IBM Proventia® Management SiteProtector™

# SecureSync Guide

Version 2.0, Service Pack 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.

May 30, 2008

# Contents

## Preface

## Chapter 1: Introduction to SiteProtector - SecureSync

## Chapter 2: Preparation

## Chapter 3: Failover

## Chapter 4: Failback

## Chapter 5: Recovering the Primary Site

## Chapter 6: Troubleshooting

# Preface

## Overview

### Introduction

This guide explains to use the SiteProtector - SecureSync feature for failover and for failback or recovery of your SiteProtector system.

### Audience

This guide is written for the person who configures, updates, and maintains a SiteProtector system. For many Sites, that person is the Security Manager who is responsible only for maintaining the security of the network. For other Sites, the Security Manager may also be responsible for aspects of network and security administration, such as network administration and security analysis.

### License agreement

For licensing information about 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 IBM Internet Security 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<br>**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 IBM Internet Security Systems Contact Technical Support Web page at http://www-935.ibm.com/services/us/index.wss/offering/iss/a1029178.

Chapter 1

# Introduction to SiteProtector - SecureSync

## Overview

### Introduction

Use SiteProtector - SecureSync to configure Sites for failover and for failback or recovery.

### Terminology

Table 2 defines terms used in this guide.

| Term | Definition |
|---|---|
| Site | A deployment of a SiteProtector system |
| Primary Site | The designation for the currently active SiteProtector system in a Site configured for SiteProtector - SecureSync |
| Secondary Site | The designation for the SiteProtector system that is configured for failover in a Site configured for SiteProtector - SecureSync |
| Fail over | The manual process of activating the secondary Site when the primary Site fails |
| Fail back | The manual process of reactivating the primary Site when it is operational again and then disabling the secondary Site |
| Disaster recovery | The manual process of recovering the primary Site after a catastrophic failure |

**Table 2:** *Terminology*

### In this chapter

This chapter contains the following topics.

# The SiteProtector - SecureSync Process

### Introduction

The SiteProtector - SecureSync process provides a structured method for implementing a failover and disaster recovery solution. The goals of the process are as follows:

- To ensure that you maintain SiteProtector system functionality in the event of catastrophic failure, network outage, or other disaster that causes your primary Site to be unavailable
- To ensure that you do not lose important SiteProtector system data if the primary Site becomes unavailable

### Stages of the process

Table 3 describes the stages of the SiteProtector - SecureSync process.

| Stage | Description |
|---|---|
| 1: Preparation | • Prepare the primary and secondary Sites.<br>• Configure stand-alone components in the primary Site, such as Event Collectors, to fail over to the secondary Site. |
| 2: Failover | Activate agent management at the secondary Site. |
| 3: Failback | • Transfer data to the primary Site or to a reinstalled primary Site.<br>• Reactivate agent management at the Site. |
| 4: Disaster Recovery, in lieu of failback | • Reinstall a SiteProtector system.<br>• Restore the SiteProtector system Database. |

**Table 3:** *Stages of the SiteProtector - SecureSync process*

# The SiteProtector - SecureSync Feature Set

## Introduction

The SiteProtector - SecureSync feature supports the SiteProtector - SecureSync process.

## Purpose

This feature gives you the following abilities:

- To transfer data between the primary and secondary Sites
- To enable and disable agent management at the Sites
- To distribute authentication keys for the secondary Site or a reinstalled Site

## Menu options

Table 4 describes the SiteProtector - SecureSync menu options.

| Menu Option | Description |
|---|---|
| Import/Export Site Data | Starts the SecureSync Import/Export Wizard, which assists you in transferring configuration, event, and policy data between the primary and secondary Sites. |
| Distribute Keys | • Distributes authentication keys to all the managed agents<br>• Used on the primary Site to distribute keys for the secondary Site<br>• Used on the secondary Site to distribute keys for a reinstalled primary Site |
| Manage Agents | • Enables agent management at the Site<br>• Used on the secondary Site to fail over to the secondary Site |
| Release Agents | • Disables agent management at the Site<br>• Used on the secondary Site to fail back to the primary Site |
| Set as Secondary Site | • Enables use of the Manage Agents and Release Agents options<br>• Changes the site icon |

**Table 4:** *SiteProtector - SecureSync menu options*

# The SecureSync Import/Export Wizard

**Introduction**

This topic describes the SecureSync Import/Export Wizard and how it can be used to transfer data between the primary and secondary Sites. The wizard restricts the functions available based on the Site designation.

**Prerequisites**

Before you can use the SecureSync Import/Export Wizard, you must prepare the Sites involved in the data transfer.

**Reference:** See "Preparation" on page 13.

**Required information**

You must know the path of the shared folder where the Wizard saves and retrieves data archive files, including the server name and drive letter.

**Example:**

```
\\server\c$data\SPArchives
```

**Time requirements**

The time required to transfer data between Sites depends on the amount of data you are transferring and the current data loading activity on the Sites.

**Archive files**

When the Wizard runs an export job, it automatically creates an archive file in JAR format and gives the file a system-generated filename. The filename includes the date and time of the job and the type of Site (primary or secondary). The wizard saves the file to a user-defined location.

**Examples**

- `FailoverArchive_Primary_2005-05-03_1-42-01_PM.jar`
- `FailoverArchive_Secondary_2005-05-03_1-47-05_PM.jar`

When the Wizard runs an import job, it imports data from the archive file in the user-defined location. If there are multiple archive files in the location, then the Wizard imports from the most current file.

When you set up an export or import job, the Wizard asks you to specify the path for data archives. You cannot include the exact filename in this path.

## Primary Site jobs

Table 5 describes the data export and import jobs available on the primary Site.

| Job | Description |
|---|---|
| Export primary Site configuration data | Exports the following primary Site configuration data[a], [b]to an archive file:<br>• Policies<br>• Command jobs<br>• Responses<br>• Application lists<br>• Groups<br>• Components[c]<br>• Site filters<br>• Grouped assets<br>• Licenses<br>• Site ranges<br>• Group settings<br>• Autoticketing rules<br>• Policy repositories<br>• Permissions for all users and groups only[d] |
| Import secondary Site policy data | Imports the secondary Site configuration data from an archive file. |
| Import secondary Site event data | Imports the secondary Site event data from an archive file. |
| Import secondary Site policy and event data | Imports the secondary Site event and configuration data from an archive file. |

**Table 5:** *Primary Site data export and import jobs*

[a] Files needed for Remedy integration are not included in the data export. If you want to integrate the secondary Site with Remedy, then you must manually replicate these settings on the secondary Site *after* you fail over to the Site. For more information about a SiteProtector system and Remedy integration, see the chapter about configuring ticketing in the *SiteProtector System System Configuration Guide*.

[b] OnDemand Services account information is not carried over. If you use OnDemand Services, you must replicate the account information on the secondary site.

[c] This does not include any Core or SP Firmware components.

[d] All permissions are exported, but local users and groups on the primary Site cannot access the secondary Site.

