complete this task if you did not configure a key administrator before you used the server_sensor_typical.rsp response file to install a sensor. Configure communication with SiteProtector, after silent installation of the sensor, by defining a key administrator.	See "Task 6: Configuring communication with SiteProtector after silent installation" on page 60.

Table 7: *Tasks in the silent installation process*

Task 4: Configuring communication with SiteProtector before silent installation

To configure communication with SiteProtector:

1. Open the `server_sensor_typical.rsp` file located in the directory where you unpackaged the installation package.
2. Add the following lines

   ```
   [KeyAdministrators]
   KeyAdministrator_1=xxx.xxx.xxx.xxx
   ```

   Where *xxx.xxx.xxx.xxx* is the IP address of the SiteProtector system.
3. Save the file, and then close the file.

Task 5: Installing server sensor non-interactively

To install server sensor non-interactively:

1. Locate the installation file `Setup.exe` in the directory where you unpackaged the installation files.
2. From the Start menu, select **Start→Run**.
3. In the **Run** window, type the following:

   ```
   "full_path_to_file\Setup.exe" -g
   full_path_to_response_file\response_file_name.rsp -s
   ```

   Example: `"d:\ServerSensor\Windows\Setup.exe" -g c:\temp\my_auto_inst_file.rsp -s`

Task 6: Configuring communication with SiteProtector after silent installation

To configure communication with SiteProtector:

1. Open the Services window.
2. Double-click the issDaemon service.
3. Click **Stop** to stop the sensor.
4. Open the `iss.access` file located in the `issDaemon` directory.
5. Add the following lines below the [\Roles\KeyAdministrator\] line:

   `[\Roles\KeyAdministrator\`*`xxx.xxx.xxx.xxx`***`\]`**
   `[\Roles\KeyAdministrator\`*`SiteProtector_Hostname`***`\]`**

   Where *`xxx.xxx.xxx.xxx`* is the IP address of the SiteProtector system, and *`SiteProtector_Hostname`* is the hostname of the SiteProtector system.
6. Save the file, and then close the file.
7. In the Services window, double-click the issDaemon service.
8. Click **Start** to start the sensor.

   The silently installed sensor begins communicating with SiteProtector.

Silent install log file

When you install a sensor using the silent installation option, the installation program generates a log file called `setup.log`. You can find the `setup.log` file in the directory where the `setup.ini` is located. You can specify an alternate silent install log file location using the `-f2` switch.

The following shows the contents of the setup.log file for a successful silent installation:

```
[InstallShield Silent]
Version=v6.00.000
File=Log File
[ResponseResult]
ResultCode=0
[Application]
Name=RealSecure Server Sensor 7.0 SR4.4
Version=7.0
Company=ISS
Lang=0009
```

Silent install log file result codes

After you install a sensor using the silent installation option, check the silent install log file `setup.log` to see if the setup succeeded. Table 8 lists the possible result codes and their meanings:

Result Code	Meaning
0	Success
-1	General error
-2	Invalid mode
-3	Required data not found in the Setup.iss file
-4	Not enough memory available
-5	File does not exist
-6	Cannot write to the response file
-7	Unable to write to the log file
-8	Invalid path to the InstallShield Silent response file
-9	Not a valid list type (string or number)
-10	Data type is invalid
-11	Unknown error during setup
-12	Dialog boxes are out of order
-51	Cannot create the specified folder
-52	Cannot access the specified file or folder
-53	Invalid option selected

Table 8: *Silent mode return codes*

Working with Cryptographic Providers During a Windows Installation

Introduction

Cryptographic providers encrypt communications between the Console and sensors, the Console and the event collector, and the event collector and sensors. Encrypting communications secures the information that is passed between these components.

Background

For more information about setting up encryption, see “Customizing Encryption” on page 31. For more information about changing cryptographic providers after you have installed a component, see “Restoring Archived Private Keys” on page 103.

Adding a provider

To add a provider during installation:

1. In the Cryptographic Providers window, click **Add**.
2. Select a provider from the list of providers installed on your system.

   Note: Add the RSA 1536 provider if it does not appear in the list.
3. Click **OK**.

Changing default algorithms for the provider

To change the default algorithms during installation:

1. Click **Add** to add the provider to customize.
2. Clear the **Use algorithm defaults** box.

   The Configure Algorithms window opens.
3. Choose an algorithm for each of the three categories.
4. Click **OK**.

   Important: You must use the same algorithm for the Console and each sensor. If you do not, the components cannot communicate with one another.

Deleting a provider

To delete a cryptographic provider during a Windows-based installation:

1. Select the provider that you do not want the Console to use.
2. Click **Delete**.

   Note: If you delete a provider by mistake, click **Add** to add it back to the list. Deleting a provider does not delete the public/private key pair associated with that provider configuration. If you later add the provider back to your configuration, the system uses the existing key pair rather than generating a new key pair.

Archiving Private Keys

Introduction

Use the Archive Private keys window to archive a copy of the cryptographic provider's private key that was created during installation.

Important: The setup program can only archive private keys when it creates them; it cannot archive existing private keys.

Benefit

If you archive a copy of the private key, you can recover the private key if it becomes damaged or destroyed. The archived copy of the private key is encrypted and passphrase protected.

If you choose not to archive the private key

If the private key becomes damaged or destroyed and you *do not have* an archived copy of the key, you must reinstall the component that has the damaged key to create a new private/public key pair, and then copy the new public key to other components.

Reference: For more information, see "Restoring Archived Private Keys" on page 103.

Archiving the private key

To archive the private key during installation:

1. Select the **Archive the private keys** check box.
2. Use the default location, or type a location in the **Save the key files in this folder** field.
3. Type a passphrase in the **Passphrase** box.
4. Type the passphrase in the **Confirm** box.
5. Click **Next**.

Bypass archiving

To bypass archiving during installation:

1. Clear the **Archive the private keys** check box.
2. Click **Next**.
3. Click **Next**.

   The Start Copying Files window opens.

4. Do the settings need to be adjusted?
   - If *yes*, click **Back** and adjust the settings as needed.
   - If *no*, click **Next**.

   The installation program reviews the bindings settings and displays a message that the bindings review is complete.
5. Click **OK**.

Chapter 5

Installing on a Solaris Platform

Overview

Introduction

This chapter describes the sensor installation procedures for Solaris environments.

Note: The installation package for RealSecure Server Sensor for Solaris includes all enhancements released with Service Release 4.3. When you install RealSecure Server Sensor for Solaris, the sensor will show as a version 7.0 sensor with Service Release 4.3 applied.

Limitation

RealSecure Server Sensor for Solaris platforms monitors activity on software that is part of the Trusted Computer Base (TCB). If you allow users to access the sensor with non-TCB software, such as Secure Shell (SSH) and GNU’s su, the sensor cannot monitor the user’s activity.

Important

Before you install the sensor, be sure you read Chapter 3, "Before You Install RealSecure Server Sensor", which starts on page 21. Chapter 3 identifies prerequisites you *must* meet to ensure a successful installation.

In this chapter

This chapter contains the following topics:

Installation Options

Installation options

You can install the sensor on a Solaris platform using one of the following options:

- typical
- custom
- automated

Container support

RealSecure Server Sensor for Solaris, Service Release 4.3 supports Containers on Solaris 10; however, if you install the sensor on non-global zones, the network monitoring component will not be installed.

Typical installation

If you do not need to customize any sensor installation settings, use the default settings provided by the Typical installation option.

A typical installation uses the following default settings:

Option	Setting
Installation directory	/opt/ISS
Sensor name	server_sensor_1
Automatic key import	Disabled
Key management	No key administrators
Cryptographic provider	RSA Built-In Provider, Strong Encryption Version
Blocking	Disabled When enabled, and you apply a predefined policy other than Blank_Solaris.policy, blocks suspicious traffic using recommendations from IBM ISS.
Enforce audit policy	Disabled When enabled, and audit-related signatures are enabled in the sensor policy, enforces the default audit policy, which provides the best protection for your system using recommendations from IBM ISS.

Table 9: *Typical installation settings*

Option	Setting
Network monitoring component	**Global Zone** Enabled Installs the network monitoring component. **Non-Global Zone** Disabled Does not install the network monitoring component.
Apache server monitoring	Enabled Checks for Apache Web server, prompts for Apache files, and installs the Apache monitoring component.

Table 9: *Typical installation settings (Continued)*

Custom installation

If you need to customize any installation settings, use the Custom installation option.

Automated installation

If you intend to install RealSecure Server Sensor on more than one computer and all the sensors will have the same settings, use the Automated installation option. With this option, you respond to installation questions, save these responses to a response file, and then use the response file when you install other sensors. The Automated installation option allows you to install many sensors without having to monitor each installation.

Typical Installation

Introduction

The typical installation option uses default settings to quickly install the sensor.

Reference: For a list of the default settings, see Table 9, "Typical installation settings" on page 68.

Prerequisite

The installation package for RealSecure Server Sensor for Solaris is stored in a tar file. Before you can install a server sensor, you must untar this file using the following command:

```
tar -xvf ServerSensor.tar
```

Procedure

To install a sensor on a Solaris platform:

1. Log on using a superuser account, such as **`root`**.
2. Copy the installation package to your local drive.
3. Type **`./pkgISSXssinstall.sh`**, and then press ENTER.
4. Press ENTER to install all the files that are in the package.
5. Type **`y`** to read the license agreement.
6. Type **`y`** to accept the license agreement.
7. Type **`y`** to install the sensor with the default parameters.
8. Continue through the installation questions. Use the following table as a guide:

Setting	Option
Full path to the Apache httpd program file	Type the full path to the Apache program file you want to protect, and then press ENTER.
Full path to the Apache httpd.conf file	Type the full path to the Apache configuration file you want to protect, and then press ENTER.

9. Restart the computer.

Custom Installation

Introduction

Use the custom installation option to install specific components and to change default settings.

Prerequisite

The installation package is stored in a tar file. Before you can install a sensor, you must untar this file using the following command:

```
tar -xvf ServerSensor.tar
```

Procedure

To install a sensor using a custom configuration:

1. Log on using a superuser account, such as **`root`**.
2. Copy the installation package to your local drive.
3. Type **`./pkgISSXssinstall.sh`**, and then press ENTER.

   The installation package opens.
4. Press ENTER to install the package.
5. Type **`y`** to read the license agreement.
6. Type **`y`** to accept the license agreement.
7. Type **`n`** to install the sensor with custom parameters.
8. Continue through the installation questions. Use the following table as a guide:

Setting	Option
Installation directory	Do one of the following: • Press ENTER to use the default directory (/opt/ISS). • Type the path to the directory you want to use. **Note**: The sensor creates a symlink from /opt/ISS to the custom directory you specify.
Sensor name	Type a custom name for the sensor. **Note:** Use only alphanumeric characters with underscores for sensor names.

Setting	Option
Automatically import authentication key	Type **y** to have the sensor receive the initial authentication key over a standard network connection initiated from the console. **Important:** SiteProtector users must select this option if using authentication. **Reference:** For more information, see "Automatically Importing Authentication Keys" on page 29.
Key management	Type **y** to set up key administrators. **Note:** You can set up more than one key administrator. Use the format *computername_username* or *computername*.
BSM auditing	If BSM auditing is not enabled, do one of the following: • Type **y** to continue the installation with BSM auditing disabled. **Note:** If the BSM is not enabled, the sensor cannot detect certain security events. • Type **n** to exit the installation program. **Reference:** See "Enabling the Basic Security Module (BSM) on Solaris Platforms" on page 43.
Enforce audit policy	Type **y** to enable enforce audit policy (EAP). **Note:** When you enable EAP, and audit-related signatures are enabled in the sensor policy, the sensor enforces the default audit policy, which provides the best protection for your system using recommendations from IBM ISS.
Network monitoring component	Type **y** to install the network monitoring component of the sensor.
Enable blocking	Type **y** to have the sensor block suspicious traffic immediately after the installation ends. **Note:** This option is only available if you are using the network monitoring capabilities of the sensor. If you select this option, the sensor blocks suspicious traffic immediately upon installation using recommendations from IBM ISS.

Setting	Option
Full path to the Apache httpd program file	Type the full path to the Apache program file you want to protect, and then press ENTER.
Full path to the Apache httpd.conf file	Type the full path to the Apache configuration file you want to protect, and then press ENTER.

9. Restart the computer.

Automated Installation

Introduction

You can install RealSecure Server Sensor on Solaris systems automatically if you use pkgask to generate a response file and use an admin file to suppress the run package setup scripts confirmation request from the pkgadd command.

Process overview

The following table outlines the process for completing an automated installation of the sensor:

Task	Description
1	Untar the installation package.
2	Generate a response file.
3	Create an admin file.
4	Install the sensor.

Task 1: Untar the installation package

The installation package is stored in a tar file. Before you can install the sensor, you must untar this file.

Untarring the package

To untar the installation package:

- Run the following command:

```
tar -xvf ServerSensor.tar
```

Task 2: Generate a response file

The pkgask command runs the request script for a package and stores the information necessary to install the package. The request script is similar to pkgadd, but no files are installed.

Important: You cannot generate a response file on a system that already has a sensor installed.