## Secondary Site jobs

Table 6 describes the data import and export jobs available on the secondary Site.

| Job | Description |
|---|---|
| Import primary Site configuration data<br>**Caution:** This job overwrites all existing configuration data on the Site. You should run this job on the secondary Site or a new Site only. | Imports the following primary Site configuration data[a,b] from an archive file:<br>• Policies<br>• Command jobs<br>• Responses<br>• Application lists<br>• Groups<br>• Components[c]<br>• Site filters<br>• Grouped assets<br>• Licenses<br>• Site ranges<br>• Group settings<br>• Autoticketing rules<br>• Policy repositories<br>• Permissions for domain users and domain groups only[d] |
| Export secondary Site policy data | Exports configuration data to an archive file.<br>**Important:** This job does not export any configuration data, such as changes to groups or group settings. |
| Export secondary Site event data | Exports event data to an archive file. |
| Export secondary Site policy and event data | Exports configuration and event data to an archive file. |

**Table 6:** *Secondary Site data import and export jobs*

[a] Files needed for Remedy integration are not included in the data export. If you want to integrate the secondary Site with Remedy, then you must manually replicate these settings on the secondary Site *after* you fail over to the Site. For more information about a SiteProtector system and Remedy integration, see the chapter about configuring ticketing in the *SiteProtector System System Configuration Guide.*

[b] OnDemand Services account information is not carried over. If you use OnDemand Services, you must replicate the account information on the secondary site.

[c] This does not include any Core or SP Firmware components.

[d] All permissions are exported, but local users and groups on the primary Site cannot access the secondary Site.

## Starting the wizard

To start the SecureSync Import/Export Wizard:

1. In the SiteProtector Console, select the Site Node in the **My Sites** pane.
2. Click **Tools→SecureSync→SecureSync Import/Export Site Data**.

   The SecureSync Import/Export Wizard begins.
3. Verify that the type of Site you intended to export data from or import data into is selected, and then click **Next**.

   **Note:** If the type of Site is not correct, log on to the correct Site, or change the Site you are on to the correct type.
4. Follow the onscreen instructions.

Chapter 2

# Preparation

## Overview

**Introduction**

This chapter explains how to prepare the primary and secondary Sites. This is the Preparation stage of the SiteProtector - SecureSync process.

**Note:** If you have to reinstall the primary Site for any reason, such as disaster recovery, use the procedures in this chapter to prepare the reinstalled primary Site.

**In this chapter**

This chapter contains the following topics.

# Site Preparation Checklists

### Introduction

This topic provides task checklists to ensure that you perform all the tasks required to prepare the primary Site, the secondary Site, a reinstalled primary Site, and a Site migration.

### Primary Site checklist

Table 7 provides a checklist of the tasks required to prepare the primary Site.

| ✓ | Tasks |
|---|---|
| □ | Distribute the reinstalled Site keys to all managed agents.<br>See "Distributing Site Keys to Agents" on page 17. |
| □ | Configure the Application Server with the required Database permissions.<br>See "Configuring Application Server Permissions" on page 20. |
| □ | Set up a shared folder for data archives.<br>See "Setting Up a Shared Folder for Data Archives" on page 22. |
| □ | Configure the Sensor Controller and SQL Server services to log on as a user with permission to access the shared folder.<br>See "Configuring Services with Shared Folder Permissions" on page 24. |
| □ | Schedule an export configuration data job.<br>See "Schedule SiteProtector - SecureSync Import/Export to Secondary Site" on page 25. |
| □ | Reset the passwords for Event Collectors, Agent Managers, and the SecurityFusion module.<br>See "Resetting Component Passwords" on page 26. |

**Table 7:** *Checklist for preparing the primary Site*

### Secondary Site checklist

Table 8 provides a checklist of the tasks required to prepare the secondary Site.

| ✓ | Task |
|---|---|
| □ | Install the secondary Site and ensure that it meets all the secondary Site requirements.<br>See "Secondary Site Requirements and Considerations" on page 16. |
| □ | Designate the Site as the secondary Site.<br>See "Setting the Site as the Primary or Secondary Site" on page 19. |
| □ | Distribute the secondary Site keys to all managed agents.<br>See "Distributing Site Keys to Agents" on page 17. |
| □ | Configure the Application Server with the required Database permissions.<br>See "Configuring Application Server Permissions" on page 20. |
| □ | Set up a shared folder for data archives.<br>See "Setting Up a Shared Folder for Data Archives" on page 22. |
| □ | Configure the Sensor Controller and SQL Server services to log on as a user with permission to access the shared folder.<br>See "Configuring Services with Shared Folder Permissions" on page 24. |

**Table 8:** *Checklist for preparing the secondary Site*

| ✓ | Task |
|---|---|
| □ | Schedule an import configuration data job.<br>See “Schedule SiteProtector - SecureSync Import/Export to Secondary Site” on page 25. |
| □ | Create user accounts for Event Collectors, Agent Managers, and the SecurityFusion module in the secondary Site Database.<br>See “Creating User Accounts for Components in the Site Database” on page 29. |
| □ | Create a DSN for the secondary Site Database on each Event Collector.<br>See “Creating a Data Source Name (DSN)” on page 32. |
| □ | If you want to integrate the secondary Site with Remedy, then you must replicate the settings manually on the secondary Site. See the *SiteProtector System Remedy iNote* for more information about integrating the Site with Remedy. |

**Table 8:** *Checklist for preparing the secondary Site (Continued)*

# Secondary Site Requirements and Considerations

### Introduction

The secondary Site is a backup Site for your primary Site. The secondary Site, including the Event Collector, Agent Manager, and X-Press Update Server, must run in passive standby mode. The secondary Site must not be responsible for any agent management or data collection activities. The secondary Site becomes active only when you manually activate it at failover and remains active until you manually deactivate it at failback.

### Requirements

The secondary Site must meet the following requirements:

- The Site must meet the minimum system requirements as specified in the *SiteProtector System Requirements*.
- The Site components, specifically the Database and Core components, must be updated to the same version, XPU, and Service Pack levels as the Site components in the primary Site.
- The following minimum levels are required.

| Component | Minimum Level |
|---|---|
| Event Collector | 6.9 (SP1.13) |
| Agent Manager | XPU 6.9 (SP7.1) |
| SecurityFusion module | SP1.5 |

- The Site time must be synchronized with the time on the primary Site.

### Rules to observe

Observe the following rules:

- Do not manually register any secondary Site components to the primary site.
- Do not set any secondary Site components to communicate with any primary site components.
- Do not uninstall the Agent Manager and Event Collector installed as part of the secondary Site even though these components are not used to manage agents. If you uninstall these components, then you cannot update the secondary Site.

# Distributing Site Keys to Agents

**Introduction**

A SiteProtector system uses public-key encryption to securely communicate with managed agents. Before the agents can communicate with a Site, the agents must have copies of the authentication keys for that Site.

If you are preparing a secondary Site, then you must distribute the keys for the secondary Site to all managed agents. If you are preparing a reinstalled primary Site, then you must distribute the keys for the reinstalled primary Site to all managed agents.

**Source location of distributed keys**

The Key Distribution function distributes keys from the following folder on the computer that is managing agents:

```
\Program Files\ISS\SiteProtector\Application Server\failover\keys
```

**Destination location of distributed keys**

This function distributes the keys to the appropriate folder on the computer where the agent is installed. The specific directory varies depending on the agent and the operating system. Table 9 gives examples of the directories where the job puts the keys.

| Hardware or Software | Example Directory |
|---|---|
| Windows | `\Program Files\ISS\IssSensors\`*`AgentName`*`\Keys` |
| SiteProtector system Components | `\Program Files\ISS\RealSecure SiteProtector\`*`ComponentName`*`\Keys` |
| Linux/Solaris Sensors | `/opt/ISS/issSensors/`*`AgentName`*`/Keys` |
| Nokia Sensors | `/opt/ISS/RealSecure7_0/Keys`<br>`/opt/ISS/issSensors/network_sensor_2/Keys` |

**Table 9:** *Directories where key distribution job puts keys*

**Tasks overview**

Table 10 describes the tasks for distributing Site keys to all managed agents.

| Task | Description |
|---|---|
| 1 | If you are distributing keys for the secondary Site, then you copy the key subdirectories from the secondary Site to the primary Site.<br>If you are distributing keys for a reinstalled primary Site, then you copy the key subdirectories from the reinstalled Site to the secondary Site. |
| 2 | Run a distribute keys to all managed agents job. |

**Table 10:** *Tasks for distributing Site keys*

## Copying Site keys

To copy the CerticomNRA and RSA key subdirectories to the primary Site.

| Copy... | To... |
|---|---|
| the following key subdirectories:<br>• `\Program Files\ISS\SiteProtector\Application Server\Keys\CerticomNRA`<br>• `\Program Files\ISS\SiteProtector\Application Server\Keys\RSA` | the following folder on the Application Server:<br>`\Program Files\ISS\Site Protector\Application Server\failover\keys` |

**Note:** If you are distributing the keys for a reinstalled Site, then you copy the subdirectories to this location on the secondary Application Server.