Generating a response file

To generate a response file:

1. Run the following command:

   pkgask -d *full_path_and_name_of_installation_image* **-r** *full_path_to_response_file*

   Example: `pkgask -d /tmp/Sensor/pkgISSXss -r /tmp/ssResponse`

2. Respond to the installation prompts.

   Reference: See "Typical Installation" on page 70 or "Custom Installation" on page 71.

Task 3: Create an admin file

An admin file contains installation parameters for the Solaris package administration commands. You must use an admin file to install a sensor because the installation package contains shell scripts that are run with superuser (or root) permissions. To run `pkgadd` non-interactively for a package that has installation scripts, you must specify an admin file, and then turn off these checks.

The admin file should contain, at a minimum, the following line:

```
action=nocheck
```

Task 4: Install the sensor non-interactively

After you have created the response and admin files, you can run `pkgadd` in a non-interactive mode to install sensors on identical systems.

Installing a sensor

To install a sensor using the response file:

1. Run the following command:

   pkgadd -n -r *full_path_to_response_file* **-a** *full_path_to_admin_file* **-d** *full_path_and_name_of_installation_image* **all**

   Note: If you have to use two lines to enter this command, then type a backslash (\) at the end of the first line so that the shell does not create new lines.

   Example:
   ```
   pkgadd -n -r /tmp/ssResponse -a /tmp/rs_admin \
   -d /tmp/Sensor/pkgISSXss all
   ```

2. Restart the computer.

Chapter 6

Installing on an AIX Platform

Overview

Introduction

This chapter describes the sensor installation procedures for AIX environments.

Note: The installation package for RealSecure Server Sensor for AIX includes all enhancements released with Service Release 4.2. When you install RealSecure Server Sensor for AIX, the sensor will show as a version 7.0 sensor with Service Release 4.2 applied.

Important

Before you install the sensor, be sure you read Chapter 3, "Before You Install RealSecure Server Sensor", which starts on page 21. Chapter 3 identifies prerequisites you *must* meet to ensure a successful server sensor installation.

In this chapter

This chapter contains the following topics:

Installation Options

Installation methods

Install the sensor on an AIX platform using one of the following options:

Note: You can only install one sensor on each instance of an AIX operating system.

- typical
- custom
- automated

LPAR support

The following versions of RealSecure Server Sensor for AIX support LPARs:

- Service Release 4.1 supports LPAR on AIX 5.1, 5.2, and 5.3.
- Service Release 4.2 supports LPAR on AIX 5.2, 5.3, and 6.1.

WPAR support

RealSecure Server Sensor for AIX, Service Release 4.2 supports system WPARs on AIX 6.1.

Typical installation

If you do not need to customize any sensor installation settings, use the default settings provided by the typical installation option.

A typical installation uses the following default settings:

Option	Setting
Installation directory	/opt/ISS
Sensor name	server_sensor_1
Automatic key import	Enabled **Note:** In Service Release 4.1 and earlier, automatic key import is disabled by default.
Key management	No key administrators
Cryptographic provider	RSA Built-In Provider, Strong Encryption Version

Table 10: *Typical installation settings*

Option	Setting
Blocking	Disabled When enabled, and you apply a predefined policy other than Blank_AIX.policy, blocks suspicious traffic using recommendations from IBM ISS.
Enforce audit policy	Disabled When enabled, and audit-related signatures are enabled in the sensor policy, the sensor enables the necessary audit flags to provide the best protection for your system using recommendations from IBM ISS.
Network monitoring component	Enabled Installs the network monitoring component.

Table 10: *Typical installation settings (Continued)*

Custom installation

If you need to customize any installation settings, use the custom installation option.

Note: When installing the sensor to the trusted computing base, you cannot use a custom installation path; you can, however, customize other installation options.

Automated installation

If you intend to install RealSecure Server Sensor on more than one computer and all the sensors will have the same settings, use the automated installation option. With this option, you respond to installation questions, save these responses to a response file, and then use the response file to install other sensors. The automated installation option allows you to install many sensors without having to monitor each installation.

Sync command installation

If you intend to install RealSecure Server Sensor in a workload partition environment, the preferred method is to use the sync commands. See “Installation Options for Workload Partition Environments” on page 85.

AIX version 6.1 introduced workload partitions (WPARs). WPARs are virtualized operating system environments that are created within a single AIX image.

Typical Installation

Introduction

The typical installation option uses default settings to quickly install RealSecure Server Sensor.

Reference: For a list of the default settings, see Table 10, "Typical installation settings" on page 78.

Installing a sensor

To install a sensor on an AIX platform:

1. Log on using a superuser account, such as **`root`**.
2. Copy the installation package to your local drive.
3. Type **`./ServerSensor-AIX-7-0.shar`**, and then press ENTER.
4. Type **`y`** to read the license agreement.
5. Type **`y`** to accept the license agreement.
6. Type **`y`** to install the sensor with the default parameters.

   The program completes the installation and removes all temporary files created during the installation.

Custom Installation

Introduction

Use the custom installation option to specify which components to install and to change any default settings.

Installing a sensor

To install a sensor on an AIX platform:

1. Log on using a superuser account, such as **`root`**.
2. Copy the installation package to your local drive.
3. Type **`./ServerSensor-AIX-7-0.shar`**, and then press ENTER.
4. Type **`y`** to read the license agreement.
5. Type **`y`** to accept the license agreement.
6. Type **`n`** to install the sensor with custom parameters.
7. Continue through the installation. Use the following table as a guide:

Option	Setting
Installation directory	Do one of the following: • Press enter to use the default (/opt/ISS). **Important:** If the opt/ISS directory already exists, the system backs it up and renames it /opt/ISS.bak. • Type the path to the directory you want to use. **Important:** You cannot use a custom installation path when installing to the trusted computing base. **Note:** The path cannot be a sub-directory of /opt/ISS. **Note:** If the /*`custom_path`*/ISS directory already exists, the system backs it up and renames it /*`custom_path`*/ISS.bak. **Note:** On AIX 6.1 systems the sensor relocates the installation files to an /opt/ISS subdirectory in the custom directory; all other installations create a symlink from /opt/ISS to the custom directory.

Option	Setting
Sensor name	Type `y`, and then type a custom name for the sensor. **Note:** Use only alphanumeric characters with underscores for sensor names. **Note:** The sensor creates a symlink from the custom sensor name you specify to /*path*/ISS/issSensors/server_sensor_1.
Automatically import authentication key	Type `y` to have the sensor receive the initial authentication key over a standard network connection initiated from the Console. **Important:** SiteProtector users must select this option if using authentication.
Key management	Do one of the following: • Type the IP address of the Console computer. • Type the name for the Console computer's Public Key Administrator. Use the format *computername_username* **Important:** You should add at least one key administrator at this time; if you do not add an administrator now, you must reinstall the sensor to set up a key administrator.
Enforce audit policy	Type `y` to enable enforce audit policy (EAP). **Note:** When you enable EAP, and audit-related signatures are enabled in the policy, the sensor enables the necessary audit flags to provide the best protection for your system using recommendations from IBM ISS.
Network monitoring component	Type `y` to install the network monitoring component of the sensor.
Enable blocking	Type `y` to have the sensor block suspicious traffic immediately after the installation completes. **Note:** This option is only available if you are using the network monitoring capabilities of the sensor. If you select this option, the sensor blocks suspicious traffic immediately upon installation using recommendations from IBM ISS.

Automated Installation

Introduction

You can automatically install a sensor on an AIX platform using the automated installation option.

Process overview

The following table outlines the process for completing an automated installation:

Task	Description
1	Generate a response file.
2	Install the sensor non-interactively.

Task 1: Generate a response file

You can save your responses to the installation program prompts in a response file. You can then use that response file to install other sensors without having to monitor each installation.

Important: You cannot generate a response file on a system that already has a sensor installed.

Generating a response file

To generate a response file:

1. Log on using a superuser account, such as **`root`**.
2. Copy the installation package to your local drive.
3. Run the following command:

   `./ServerSensor-AIX-7-0.shar -c` *`response_filename`*

   Example: `./ServerSensor-AIX-7-0.shar -c MyResponseFile`

   Note: The response file name cannot start with a hyphen (-).

   Note: If you specify a path in addition to the filename, the response file is placed in the specified location.
4. Respond to the installation prompts.

   Reference: See “Typical Installation” on page 80 or “Custom Installation” on page 81.

Task 2: Install the sensor

After you create the response file, you can install sensors on other systems using the response file. When you use the response file to install a sensor, you do not need to respond to the installation prompts each time you install a sensor.

Installing a sensor

To install the sensor using the response file:

- Run the following command:

  ./ServerSensor-AIX-7-0.shar -r *full_path_to_response_file*

  Example: `./ServerSensor-AIX-7-0.shar -r /var/MyResponseFile`

  Note: Replace *full_path_to_response_file* with the location and name of the response file you created in the previous task.

Installation Options for Workload Partition Environments

Introduction

There are several installation options available when you install RealSecure Server Sensor for AIX, Service Release 4.2 on an AIX 6.1 to system workload partition environments. Use Table 11 to identify your installation environment, and then use the referenced procedure to complete the installation.

Note: Workload partitions were introduced with AIX version 6.1.

Installation options in workload partition environments

When you install the sensor in a workload partition environment, you have the following options:

Option	Description	Reference
install in the global partition and sync to the workload partitions	The installation places the sensor files in the /opt directory of the global environment. Read-only files are shared from the global environment to the workload partitions. The network monitoring component of the sensor resides in the global partition and monitors all network traffic to and from the workload partitions. **Note:** This allows the workload partition to share files from the global partition and thus reduces the installation footprint. **Important:** On Trusted AIX systems, this is the only supported installation method.	“Preferred method” on page 87
install in the global partition and install in the workload partitions	The installation places the sensor files in the global environment; all sensor files are also installed in the workload partition. The network monitoring component of the sensor resides in the global partition and monitors all network traffic to and from the workload partitions.	“Alternate method” on page 88

Table 11: *Workload partition installation options*

Option	Description	Reference
install in only the workload partition	The installation places all sensor files in the specified directory. **Important:** When you install only in the workload partition, the network monitoring component of the sensor is not installed.	“Installing in Only a Workload Partition” on page 89

Table 11: *Workload partition installation options (Continued)*

Workload partitions and network monitoring

The network monitoring component of the sensor cannot be installed in the workload partition. If you want the protection offered by the network monitoring component, choose an installation option that installs the sensor in the global environment and also in the workload partition; in this configuration the network monitoring component on the global partition monitors network traffic in the workload partitions.

Workload partitions created after sensor installation

If you install the sensor in the global partition and then, at a later time, create a new workload partition, the system will automatically synchronize the installation to the new workload partition.

Installing in Global and Workload Partition Environments

Introduction

Use one of the procedures in this topic to install the sensor if your environment includes workload partitions and you want to install the sensor to both the global environment and the workload partition.

Preferred method

To install the sensor in both the global and workload partitions:

Important: Use this option if you must have the network monitoring component of the sensor.

1. Install the sensor in the global environment using one of the following methods:

Method	Description
typical installation	See “Typical Installation” on page 80.
custom installation	**Important:** You must accept the default installation directory. See “Custom Installation” on page 81.

2. To install to the workload partition, use one of the following methods:

Method	Description
syncwpar *partition_name*[1]	Executed from the global environment, this command synchronizes a specific partition with the global environment.
syncwpar -A[1]	Executed from the global environment, this command synchronizes all of the available system workload partitions with the global environment.
syncroot[1]	Executed from a workload partition, this command synchronizes the partition with the global environment.

[1] This installs any writable files in the /var/ISS directory on the workload partition and creates a symlink to any read-only components, which remain in the global environment.

Alternate method

To install the sensor in both the global and workload partitions:

Important: This installation method is not supported on Trusted AIX systems.

Note: This does not make the best use of space as you are not sharing any resources from the global environment to the workload partition.

1. Install the sensor in the global environment using one of the following methods:

Method	Description
typical installation	See “Typical Installation” on page 80.
custom installation	See “Custom Installation” on page 81. **Note:** As you are not synchronizing the installation to the workload partition, you can install to any directory in the global partition.

2. Install the sensor in the workload partition using one of the following methods:

Method	Description
typical installation	See “Typical Installation” on page 80.
custom installation	See “Custom Installation” on page 81. **Important:** If /opt is read-only, you must specify a custom installation location; if /opt is read-write, you can install to any location.

Installing in Only a Workload Partition

Introduction

Use one of the procedures in this topic to install the sensor if your environment includes workload partitions but you want to install in only the workload partition.

Important: This installation method is not supported on Trusted AIX systems.

Procedure

To install the sensor in only the workload partition:

Important: When you install in only the workload partition, the sensor does not provide network monitoring.

- Use one of the following methods:

If /opt is...	Then...
read-only	See “Custom Installation” on page 81. **Important:** You must specify a custom installation directory as /opt is read-only.
read-write	Use one of the following installation methods: • “Typical Installation” on page 80 • “Custom Installation” on page 81 **Note:** You can specify any installation directory as /opt is read-write.

Chapter 7

Installing on an HP-UX Platform

Overview

Introduction

This chapter describes the sensor installation procedures for HP-UX environments.

Note: The installation package for RealSecure Server Sensor for HP-UX includes all enhancements released with Service Release 4.1. When you install RealSecure Server Sensor for HP-UX, the sensor will show as a version 7.0 sensor with Service Release 4.1 applied.