## Distributing secondary Site keys

To distribute keys for the secondary Site to managed agents:

1. Start a Console, and connect to the Site that is managing agents.
2. In the left pane, then select the Site Node.
3. Click **Tools**→**SecureSync**→**Distribute Keys**.
4. In the Key Distribution window, select the Schedule icon.
5. In the **Recurrence Pattern** section, select **Run once**.
6. Click **OK**.

   The job distributes keys to one agent at a time. The time required to complete the entire job depends on the number of agents installed in the Site.

# Setting the Site as the Primary or Secondary Site

**Introduction**

Use the SiteProtector - SecureSync option, **Set as secondary Site**, to change a primary Site to a secondary site or to change a secondary Site to a primary Site.

**Note:** A primary Site is used to actively manage agents. A secondary Site is designated as a failover environment until it is needed to actively manage agents.

**Procedure**

To set a Site as primary or secondary:

1. In the **My Sites** pane, select the Site Node.
2. Click **Tools**→**SecureSync**→**Set as Secondary Site**.

   **Note:** When the Site is set to a secondary Site, a check mark appears in front of the **Set as Secondary Site** option. The check mark does not appear when the Site is set to a primary Site.

# Configuring Application Server Permissions

### Introduction

Before you can transfer data between Sites, you must configure the Application Servers in each Site with permission to insert data into the Site Database. To configure the Application Server with the required database permissions, you must grant “bulkadmin” permission to the IssApp user account.

**Note:** This topic contains procedures for configuring application server permissions for both SQL 2000 and SQL 2005. Depending on your SQL version database, follow the appropriate procedural step process to configure your application server’s permissions.

### Configuring application server permissions for SQL 2005

To configure the Application Servers with the required SQL 2005 database permissions:

1. On the Database Server computer, select **Start→All Programs→Microsoft SQL Server 2005→SQL Server Management Studio**.

   The **SQL Server 2005** box appears.
2. In the **SQL Server 2005** box, verify that the Server type, Server name, and Authentication fields are correct, and then click **Connect**.
3. On the right pane tree, select **Databases→RealSecureDB**.
4. Right-click **RealSecureDB**, and then select **New Query**.
5. In the **Query -** *`database server name`***.RealSecureDB** pane, type the following:
   `sp_addsrvrolemember 'issapp', 'bulkadmin'`
6. From the **Query** menu, select **Execute**.

   SQL Analyzer runs the command.
7. Close the SQL Query Analyzer.

### Configuring application server permissions for SQL 2000

To configure the Application Servers with the required SQL 2000 database permissions:

1. On the Database Server computer, select **Start→Programs→Microsoft SQL Server→Query Analyzer**.
2. In the **SQL Server** box, select the SQL Server to which you want to connect.
3. In the **Login name** box, type the SQL Server login name.
4. In the **Password** box, type the SQL Server password.
5. Click **OK**.

   The SQL Query Analyzer appears.

   **Note:** SQL Query Analyzer automatically defaults to the master database.
6. From the **Query** menu, select **Change Database**.

   The Select Database of *`Database Name`* window appears.
7. Select **RealSecureDB,** and then click **OK**.
8. In the **Query -** *`database server name`***.RealSecureDB** pane, type the following:
   `sp_addsrvrolemember 'issapp', 'bulkadmin'`
9. From the **Query** menu, select **Execute**.

   SQL Analyzer runs the command.

10. Close the SQL Query Analyzer.

**Note:** In the event you used the packages, then NT or SQL Authorization could have been selected. If you select to use the NT Authorization from the package installation, then you must set the Application Server to log.

# Setting Up a Shared Folder for Data Archives

### Introduction

The SecureSync Import/Export Wizard exports Site data to an archive file and imports Site data from an archive file. The location of the archive file is user-defined. IBM ISS recommends that you use a shared folder for data archives that both the primary and secondary Sites have permission to access. This approach facilitates the data transfer process between the Sites and eliminates the need to manually transport the archive file from one Site to the other.

**Important:** If you use a shared folder for data archives, you must configure the Sensor Controller and SQL Server service to log on and run under a user account with permission to access the shared folder. If you do not want to change the log on credentials for these services, then you must develop an alternative strategy for transporting the data archive file between the Sites.

### Alternative methods

The following are alternative methods for transporting the Wizard-generated data archive file between Sites:

- Export the data archive file to a local folder on the primary Site, and then create a program, such as a batch program, to move the data archive file to a folder on the secondary Site where the Wizard can then import the file.
- Export the data archive file to a local folder on the primary Site, and then manually transport the data archive file to folder on the secondary Site where the Wizard can then import the file.

### Location of shared folder

When you create the shared folder for data archives, you should create the folder in a separate location from the SiteProtector system deployment. This approach ensures that the shared folder remains available regardless of the operational status of the primary or secondary Site.

### Space requirements

The drive space required on the shared folder varies according to the types of events and the number of custom policies in the data archive file. Table 11 lists the approximate space requirements for data archive files.

| File | Requirements | Example |
|---|---|---|
| Archive File for Event Data | One event in the archive file requires approximately 95 bytes. | A file containing 15 million events is approximately 1.3 GB. |
| Archive File for Policies and Configuration Data | The base size of the archive file is approximately 4 MB.<br>**Note:** You can expect to require approximately 40 KB of additional size per custom policy in the Site. | If the archive file contains the following amounts of data, then it is approximately 5,694 KB in size:<br>• 46 Custom Policies<br>• 4019 Groups<br>• 63864 Hosts |

**Table 11:** *Space requirements for data archive files*

### Temporary drive space requirements

When you run jobs to import data from the shared folder, a SiteProtector system requires temporary drive space on the shared folder to run the job. The amount of temporary space required depends on the types of data and the amount of data that you are importing. Importing one event requires approximately 700 bytes of temporary space.

### Example

You are importing a data archive file that contains 15 million events. You need 9.7 GB of temporary space on the shared folder to run the job.

## Process

The process for setting up a shared folder varies depending on your security requirements, environment, and platform.

If you are using a Windows platform, then you can create a shared folder or allow sharing on an existing folder. You also need to set the permissions on the shared folder so that Administrators have Full Control. For more information about creating shared folders and setting folder permissions, refer to the Microsoft documentation.

# Configuring Services with Shared Folder Permissions

### Introduction

If you choose to use a shared folder for data archives, then you must configure the following services to log on as a user who has permission to access the shared folder:

- Sensor Controller service
- SQL Server service

If you do not run these services under a user account that has permission to access the shared folder, then the SecureSync Import/Export Wizard cannot access the shared folder, and the data transfer jobs will fail.