Important

Before you install the sensor, be sure you read Chapter 3, "Before You Install RealSecure Server Sensor", which starts on page 21. Chapter 3 identifies prerequisites you *must* meet to ensure a successful installation.

In this chapter

This chapter contains the following topics:

Installation Options

Installation methods

You can install the sensor on an HP-UX platform using one of the following options:

- typical
- custom
- automated

Typical installation

If you do not need to customize any sensor installation settings, use the default settings provided by the Typical installation option.

A typical installation uses the following default settings installation:

Option	Setting
Installation directory	/opt/ISS
Key management	No key administrators
Network monitoring component	Enabled Installs the network monitoring component.
Blocking	Disabled When enabled, and you apply a predefined policy other than Blank_HP-UX.policy, blocks suspicious traffic using recommendations from IBM ISS.
Enforce audit policy	Disabled When enabled, and audit-related signatures are enabled in the sensor policy, enforces the default audit policy, which provides the best protection for your system using recommendations from IBM ISS.
Automatic key import	Disabled
Sensor name	server_sensor_1
Cryptographic provider	RSA Built-In Provider, Strong Encryption Version

Table 12: *Typical installation settings*

Custom installation

If you need to customize any installation settings, use the Custom installation option.

Automated installation

If you intend to install RealSecure Server Sensor on more than one computer and all the sensors will have the same settings, use the Automated installation option. With this option, you respond to installation questions, save these responses to a response file, and then use the response file when you install other sensors. The Automated installation option allows you to install many sensors without having to monitor the each installation.

Typical Installation

Introduction

The typical installation option uses default settings to quickly install the sensor.

Reference: For a list of the default settings, see Table 12, “Typical installation settings” on page 92.

Prerequisite

The files needed to complete the installation process are stored in a compressed file. Before you install a sensor, open the installation package using the **`gunzip`** command.

Restriction

You can only install one sensor on a computer that runs on an HP-UX platform.

Procedure

To install a sensor on an HP-UX platform:

1. Log on using a superuser account, such as **`root`**.
2. Copy the installation package to your local drive.
3. Type *`full path and name of installation image`*.

   Note: The full path to the installation image is the location and file name of the sensor installation file.

   Example: `# /usr/sbin/swinstall -s` *`full_path_and_name_of_installation_image`* `-x ask=as_needed ISSXss`

   The license agreement appears.
4. Type **`y`** to accept the license agreement.
5. Type **`y`** to install the sensor with the default parameters.
6. Type **`y`** to restart the system.

   Note: The sensor inserts itself as a shim into the communication stack; because of operating system restrictions, you must restart the system before the sensor can operate effectively.

Custom Installation

Introduction

Use the custom installation option to install specific components and to change default settings.

Prerequisite

The files needed to complete the installation process are stored in a compressed file. Before you install a sensor, open the installation package using the **`gunzip`** command.

Restriction

You can only install one sensor on a computer that runs on an HP-UX platform.

Procedure

To install a sensor on an HP-UX platform:

1. Log on using a superuser account, such as **`root`**.
2. Copy the installation package to your local drive.
3. Type *`full path and name of installation image`*.

   Note: The full path to the install image is the location and file name of the server sensor installation file.

   Example: `# /usr/sbin/swinstall -s` *`full_path_and_name_of _installation_image`* `-x ask=as_needed ISSXss`

   The license agreement appears.
4. Type **`y`** to accept the license agreement.
5. Type **`n`** to install the sensor with custom parameters.
6. Continue through the installation questions. Use the following table as a guide:

Setting	Option
Enforce audit policy	Type **y** to enable enforce audit policy (EAP). **Note:** When you enable EAP, and audit-related signatures are enabled in the sensor policy, the sensor enforces the default audit policy, which provides the best protection for your system using recommendations from IBM ISS.

Setting	Option
Network monitoring component	Type **y** to install the network monitoring component of the sensor.
Enable blocking	Type **y** to have the sensor block suspicious traffic immediately after the installation ends. **Note:** This option is only available if you are using the network monitoring capabilities of the sensor. If you select this option, the sensor blocks suspicious traffic immediately upon installation using recommendations from IBM ISS.
Automatically import authentication key	Type `y` to have the sensor receive the initial authentication key over a standard network connection initiated from the console. **Important:** SiteProtector users must select this option if using authentication. **Reference:** For more information, see “Automatically Importing Authentication Keys” on page 29.
Sensor name	Type a custom name for the sensor. **Note:** Use only alphanumeric characters with underscores for sensor names.
Key management	Type **y** to set up key administrators. **Note:** You can set up more than one key administrator. Use the format *`computername_username`*.
Restart the computer automatically	The sensor inserts itself as a shim into the communication stack; because of operating system restrictions, you must restart the system before the sensor can operate effectively. Do one of the following: • Type **y** to automatically restart the server as part of the installation process. • Type **n**, restart the server, and then start the sensor.

Automated Installation

Introduction

You can install RealSecure Server Sensor on HP-UX systems automatically if you use the `swask` command. The `swask` command does the following:

- generates a catalog that contains a response file
- places `swinstall` in non-interactive mode

About catalogs

A catalog is a directory that contains files that store installation parameters for HP-UX administration commands. One of these files contains responses to questions asked by the request script for an HP-UX package. The `swask` command generates this file together with the remainder of the catalog.

About the swask command

The `swask` command runs the request script for a package and stores the information necessary to install the package. The request script operates similarly to `swinstall` to install the package, but does not actually install files.

Process overview

The following table outlines the process for completing an automated installation of the sensor:

Task	Description
1	Generate a response file.
2	Run swinstall non-interactively

Generating a response file

To generate a response file:

1. Run the following command:

   swask -s *full_path_and_name_of_installation_image* **-c** *full_path_to_catalog* **-x ask=true ISSXss**

   Example: `swask -s /temp/RealSecure/ServerSensor.depot -c /var/temp/ServerSensor.depot -x ask=true ISSXss`

2. Respond to the installation prompts.

   Reference: See "Typical Installation" on page 94 or "Custom Installation" on page 95.

Non-interactive installation

After you create a catalog using `swask`, you can run `swinstall` in non-interactive mode.

Running swinstall non-interactively

To run swinstall non-interactively:

- Run the following command:

  `swinstall -s` *`full_path_and_name_of_installation_image`* **`-c`** *`full_path_to_catalog`* **`ISSXss`**

Example:

```
swinstall -s /temp/RealSecure/ServerSensor.depot -c /var/
temp/ServerSensor.depot ISSXss
```

Chapter 8

After You Install RealSecure Server Sensor

Overview

Introduction

After you install a sensor, there are certain tasks you must complete before you begin to configure your sensor to protect your server.