**Note:** You can use an alternative method for transporting Wizard-generated data archive file between the Sites. For information about alternative methods, see "Setting Up a Shared Folder for Data Archives" on page 22.

**Note:** The process for configuring services to log on as a user with permission to access the shared folder varies depending on your security requirements, environment, and platform.

### Procedure

To configure permissions for the Log On As option:

1. Open **Services** in your primary and secondary Sites.
2. Click on **MSSQLSERVER,** and then click the **Log On** tab.

### Process

If you are using a Windows platform, then you can use the Microsoft Computer Management feature to set the Log On As option for each service. For more information about configuring how services log on and run, refer to the Microsoft documentation.

# Schedule SiteProtector - SecureSync Import/Export to Secondary Site

**Introduction**

To ensure that you maintain current configuration settings on the secondary Site, it is important to automate the process of transferring primary Site configuration settings to the secondary Site. To automate the process, you schedule corresponding export and import jobs on both Sites.

**Data overwritten**

The job to import configuration data into the secondary Site is *destructive*, meaning that the job overwrites any existing data in the Site Database, including permissions.

**Temporary space requirements**

The job to export configuration data for an average Site requires approximately 50 to 100 MB of temporary disk space. For example, when you export configuration data for the primary Site, you must have 50 to 100 MB of temporary disk space on the Application Server.

**Sensor status**

After you import configuration data into the secondary Site, the managed agents appear in the secondary Site, but the status of each agent in the Site is “Not Managed.” The status of the agents remains “Not Managed” until you fail over to the secondary Site.

**New group on secondary Site**

When you import data from a primary Site to a secondary Site, the SiteProtector system creates a subgroup with the same name your Site-level group. The new group contains the core components of the secondary Site before you imported the data from the primary Site. The SiteProtector system uses this group, but you do not need it. Do not make any changes to it.

**Tip:** Name your Site-level group `Secondary` to make it easy to identify this new group.

**Procedure**

To schedule the configuration data transfer from the primary to the secondary Site:

1. On the primary Site, use the SecureSync Import/Export Wizard to schedule an export configuration data job.
2. On the secondary Site, use the SecureSync Import/Export Wizard to schedule a corresponding import primary Site configuration data job.

   **Tip:** Set the start time for the import job on the secondary Site to start approximately one hour after the start time for the export job. This will allow enough time for the export job on the primary Site to complete before the import job begins.

# Resetting Component Passwords

### Introduction

Before you can create user passwords for components in the primary site, you must reset the passwords for the following components:

- Event Collectors
- Agent Managers
- SecurityFusion module

**Note:** This topic contains procedures for resetting component passwords for both SQL 2000 and SQL 2005. Depending on your SQL version database, follow the appropriate procedural step process to reset your component passwords.

### Component password maintenance utilities

Table 12 describes the password maintenance utilities for SiteProtector system components.

| Utility | Description |
|---|---|
| Event Collector Login Utility | Use this utility to reset the password for the Event Collector. |
| Agent Manager Login Information Utility | Use this utility to reset the password for the Agent Manager.<br>**Note**: Agent Manager was formerly called Desktop Controller. In the event you are using Desktop Controller, then the utility is called DCLogin.exe. |
| SecurityFusion module Database Password Changing Utility | Use this utility to reset the password for the SecurityFusion module. |

**Table 12:** *Password maintenance utilities for SiteProtector system components*

### Resetting component passwords for SQL 2005

To reset the component password for SQL 2005:

1. On the component computer, stop the issDaemon service.
2. To start the login utility, select the appropriate component.

| Component | Locate the utility in the following directory: | Result: |
|---|---|---|
| Event Collector | `\Program Files\ISS\SiteProtector \Event Collector\ ECLogin.exe` | The SiteProtector system Event Collector Login Utility window appears. The Login text box shows the user name for the Event Collector. |
| Agent Manager | `\Program Files\ISS\ \Agent Manager\AMLogin.exe` | The Agent Manager was formerly called Desktop Controller. If you installed the utility before the name change, then the pathname to the utility is as follows:<br>`\Program Files\ISS\SiteProtector\Desktop Controller\DCLogin.exe` |

**Table 13:** *Component login utility directories*

| Component | Locate the utility in the following directory: | Result: |
|---|---|---|
| SecurityFusion module | `\SiteProtector\SecurityFusionModule\ChangeFusionPassword.exe` | The SecurityFusion module Database Password Changing Utility window appears. |

Table 13: *Component login utility directories*

3. Type the new password in the **Password** box.
4. Type the new password again in the **Confirm** box.
5. Click **Save**.
6. On the Database Server computer, select **Start**→ **All Programs**→ **Microsoft SQL Server 2005**→ **SQL Server Management Studio**.

   The **SQL Server 2005** box appears.
7. In the **SQL Server 2005** box, verify that the Server type, Server name, and Authentication fields are correct, and then click **Connect**.
8. From the left pane, click **Security**, and then click **Login.**
9. Double-click on the agent manager you want to create a new password.

   The Login Properties window for that agent manager appears.
10. From the **General** page, in the **Login Name** box, type the name of the component.
11. In the **Password** box, type the new password for the component.
12. Type the same new password in the **Confirm Password** box.
13. Check the **Enforce Password Policy** box.
14. Clear the **Enforce Password Expiration** box.

    If you check this box, you will be reminded to change your password on a regular basis.
15. Click **OK** to save your new component password.
16. Restart the issDaemon service on the component computer.

### Resetting component passwords for SQL 2000

To reset the component password for SQL 2000:

1. On the component computer, stop the issDaemon service.
2. To start the login utility, select the appropriate component.

| Component | Locate the utility in the following directory: | Result: |
|---|---|---|
| Event Collector | `\Program Files\ISS\SiteProtector\Event Collector\ECLogin.exe` | The SiteProtector system Event Collector Login Utility window appears. The Login text box shows the user name for the Event Collector. |

| Component | Locate the utility in the following directory: | Result: |
|---|---|---|
| Agent Manager | `\Program Files\ISS\ \Agent Manager\AMLogin.exe` | The Agent Manager was formerly called Desktop Controller. If you installed the utility before the name change, then the pathname to the utility is as follows:<br>`\Program Files\ISS\SiteProtector\Desktop Controller\DCLogin.exe` |
| SecurityFusion module | `\SiteProtector\SecurityFusionModule\ChangeFusionPassword.exe` | The SecurityFusion module Database Password Changing Utility window appears. |

3. Type the new password in the **Password** box.
4. Type the new password again in the **Confirm** box.
5. Click **Save**.
6. On the primary Site Database computer, select **Start→Programs→Microsoft SQL Server→Enterprise Manager**.

   The SQL Server Enterprise Manager window appears.
7. Select **Microsoft SQL Servers →SQL Server Group→(local) (Windows NT)→ Security→Logins**.
8. In the right pane, right-click the component name, and then select **Properties**.
9. In the **Password** box, type the new password for the component.
10. On the **General** tab, click **OK**.

    The Confirm Password window appears.
11. In the **Confirm new password** box, retype the password for the component, and then click **OK**.

    SQL Server Enterprise Manager resets the password.
12. Restart the issDaemon service on the component computer.

# Creating User Accounts for Components in the Site Database

**Introduction**

This topic provides instructions for creating component user accounts in the Secondary Site Database. You can use this procedure to create user accounts for Event Collectors, Agent Managers, and SecurityFusion module.

**Note:** This topic contains procedures for creating user accounts for components in the site database for both SQL 2000 and SQL 2005. Depending on your SQL version database, follow the appropriate procedural step process to create user accounts for components in the site database.

**User account requirements for failover and failback**

Table 14 describes the user account requirements for components to fail over and to fail back.

| Before a component can... | Duplicate user accounts for the component must exist in... |
|---|---|
| fail over from the primary Site to the secondary Site | • primary Site Database<br>• secondary Site Database |
| fail back from the secondary Site to the primary Site | • primary Site Database<br>• secondary Site Database |
| fail back from the secondary Site to a reinstalled Site | • secondary Site Database<br>• Reinstalled Site Database |

**Table 14:** *User account requirements for failover and failback*

**In which database do I create the user accounts?**

If you are configuring primary Site components for failover, then you must create the user accounts in the secondary Site Database.

If you are configuring components for failback to a reinstalled Site, then you must create the user accounts in the reinstalled Site Database.

**Background**

The SiteProtector system maintains a user account for each SiteProtector system component. The Site Database uses this account to identify the component, and the component uses the account to login to the Site Database. The user account includes the following details:

- A user name for the component based on the name of the computer where the component is installed

  **Example:**

  The user name for an Event Collector installed on a computer named ATL1000 is "EventCollector_ATL1000."

- An encrypted system-generated password for the component

  You cannot access the system-generated password. You can reset component passwords with the password maintenance utilities.

### Creating user accounts in the Site Database for SQL 2005

To create a user account for a component in the Site Database for SQL 2005:

1. On the Database Server computer, select **Start**→**All Programs**→**Microsoft SQL Server 2005**→**SQL Server Management Studio**.

   The **SQL Server 2005** box appears.
2. In the **SQL Server 2005** box, verify that the Server type, Server name, and Authentication fields are correct, and then click **Connect**.
3. From the left pane, click **Security**, and then click **Login.**
4. Double-click on the agent manager you want to create a user account.

   The Login Properties window for that agent manager appears.
5. From the **General** page, in the **Login Name** box, type the name of the component.
6. In the **Password** box, type the password for the component.
7. Type the same password in the **Confirm Password** box.
8. In the **Default Database** box, select **RealSecureDB**.
9. In the **Default Language** box, select the appropriate language.
10. Click the **User Mapping** page.
11. In the **Users mapped to this login** section, select **RealSecureDB**.
12. In the **Database role membership for 'RealSecureDB'** section, select the following:
    - **public**
    - **db_datareader**
    - **db_datawriter**
    - **issApplication**
13. Click **OK**.

    SQL Server Management Studio creates a user account for the component.

### Creating user accounts in the Site Database for SQL 2000

To create a user account for a component in the Site Database for SQL 2000:

1. On the Site Database computer, select **Start**→**Programs**→**Microsoft SQL Server**→ **Enterprise Manager**.

   The SQL Server Enterprise Manager window appears.
2. Select **Microsoft SQL Servers**→**SQL Server Group**→**(local) (Windows NT)**→ **Security**→**Logins.**
3. Right-click **Logins,** and then select **New Login**.

   The SQL Server Login Properties - New Login window appears.
4. In the **Name** box, type the name of the component.
5. In the **Authentication** section, select **SQL Server Authentication**.
6. In the **Password** box, type the password for the component.
7. In the **Defaults** section, in the **Database** box, select **RealSecureDB**.
8. In the **Language** box, select the appropriate language.
9. Click the **Database Access** tab.
10. In the **Specify which databases can be accessed by this login** section, select **RealSecureDB**.

11. In the **Database roles for ‘RealSecureDB’** section, select the following:
    - **public**
    - **db_datareader**
    - **db_datawriter**
    - **issApplication**
12. In the **SQL Server Login Properties - New Login** window, click **OK**.

    The Confirm Password window appears.
13. In the **Confirm new password** box, type the password for the component, and then click **OK**.

    SQL Server Enterprise Manager creates a user account for the component.

# Creating a Data Source Name (DSN)

## Introduction

The Event Collector must include a Data Source Name (DSN) for each Site Database that it communicates with. For example, if you have a primary and secondary Site, then the Event Collector must include a DSN for the primary Site Database and a DSN for the secondary Site Database.

## When is the DSN used

When you fail over to the secondary Site, the SiteProtector system asks you to enter the DSN for the secondary Site Database. This information directs the Event Collectors to send events to the secondary Site Database.

When you fail back to the primary Site, the SiteProtector system asks you to enter the DSN for the primary Site Database. This information directs the Event Collectors to send events to the primary Site Database.

## Procedure

To create a DSN for the secondary Site Database:

**Important:** When you create the DSN for the secondary Site Database, you must use the same DSN name on all Event Collectors.

1. On the Event Collector computer, select **Start→Settings→Control Panel→ Administrative Tools→DataSources.**
2. In the **ODBC Data Source Administrator** window, select the **System DSN** tab.
3. Select **Add.**

   The Create New Data Source window appears.
4. Select **SQL Server**, and click **Finish**.

   The Create a New Data Source to SQL Server window appears.
5. Type a name for the DSN, a description, and the server name of the secondary Site Database in the appropriate boxes, and then click **Next**.

   **Example:** EC_*SecondarySiteName*
6. Select **With SQL Server authentication using a login ID and password entered by the user**.
7. Select **Connect to SQL Server to obtain default settings for the additional configuration options**, and then type the Event Collector user name and password just as it appears in the user account you created for the Event Collector.

   **Note:** The user name and password must match the user name and password you created for the Event Collector.
8. Click **Next**.
9. In the ODBC Microsoft SQL Server Setup window, click **Test Data Source.**

   If you configured the connection properly, then you receive a “TEST COMPLETED SUCESSFULLY!” message.
10. Click **OK**.

## Chapter 3

# Failover

## Overview

### Introduction

This chapter explains how to fail over to the secondary Site if the primary Site fails. This is the Failover stage of the SiteProtector - SecureSync process.

### Prerequisite

Before you can fail over the secondary Site, you must properly prepare the Sites.

**Suggestion:** If you intend to use failover, remove the Event Collector (EC) and Agent Manager (AM) from their primary site and install them on another computer on the network. In case of a primary Site hardware failure, all agents will be able to migrate seamlessly to the secondary Site. If you do not do this, agents reporting to the EC/AM will have no available path to send data traffic if the primary computer fails, and you will have to manually reconfigure the agents to report to new EC/AMs.

**Reference:** See “Preparation” on page 13.

### In this chapter

This chapter contains the following topics.

# What is Failover?

### Introduction

Failover is the manual process of switching to the secondary Site.

### Allowed tasks

After you fail over to the secondary Site, you can use the secondary Site to perform policy management tasks, including the following:

- Access policies
- Configure policies
- Adjust policies
- Analyze event data
- Add agents
- Change group settings
- Change permissions
- Change permissions on known accounts

### Components and agents that fail over

The following stand-alone components fail over to the secondary Site:

- Event Collector(s), including the agents that report the Event Collectors
- Agent Manager(s), including the agents that report to the Agent Managers
- SecurityFusion module

### Components that do not fail over

The primary Site Application Server and Database do not fail over.

X-Press Update Servers in the primary Site fail over only if you specifically set up XPU Server Cascading. If you do not specifically setup XPU Server Cascading, then the Site uses the XPU Server in the secondary Site.

# Considerations for Local User Accounts

### Introduction

Starting with SiteProtector system 2.0 SP 7.0, the failover process transfers users, SiteProtector system user groups, and Windows user groups intact. For domain users, the process is seamless. For local users, you must take additional steps to ensure successful failover.

### Providing for local users

You must create interim accounts for local users and user groups in the secondary site.