Reference: For general information about setting up sensors to work with SiteProtector, see the *SiteProtector Configuration Guide*.

In this chapter

This chapter contains the following topics:

Allowing Communication Between the Sensor and SiteProtector

Introduction

If you install RealSecure Server Sensor for Windows on a system that is running ISA Server, ISA Server blocks communication between the sensor and SiteProtector.

Allowing communication

To allow communication between the sensor and SiteProtector, you must configure the ISA server to allow incoming connections to port 2998 and port 902.

Configuring Authentication Manually

Introduction

If you did not enable the automatic authentication key import option for all your components, then you must copy the authentication keys manually.

Purpose

After you install a sensor or event collector on a remote system, the component must have one or more of the Console's public authentication keys and one or more of the event collector's authentication keys before the component and the Console can communicate.

Reference: For more information about how authentication works, see "Using Authentication" on page 27.

About the Keys directory

Each component has its own `Keys` directory. This directory contains the component's public authentication keys after installation and must contain the public authentication key of any component that is authenticated.

Location of authentication keys

The following table lists the location of authentication keys:

Component	Platform	Key location
Console	n/a	\Program Files\ISS\SiteProtector\Application Server\keys\RSA\sp_con_*machine name_ length*.PubKey[1] —and— \Program Files\ISS\SiteProtector\Application Server\keys\CerticomNRA\sp_con_*machine name_length*.PubKey[2]
Event collector	n/a	\Program Files\ISS\SiteProtector\Event Collector\Keys\RSA\rs_eng_*machine name_length*.PubKey[1] —and— \Program Files\ISS\SiteProtector\Event Collector\Keys\CerticomNRA\rs_eng_*machine name_length*.PubKey[2]

Table 13: *Location of authentication keys*

Component	Platform	Key location
Sensor	Windows	\Program Files\ISS\issSensors\sensor name\Keys\RSA\rs_eng_*machine name_length*.PubKey —and— \Program Files\ISS\issSensors\sensor name\Keys\CerticomNRA\rs_eng_*machine name_length*.PubKey[2]
	Unix	/opt/ISS/issSensors/*sensor name*/Keys/RSA/rs_eng_*machine name_length*.PubKey[1] —and— /opt/ISS/issSensors/*sensor name*/Keys/CerticomNRA/rs_eng_*machine name_length*.PubKey[2]

Table 13: *Location of authentication keys (Continued)*

[1] Unix sensors do not use 1024 bit RSA encryption keys, therefore, you do not need to copy these keys to the RSA directory.

[2] Although Certicom encryption is available for backward compatibility, it will not be supported in future releases.

Which keys go where

You must copy the public authentication keys of the following components:

- copy Console keys to the event collector and to the sensors
- copy event collector keys to the sensors

Restoring Archived Private Keys

Introduction

If you installed a component on a Windows platform, you had the option to archive your private keys at the end of the installation process. Unix installations do not provide this option.

Uses for archived keys

If you archived your keys, you can use the archived copy to restore your system, if, for example:

- the hardware on which you installed a component is damaged, and must load it onto a new computer
- the Windows Registry is corrupted and your private keys are inaccessible.

Prerequisites

Before you restore the archived private keys:

- Contact Technical Support for a copy of the Key Management utility.
- Locate a copy of the archived keys.
- Install the same providers the previous Console used.

Important: The archived copy of the private key is encrypted and protected with a passphrase. You must have the passphrase to restore the archived private key.

Restore Cryptographic Private Keys utility

The Restore Cryptographic Private Keys utility allows you to restore private keys.

Procedure

To restore archived private keys:

1. Double–click `setup.exe` to access the Utilities setup program.

   The Welcome window opens.

2. Select **Restore cryptographic private keys**.

   The Restoring the Archived Private Key window opens.

3. Type the path of the folder where the archived key is stored in the **Get the key files from the directory** field, or click **Browse** to search for the folder.

4. Type the passphrase in the **Passphrase** field.
5. Type the passphrase in the **Confirm** field.
6. Click **Next**.

   After the restore process completes, the setup program terminates. If the setup program was unsuccessful in restoring the keys, it reports an error. Possible causes of failure include corrupted private key archives, incorrect passphrase, or different key names.

Unable to restore archived private keys

If you are unable to restore your private keys from their archives, you must reinstall the management Console and generate new public/private keys.

Important: Reinstalling the Console generates new cryptographic keys. You must distribute the new public keys to all sensors that you manage from this Console.

Changing Encryption Providers

Introduction

To change the cryptographic provider for a sensor or an event collector, you must uninstall and then reinstall the component with the new settings.

Available daemon encryption providers

Available daemon encryption providers and corresponding algorithms are as follows:

Provider	Algorithms
Microsoft Enhanced 1536	Exch:RSA_KEYX/1536 Secret:3DES/168 Hash:SHA1/160
Microsoft Enhanced 1024	Exch:RSA_KEYX/1024 Secret:RC4/128 Hash:SHA1/160
ISS ECNRA	Exch:EC_KEYX/239 Secret:DESX/168 Hash:SHA1/160

Table 14: *Daemon encryption providers and algorithms*

Changing the cryptographic provider on UNIX platforms

To change to RSA encryption:

1. Stop the sensor using one of the following commands:
   - on Solaris systems, type **`/etc/init.d/realsecure stop`**
   - on AIX systems, type **`/opt/ISS/issSensors/`***`sensor_name`***`/realsecure stop`**
   - on HP-UX systems, type **`/sbin/init.d/realsecure stop`**
2. In the `/opt/ISS/issDaemon/` directory, run the crypto_setup.sh shell script.
3. Select the RSA provider.
4. In the `/opt/ISS/issSensors/`*`sensor_name`* directory, run the `crypto_setup.sh` shell script.

5. Select the RSA provider.
6. Start the sensor using the following command:
   - on Solaris systems, type **`/etc/init.d/realsecure start`**
   - on AIX systems, type **`/opt/ISS/issSensors/`***`sensor_name`***`/realsecure start`**
   - on HP-UX systems, type **`/sbin/init.d/realsecure start`**

Changing the cryptographic provider on Windows platforms

To change to RSA encryption on Windows platforms:

Prerequisite: Obtain the IBM ISS Key Management 7.0 utility from the Download Center (`http://www.iss.net/download`).

1. Copy the Key Management utility to any location on the system where a sensor is installed.
2. In **Services**, stop the issDaemon.
3. Double-click `Setup.exe` to run the utility.
4. Click **Next** until the screen with the option for Utilities and Create Cryptographic Keys appears.
5. Select **Utilities**, select **Create Cryptographic Keys**, and then clear all other options.
6. Click **Next**.
7. Type the path to the sensor directory.