### Impact on permissions

Permissions are handled differently for domain and for local user accounts.

| User type | Impact on permissions |
|---|---|
| Domain users | Because the security context of a domain user is the same in both primary and secondary Sites, any permissions assigned to these users are valid and accessible in either Site. |
| Local users | Because the security context of local Windows users and user groups exists only within the local Application Server, the permissions assigned to them are inaccessible after failing over. |

**Table 15:** *Impact on permissions for domain versus local users*

### The solution for local users

To avoid having to create permissions on the secondary Site, do the following:

1. Assign permissions by SiteProtector group.
2. Add local users to the SiteProtector Group.
3. In a failover scenario, create temporary user accounts and add those users to the appropriate SiteProtector groups.
4. After failing back, the original permissions are again available, and the interim accounts (since they are local to the secondary Application Server) are inaccessible.

# Failing Over to the Secondary Site

### Introduction

Use the procedure in this topic to fail over to the secondary Site.

**Note:** In some cases, the Sensor Controller remains active in the primary Site even when the primary Site fails. If you encounter this issue, then you must stop the Sensor Controller on the primary Site before you fail over to the secondary Site.

### Prerequisite

You must designate the Site as the Secondary Site. See “Setting the Site as the Primary or Secondary Site” on page 19.

### Procedure

To fail over to the secondary Site:

1. In the left pane, select the Site Node.
2. Click **Tools**→**SecureSync** →**Manage Agents**.

   The SecureSync Manage Agents window appears.
3. Click the Parameters icon.
4. In the **DSN Name** box, type the DSN for the secondary Site Database.

   You must use the DSN name that you created on each Event Collector that points to the secondary Site Database.

   **Example:** EC_*SecondarySiteName*
5. Click the Schedule icon.
6. In the **Recurrence Pattern** section, select **Run once**.
7. In the **Event Time** box, select the date and time to fail over to the secondary Site.

   The default setting is the current date and time.
8. Click **OK**.

   The SiteProtector system checks the status of the primary Site Sensor Controller service. If the status of the Sensor Controller service is stopped, offline, or unreachable, then the job runs successfully. If the status is active, then the job fails. You must stop the primary Site Sensor Controller service, and then repeat Steps 1 through 8.

### Post-failover tasks

After you fail over to the secondary Site, you should perform the following tasks:

- Verify that the status of managed agents is “Active.”
- Verify that managed agents are reporting events to the secondary site Database.
- Stop the scheduled job to import configuration data to the secondary Site.

## Chapter 4

# Failback

## Overview

### Introduction

This chapter explains how to fail back to the primary Site and how to fail back to a reinstalled primary Site. This is the Failback stage of the SiteProtector - SecureSync process.

### In this chapter

This chapter contains the following topics.

# What is Failback?

### Introduction

Failback is the manual process of switching to the original primary Site or to a reinstalled primary Site. This process also involves merging data collected at the secondary Site to the primary Site to ensure that no security data is lost while the primary Site is unavailable.

### Preserving data from secondary Site

The Failback process preserves configuration and event data that is collected at the secondary Site. You can use the SecureSync Import/Export Wizard to transfer data from the secondary Site. When you transfer data from the secondary Site to the primary Site, the SiteProtector system merges the data into the primary Site Database. It does not overwrite any existing data in the Site Database.

### Data transfer time requirements

The data transfer process runs in the background and does not interfere with the loading and processing of current data. The time required to transfer data from the secondary Site to the primary Site depends on the amount of data you are transferring and the current data loading activity on the primary Site. The process can take several days to complete.

### Allowed tasks

After you fail back to the primary Site, you can use the primary Site to perform all SiteProtector system tasks, including the following:

- Access, change, add, and delete policies
- Add agents
- Apply updates
- Change groups and group settings

### Components and agents that fail over

The following stand-alone components fail back to the primary Site:

- Event Collector(s), including the agents that report the Event Collectors
- Agent Manager(s), including the agents that report to the Agent Managers
- SecurityFusion module

### Components that do not fail over

The secondary Site Application Server, Agent Manager, Database, Event Collector, and X-Press Update Server do not fail back to the primary Site.

### Repairing the Site

Before you can fail back to the primary Site, you must repair the primary Site. In most cases, you can perform maintenance tasks on your own or work with the IBM ISS customer support to repair the original primary Site. In some cases, you cannot repair the original primary Site and must reinstall the SiteProtector system.

If you must reinstall the SiteProtector system, then you must complete the disaster recovery process and prepare the reinstalled Site before you can fail back to it.

For more information, see the following topics:

- “Recovering the Primary Site” on page 45
- “Preparation” on page 13

## Choosing a failback process

The process you choose to fail back to the primary Site depends on whether you have to reinstall the SiteProtector system. Table 16 provides information to help you determine the best failback process.

| Did you have to reinstall the SiteProtector system to recover the primary Site? | Then see this topic... | On page... |
|---|---|---|
| No | Failing Back to the Primary Site | 41 |
| Yes | Failing Back to a Reinstalled Primary Site | 43 |

**Table 16:** *Choosing a failback process*

# Space Requirements for Failback

### Introduction

When you fail back to the primary Site, you also transfer data collected at the secondary Site to the primary Site. The process requires temporary drive space for the data transfer jobs and drive space for the data archive file. This topic provides these requirements.

### Temporary space required on the secondary Site

The temporary drive space required on the secondary Site depends on the types of data and the amounts of data that you are transferring. Table 17 lists the requirements for exporting data from the secondary Site to a data archive file.

| Job | Requirements | Location |
|---|---|---|
| Export events from the secondary Site | One event requires approximately 700 bytes of temporary space. | Site Application Server |
| Export policy data from the secondary Site | One policy requires approximately 1-3 MB of temporary space. | Site Application Server |

**Table 17:** *Temporary space requirements for data export jobs*

### Temporary space required on the primary Site

When you import data from an archive file into the primary Site, the job requires temporary space on the drive where the data archive file is stored. The temporary drive space required on this drive depends on the types of data and the amounts of data that you are transferring. Table 18 lists the requirements for importing data from the data archive file.

| Job | Requirements | Location |
|---|---|---|
| Import events into the primary Site | One event requires approximately 700 bytes of temporary drive space. | Shared folder[a] where the data archive file is stored. |

**Table 18:** *Temporary space requirements for data import jobs*

[a] If you are not using a shared folder for data archives, then you must make sure the data archive location contains adequate drive space.

### Example

Table 19 gives examples of the approximate space required to transfer 15 million events from the secondary Site to the primary Site.

| Example | Space Required |
|---|---|
| Export 15 million events from the secondary Site | Approximately 9.7 GB on the secondary Application Server |
| Import 15 million events to the primary Site | Approximately 9.7 GB on the primary Application Server |

**Table 19:** *Examples of space required to transfer data from the secondary Site to the primary Site*

# Failing Back to the Primary Site

### Introduction

Use the procedures described in this topic to fail back to the primary Site.

**Note:** If you do not want to transfer security data collected at the secondary Site to the primary Site, then you can release agents from the secondary Site without transferring data to the primary Site. IBM ISS recommends, however, that you transfer data to the primary Site when you fail back.

### Task overview

Table 20 describes the tasks required to fail back to the primary Site.

| Task | Description |
|---|---|
| 1 | Transfer configuration data from the secondary Site to the primary Site. |
| 2 | Release agents from the secondary Site. |
| 3 | Transfer event data from the secondary Site to the primary Site. |

**Table 20:** *Tasks for failing back to the primary Site*

### Transferring policy data from the secondary Site

To transfer policy data, such as policy changes, from the secondary Site to the primary Site:

1. On the secondary Site, run the export policy data job.
2. On the primary Site, run the import policy data job.

### Release agents from the secondary Site

To release agents from the secondary Site:

1. Start a Console connected to the secondary Site.
2. In the left pane, select the Site Node.
3. Click **Tools→SecureSync→Release Agents.**

   The Release Agents window appears.
4. Click the Parameters icon.
5. In the **DSN Name** box, type the DSN for the primary Site Database.

   **Note:** The default value is RSNTEventCollector. This value represents the DSN for the primary Site.
6. Click the Schedule icon.
7. In the **Recurrence Pattern** section, select **Run once**.
8. In the **Event Time** box, select the date and time to release agents from the secondary Site.
9. Click **OK**.

## Transferring event data from the secondary Site

To transfer event data from the secondary Site to the primary Site:

1. On the secondary Site, run the export event data job.
2. On the primary Site, run the import event data job.

   **Note:** You can specify the time period for which you want to transfer events to the primary Site. The default value is one day's events. If you want to transfer more than one day's events, then you need to change the time range when you run these jobs. This job merges data from the secondary Site into the primary Site Database.

# Failing Back to a Reinstalled Primary Site

## Introduction

Use the procedures described in this topic to fail back to a reinstalled primary Site.

**Note:** If you do not want to transfer security data collected at the secondary Site to the primary Site, then you can release agents from the secondary Site and manage them at the primary Site without transferring data to the primary Site. IBM ISS recommends that you transfer data to the reinstalled Site when you fail back.

## Requirements

Before you fail back to a reinstalled Site, you must complete the procedures to prepare the Site. See "Preparation" on page 13.

## Task overview

Table 21 describes the tasks required to fail back to a reinstalled primary Site.

| Task | Description |
|---|---|
| 1 | Transfer configuration data from the secondary Site to the primary Site. |
| 2 | Release agents from the secondary Site. |
| 4 | Transfer event data from the secondary Site to the primary Site. |

**Table 21:** *Tasks for failing back to a reinstalled primary Site*

## Transferring policy data from the secondary Site

To transfer policy data, such as policy changes, from the secondary Site to the primary Site:

1. On the secondary Site, run the export policy data job.
2. On the primary Site, run the import policy data job.

## Releasing agents from the secondary Site

To release agents from the secondary Site:

1. Start a Console connected to the secondary Site.
2. In the left pane, select the Site Node.
3. Click **Tools**→**SecureSync**→**Release Agents**.

   The Release Agents window appears.
4. Click the Parameter icon.
5. In the **DSN Name** box, type the DSN for the primary Site Database.

   **Note:** The default value is RSNTEventCollector. This value represents the DSN for the primary Site.
6. Click the Schedule icon.
7. In the **Recurrence pattern** section, select **Run Once**.
8. In the **Event time** box, select the date and time to release agents from the secondary Site.
9. Click **OK**.

### Transferring event data from the secondary Site

To transfer event data from the secondary Site to the primary Site:

1. On the secondary Site, run the export event data job.
2. On the primary Site, run the import event data job.

   **Note:** You can specify the time period for which you want to transfer events to the primary Site. The default value is one day's events. If you want to transfer more than one day's events, then you need to change the time range when you run these jobs. This job merges data from the secondary Site into the primary Site Database.

Chapter 5

# Recovering the Primary Site

## Overview

### Introduction

This chapter explains how to recover the primary Site. This is the Disaster Recovery stage of the SiteProtector - SecureSync process. This process requires that you completely reinstall the SiteProtector system.

**Reference:** This chapter does not provide detailed instructions for applying updates or registering agents. For information about the following tasks, see the *SiteProtector System Configuration Guide*:

- Registering and unregistering agents
- Updating the SiteProtector system

### Prerequisite

You must have a full backup copy of the SiteProtector system Database called RealSecureDB. If you do not have a full backup copy of this database, then you cannot perform the procedures in this chapter.

### In this chapter

This chapter contains the following topics.

# Primary Site Recovery Checklist

**Introduction**

This topic provides a task checklist to ensure that you perform all the tasks required to recover the primary site.

**Checklist**

Table 22 provides a checklist of the tasks required to recover the primary site.

| ✓ | Task |
|---|---|
| ❑ | Restore the Site Database.<br>See "Restoring the Site Database" on page 48. |
| ❑ | Reinstall the Application Server.<br>See "Reinstalling the Site Application Server" on page 50. |
| ❑ | Update the SiteProtector system, including all SiteProtector system components, to the most current service pack and XPU levels.<br>See "Updating the SiteProtector System" on page 51. |
| ❑ | Prepare the reinstalled Site.<br>See "Preparation" on page 13. |

**Table 22:** *Checklist for recovering the primary Site*

# Requirements for the Reinstalled Site

### Introduction

The reinstalled Site replaces the original primary Site. The reinstalled Site becomes active when you fail back to the Site.

### Requirements

The reinstalled Site must meet the following requirements:

- The Site must meet the minimum system requirements as specified in the *SiteProtector System Requirements*.
- The components in the reinstalled Site must be the same version, XPU, and Service Pack levels as the components in the secondary Site.
- The following minimum levels are required.

| Component | Minimum Level |
|---|---|
| Event Collector | 6.9 (SP1.13) |
| Agent Manager | XPU 6.9 (SP7.1) |
| SecurityFusion module | SP1.5 |

- The Site time must be synchronized with the time on the secondary Site.
- You must use the following information when you reinstall the Site:
  - IP address of the original Application Server
  - IP address of the original Database
  - Site Group Name of the original site

### Locating IP addresses and Site names

The `Failover_SiteInfo.txt` file contains the IP addresses, host names, and Site names for the original Site. The Wizard includes this file in the data archive file (JAR file) when you export configuration data from the primary Site. The Wizard stores the data archive file in the shared folder that you setup for data archives. You can open the data archive file with a file compression utility, such as WinZip. The procedure for opening the file varies, depending on the utility you use.

# Restoring the Site Database

### Introduction

This topic provides information about restoring the primary Site Database.

### Before You begin

Before you restore the Site Database, you should perform the following tasks:

- Delete the Event Collector and Agent Manager, and Update Server from the secondary Site.
- Verify that you have a full backup of the SiteProtector system Database. The SiteProtector system Database is called *RealSecureDB*.
- Verify that you have access to a Deployment Manager.
- Choose the computer where you want to reinstall the Site Database.
- Load and fully patch the operating system on this computer.
- Install and patch SQL Server on this computer.

### Required information

You must have the following information when you reinstall the Site Database:

- The Site Group Name of the original Site
- The IP address of the original Site Database

### Task overview

Table 23 describes the tasks required to restore the primary Site Database.

| Task | Description |
|---|---|
| 1 | Reinstall the Site Database. |
| 2 | Restore the SiteProtector system data to the Site Database. |

**Table 23:** *Tasks for restoring the primary Site Database*

### Reinstalling the Site Database

To reinstall the Site Database:

1. On the computer where you want to reinstall the Site Database, open Internet Explorer, and navigate to the Deployment Manager.
2. Complete Part 1 of the Recommended installation.

   **Important:** When the installation program prompts you for the Site Group Name and IP address, you must enter the Site Group Name and IP address for the original Site.

### Restoring data to the Site Database

To restore the RealSecureDB backup file to the reinstalled Site Database:

1. On the Site Database computer, issDaemon, and SQLSERVERAGENT services.
2. Open Enterprise Manager, and then restore the RealSecure DB backup.

   **Note:** When you restore the RealSecureDB backup, the process overwrites the RealSecureDB file that was installed when you reinstalled the Site Database.