   Note: The default location is `c:\Program Files\ISS\issSensors\server_sensor_1`
8. Select **Managed Component**.
9. Verify that the cryptographic providers on the next screen are RSA 1024, RSA 1536, or both.
10. Click **Next**.
11. Click **Next**.
12. Archive your keys.
13. Click **Next**.

    The system generates new keys.

Adding Key Administrators

Introduction

To allow a user to transfer authentication keys or other files to and from sensors, the user must have key administrator status.

General procedure

You can add a key administrator to a sensor from the Console if you selected at least one key administrator when you installed the sensor.

Key administrators and multiple sensors

When you designate a key administrator for one component, that administrator automatically becomes the key administrator for any other component installed on the same computer.

Reference

For information about using the Console to add a key administrator, see the SiteProtector Help.

Windows

For Windows-based sensors, you must set up at least one key administrator during the installation process or enable auto-import during installation (the first person to connect to the sensor gains key administrator rights).

Unix

If you did not configure a key administrator during the installation process, you can use a script from the command line to add a key administrator later. Run the **`keyadmin_setup.sh`** command in the `/opt/ISS/issDaemon/` directory

Monitoring Local Syslog Events

Introduction

Before the sensor can monitor for local syslog events, you must configure the `syslog.conf` file.

Procedure

To configure the `syslog.conf` file:

1. Open the syslog configuration file, `/etc/syslog.conf`, using a text editor.

   Example: `vi /etc/syslog.conf`

2. Add the following line:

   ```
   *.info    /path/messages_file
   ```

   This line of text identifies the path to your syslog file. The default path is `/var/adm/messages`.

   Example: `*.info    /var/adm/messages`

3. To use the new syslog.conf file, do one of the following:

1. Open the syslog configuration file, `/etc/syslog.conf`, using a text editor.

   Example: `vi /etc/syslog.conf`

2. Add the following line:

   ```
   *.info    /path/messages_file
   ```

   This identifies the path to your syslog file. The default path is `/var/adm/messages`.

   Example: `*.info    /var/adm/messages`

3. To use the new syslog.conf file, do one of the following:

To...	Type...
restart the syslog daemon on AIX systems	**`refresh -s syslogd`**

restart the syslog daemon on Solaris systems	**`/etc/init.d/syslog stop`**
	`/etc/init.d/syslog start`

restart the syslog daemon on HP-UX systems	**`/sbin/init.d/syslogd stop`**
	`/sbin/init.d/syslogd start`

To...	Type...

reread the syslog.conf file	**`kill -HUP`**
	`syslogd_process_id`

Monitoring the Mail Subsystem on HP-UX Systems

Introduction

HP-UX systems log messages generated by the mail subsystem to /var/adm/syslog/mail.log. Before server sensor can monitor events generated by the mail subsystem, you must configure the mail messages to be logged to the syslog.

Procedure

To log mail subsystem messages to the syslog:

1. Open the syslog configuration file, `/etc/syslog.conf`, using a text editor.

   Example: `vi /etc/syslog.conf`

2. Change the following line:

   ```
   *.info;mail.none /var/adm/syslog/syslog.log
   ```

   to:

   ```
   *.info /var/adm/syslog/syslog.log
   ```

3. To use the new syslog.conf file, type the following commands to restart the syslog daemon, syslogd:

   - /sbin/init.d/syslogd stop
   - /sbin/init.d/syslogd start

Restarting the Apache Web Server

Introduction

If you are using the sensor to protect an Apache Web Server, you must restart the Web server to finish configuration of the Web server monitoring component.

Testing the Sensor

Introduction

After you apply a policy to a sensor, you should be able to monitor network activity from the Console. Depending on the behavior of the network, data may not appear on the Console immediately.

Testing the sensor

If you have applied a policy and started sensors, but no information appears on the Console, test the sensor by logging in or by changing the audit policies.

Running a network scan

If you have an Internet Scanner or Enterprise Scanner available, run a scan against the system where the sensor is located. The sensor should send alerts that indicate the system is being accessed.

Reference: For more information about sensor settings, see the *RealSecure Server Sensor Policy Guide*.

Starting and Stopping Sensors

Introduction

You can start and stop sensors from the Console or at the computer where the sensor is installed. This topic describes how to start the sensors manually from the computer on which the sensor is installed.

Reference: For information about starting or stopping the sensor using the Console, see the SiteProtector Help.

Starting and stopping a sensor on Windows

To start or stop a sensor running on a Windows platform:

1. Open the Services window.
2. Double-click the issDaemon service.
3. Do one of the following:
   - Click **Start** to start the sensor
   - Click **Stop** to stop the sensor

Starting a sensor on Solaris

To start a sensor running on a Solaris platform:

- Restart the system.

  The sensor starts when the system starts.
- Type the following command:

  ```
  /etc/init.d/realsecure start
  ```

Stopping a sensor on Solaris

To stop a sensor running on a Solaris platform:

- Type the following command:

  ```
  /etc/init.d/realsecure stop
  ```

Starting a sensor on HP-UX

To start a sensor running on an HP-UX platform:

- Type the following command:

  ```
  /sbin/init.d/realsecure start
  ```

Stopping a sensor on HP-UX

To stop a sensor running on an HP-UX platform:

- Type the following command:

  ```
  /sbin/init.d/realsecure stop
  ```

Starting a sensor on AIX

To start a sensor running on an AIX platform:

- Type the following command:

  ```
  /opt/ISS/issSensors/sensor_name/realsecure start
  ```

Stopping a sensor on AIX

To stop a sensor running on an AIX platform:

- Type the following command:

  ```
  /opt/ISS/issSensors/sensor_name/realsecure stop
  ```

Chapter 9

Uninstalling a Sensor

Overview

Introduction

This chapter provides the procedures needed to uninstall RealSecure Server Sensor from your system.

In this chapter

This chapter contains the following topics:

Uninstalling a Sensor from a Windows Platform

SiteProtector and RealSecure server sensor

If you installed the sensor on the same computer as SiteProtector, do not uninstall the sensor until you are ready to uninstall SiteProtector.

Procedure

To uninstall a sensor from a Windows system:

Important: As part of the uninstallation process, IIS must be restarted to unregister the SSL traffic monitoring component.

1. In the **Add/Remove Programs** utility, select the sensor you want to uninstall.
2. Click **Add/Remove**.

   The InstallShield Wizard window opens, and then the Question window opens.
3. Click **Yes** to uninstall this component.

   The RealSecure Setup window opens.
4. Click **No** to continue the uninstallation process.
5. Click **Yes** to restart IIS and continue the uninstallation process.
6. Does the system detect shared files?
   - If *yes*, go to Step 7.
   - If *no*, go to Step 8.

     The Install Wizard Complete window opens.
7. Click **Yes** to delete the shared file or click **No** to leave the shared file on the computer.
8. Do you want to keep the uninstall log created by this uninstallation?
   - If *yes*, go to Step 9.
   - If *no*, select **Do not keep the uninstall log file**.
9. Do you want to keep the keys used by this sensor?
   - If *yes*, go to Step 10.
   - If *no*, select **Do not keep the keys used by this sensor**.
10. Click **Finish**.

Uninstalling a Sensor from a Solaris Platform

Introduction

This topic provides information about uninstalling a sensor from a Solaris system.

Important: If you installed the sensor in a non-default directory, uninstalling the sensor removes the directory from your system.

Uninstalling the sensor

To uninstall a sensor from a Solaris system:

1. Log on using a superuser account, such as **`root`**.
2. Type the following command to remove the sensor:

   ```
   pkgrm ISSXss
   ```

   The uninstallation program asks you to confirm the removal.
3. Type **`y`** to confirm.

   Note: You may see a message that indicates dependencies with the global zone; you can safely ignore this message as the uninstallation process will not remove any shared files.
4. Restart the Solaris system.

   The uninstallation is complete.

Remove the installation package

Manually remove the installation package, `ServerSensor.tar` file and its associated package files.

Uninstalling a Sensor from an HP-UX Platform

Introduction

This topic provides information about uninstalling a sensor from an HP-UX system.

Procedure

To uninstall a sensor from an HP-UX system:

1. Log in using a superuser account, such as **`root`**.
2. Type the following command:

   ```
   # /usr/sbin/swremove ISSXss
   ```

3. To uninstall the network monitoring component, restart the computer.

Uninstalling a Sensor from an AIX Platform

Introduction

This topic provides information about uninstalling a sensor from an AIX system.

Procedure

To remove a sensor from an AIX system:

1. Log in using a superuser account, such as **`root`**.
2. Type one of the following commands:
   - To uninstall from /opt, type **`# installp -u ISSXss`**

     Note: Use this option for typical and custom installations on all systems except AIX 6.1 and for typical installations on AIX 6.1. As custom installations on all AIX systems except AIX 6.1 were located in /opt and symlinked to the custom directory, you must uninstall from the /opt directory.
   - To uninstall from a custom location, type **`#installp -R`** *`custom_path`* **`-u ISSXss`**

     Note: Use this option for custom installations on AIX 6.1 systems as these custom installations were installed to the custom location.
3. If the C2 audit feature was enabled when you uninstalled the sensor, you must restart the feature to completely uninstall the sensor.

Remove the installation package

Manually remove the installation package, `ServerSensor-AIX-7-0.shar file`.

Uninstalling Upgrades

Uninstalling a remote upgrade

You cannot uninstall a full remote upgrade installed on a sensor using the Console. To uninstall the upgrade, you must uninstall the sensor, and then reinstall the correct sensor version.

Chapter 10

Troubleshooting

Overview

Introduction

The chapter describes several techniques for troubleshooting issues you may come across as you install a sensor.

In this chapter

This chapter contains the following topics:

No Communication Between RealSecure Server Sensor for Windows and SiteProtector

Issue	You are running ISA Server and you have configured communication between RealSecure Server Sensor for Windows and SiteProtector, but there is no communication between these components.
Background	ISA Server blocks communication between RealSecure Server Sensor and SiteProtector.
Solution	Configure the ISA server to allow incoming connections to port 2998 and port 902.

Error Messages

Introduction

This topic describes error messages you may encounter and what you can do to resolve them.

Deployment Wizard errors

If you encounter errors as you run the Deployment Wizard, you cannot click **Finish** to close the wizard. To continue, do one of the following:

- read the error text, and then fix the error
- click **Cancel**.

  The system saves all settings and changes you made.

Sensor management errors

All sensors should have a single management address that is used by all Consoles and event collectors. If a sensor is managed at multiple IP addresses, an error message may occur that says the sensor is not being managed by the event collector. This error occurs when the IP address used by the event collector for a sensor is different from the IP address used by the Console to manage that same sensor.

Connecting to sensors takes too long

When you monitor a sensor in the Console, it may take 60 seconds or longer before you see a “connected” status in the Event Status column. This is because there are two connections. The event collector must be connected to the sensor, and the Console must be connected to the event collector.

After you add a sensor to an event collector, you must wait for the following:

- The event collector to connect to the sensor. If this connection fails for some reason and you are monitoring the event collector, an EventCollector_Error message appears.
- The Console to connect to the event collector that is monitoring the sensor. If this connection fails for some reason, an error message appears in the Event Status column of the Managed Assets window of the Console.

If errors occur with either of these connections, the event collector and the Console periodically attempt to reconnect the components. Because the retry logic for one connection is not synchronous with the retry logic for the other connection, it can sometimes take as long as one or two minutes before the sensor is reconnected and you see events.

ISS Daemons

Introduction

For troubleshooting purposes, you may need to manually start or stop the issDaemon.

Definition: ISS daemon

The issDaemon is a component that manages the following:

- commands from the Console
- the connection between components, such as the communication between an event collector and a sensor

Managing daemons on a Windows system

On a Windows system, you can manage the daemon through the Windows Services Control Panel.

Reference: For a detailed procedure, see “Starting and Stopping Sensors” on page 113.

Managing daemons on Solaris systems

On Solaris systems, you can manage the daemon using the following commands:

```
/etc/init.d/realsecure start
/etc/init.d/realsecure stop
```

Managing daemons on HP-UX systems

On HP-UX systems, you can manage the daemon using the following commands:

```
/sbin/init.d/realsecure start
/sbin/init.d/realsecure stop
```

Managing daemons on an AIX system

On an AIX system, you can manage the daemon using the following commands:

```
/opt/ISS/issSensors/sensor_name/realsecure start
/opt/ISS/issSensors/sensor_name/realsecure start
```

Remote Upgrades

Introduction

This topic describes some of the error messages that you may receive when you upgrade a sensor remotely, and how you can resolve the errors.

Signature error messages

The sensor cannot monitor signatures that are included in the upgrade until you apply a policy that contains the new signatures. The sensor issues warnings if the current policy does not support the new signatures.

Reference: For more information about applying a policy, refer to "applying policies" in the SiteProtector Help.

Policy and control channel error messages

If you receive the following error message after you upgrade, you must stop managing the sensor, and then start managing the sensor again to correct the problem:

```
The sensors current policy file was not successfully
transferred when the control channel was opened and
therefore it is not available to the application. This is
usually due to a problem reading the file from the sensor
after opening the control channel. It can also be due to the
fact that after a fresh install there is not current policy
file until the sensor is started if this is the case then
Start the sensor. [ID=0xc72c0026]
```

Index