3. In the SQL Server Enterprise Manager window, select **Console Root**→**Microsoft SQL Servers**→**SQL Server Group**→**(local) (Windows NT)**→**Databases**→**RealSecureDB**→**Users**.

   The RealSecureDB Users window appears.

4. Select all SiteProtector system users, including Event Collector_*HOSTNAME*, Agent Manager_*HOSTNAME*, and SecurityFusionModule_*HOSTNAME*, and then delete the users.

   **Note:** *HOSTNAME* is the name of the computer where the component is installed.

   **Examples:** AgentManager_BACKUPAPP, EventCollector_BACKUPDB, IssApp, and RPDMLogin

5. In the SQL Server Enterprise Manager, select **New Database User**.

   The Database User Properties - New User window appears.

6. In the **Login name** box, select **EventCollector**_*HOSTNAME* where *HOSTNAME* is the name of the host where the component is installed.

   **Example:** EventCollector_BACKUPDB

7. In the **Database role membership** box, select the following permissions:

   - **public**
   - **db_datareader**
   - **db_datawriter**
   - **IssApplication**

8. Restart the issDaemon and SQLSERVERAGENT services.

# Reinstalling the Site Application Server

## Introduction

After you restore the Site Database, you can reinstall the Application Server.

**Caution:** Do not reinstall the Application Server until after you restore the Site Database. The Application Server installation makes important changes to the database, so the database must be restored completely before you reinstall the Application Server.

## Before You Begin

Before you reinstall the Application Server, perform the following tasks:

- Verify that you have access to a Deployment Manager.
- Choose the computer where you want to reinstall the Application Server.
- Load and fully patch the operating system on this computer.

## Required Information

You must provide the following information when you reinstall the Application Server:

- The Site Group Name of the original Site
- The IP address of the original Application Server

## Procedure

To reinstall the Application Server:

1. On the computer where you want to reinstall the Application Server, open Internet Explorer, and navigate to the Deployment Manager.
2. Complete Part 2 of the Recommended installation.

# Updating the SiteProtector System

**Introduction**

After you recover the Site Database and reinstall the Application Server, you must update the SiteProtector system. This process accomplishes the following:

- Restores licenses
- Registers and configures Event Collectors and Agent Managers
- Updates the Site components to the correct versions

**Reference:** For specific instructions on how to perform the tasks described in this topic, see the *SiteProtector System Configuration Guide*.

**Requirements**

The version of the recovered Site and the secondary Site must be the same if you want to transfer data from the secondary Site to the recovered Site.

**Procedure**

To update the SiteProtector system:

1. Start a Console connected to the reinstalled Site.
2. Do you have a backup copy of the LicRep.xml file?

| If... | Then... |
|---|---|
| Yes | 1. Copy the LicRep.xml file to following folder:<br>`Application Server\license\repository`<br>2. Restart the Web Server and Sensor Controller services. |
| No | 1. Remove all licenses.<br>2. Manually add the license files to your SiteProtector system. |

3. Unregister the Event Collector, Agent Manager, and Update Server on the primary Site Application Server and Site Database.
4. Re-register the Event Collector on the Primary Site.
5. Re-register the Agent Manager, and then assign the Agent Manager to the Event Collector on the Primary Site Database
6. Reconfigure the Agent Manager and Update Server.
7. Update all SiteProtector system components, including Event Collectors and Agent Managers, to the same level as the SiteProtector system components in the secondary Site.

## Chapter 6

# Troubleshooting

## Overview

### Introduction

This chapter provides descriptions and solutions for some of the issues you may encounter when you work with the SiteProtector - SecureSync feature. It is not intended to represent a complete list of potential SiteProtector system issues.

### Knowledgebase and IBM ISS Customer Support

For the most complete and up-to-date list of SiteProtector system issues, see the IBM ISS Knowledgebase at http://www.iss.net/support/knowledgebase/. If the Knowledgebase does not help you resolve the issue, contact IBM ISS Customer Support.

### In this chapter

This chapter contains the following topics:

# Issues Related to Event Collectors

### Event Collector fails with primary Site

**Description:** Your only Event Collector fails when the primary Site fails.

**Solution:** After you fail over to the secondary Site, you must manually reassign all managed agents to the Event Collector in the secondary Site. When you fail back to the primary Site, you must manually reassign the agents to the Event Collector in the primary Site. To avoid this problem, you should install an additional stand-alone Event Collector in the primary Site and configure the Event Collector to fail over to the secondary Site.

### Event Collector fails to connect to secondary Database

**Description:** After you fail over to the secondary Site, the Event Collectors cannot connect to the secondary Site Database.

**Solution:** You should verify that user accounts exists in the secondary Site Database for all the Event Collectors. The user name and password for the Event Collectors in the secondary Site Database and the primary Site Database must be exactly the same.

To do this, stop the Event Collector, and then set the user name and password on the database. Use the Event Collector log in tool to set the user name and password on the Event Collector. See “Creating User Accounts for Components in the Site Database” on page 29.

### Verifying the DSN

**Description:** When you fail over to the secondary Site, you want to make sure the Event Collector data is pointing to the correct DNS file.

**Solution:** You can confirm the DSN that is in use in the file “current.policy” located in the `\Program Files\ISS\SiteProtector\EventCollector\current.policy` assigned to the “DataSource” value.

If the DSN is listed incorrectly (RSNTEventCollector or the secondary DSN that you created can be found by searching for the DataSource value) you can stop your issDaemon on the Event Collector, manually correct the DSN, then start the issDaemon on the Event Collector. The new DataSource fill be used by the Event Collector.

# Issues Related to Groups

### Cannot locate group for core components

**Description:** After you import data from the data archive file into the primary Site, the SiteProtector system core components do not appear in the top level group.

**Solution:** You should look for the core components in the Ungrouped Assets folder. Sometimes, the import job moves the components to this folder.

If the secondary Site was grouped on the primary Site, then the components should be in that group when you fail over.

# Issues Related to Local User Permissions

**After failing over, permissions for local users are inaccessible**

**Description:** The security context for local users exists within the local Application Server of the primary Site, so the permissions for these users is inaccessible on the secondary Site.

**Solution**: See "Considerations for Local User Accounts" on page 35.

# Issues Related to Agents

### Offline status

**Description:** After you run the Manage Agents job, the status of some agents is “Offline.”

**Solution:** You should restart the issDaemon service on the agent. This action automatically resets the control channels used by the agents and should return the agent status to “Active.”

### Not Responding status

**Description:** After you run the Manage Agents job, the status of some agents is “Not Responding.”

**Solution:** You should verify that you distributed the keys for the Site that is trying to manage the agents. See “Distributing Site Keys to Agents” on page 17.

## Issues Related to Distributing Site Keys

### No key subdirectories in the key directory

**Description:** The key distribution job fails because the CerticomNRA and RSA key subdirectories do not exist in the `failover\keys` directory.

**Solution:** You should verify that the subdirectories exist in the `failover/keys` directory, and then run the key distribution job again. See "Distributing Site Keys to Agents" on page 17.

### Agent status is Not Responding

**Description:** The key distribution job does not distribute keys to a agent when the status of the agent is "Not Responding."

**Solution:** You should verify that all the agents are Active, and then run the key distribution job again. The job can distribute keys to Active agents only.

### Application Server does not have Key Administrator permission

**Description:** The key distribution job fails because the Application Server does not have Key Administrator permissions on the agent.

**Solution:** You should add the Key Administrator role to the agent.

To add the key administrator role:

1. On the sensor, stop the issDaemon service.
   - On Windows, stop the issDaemon service
   - On Linux/Solaris, run `/etc/init.d/realsecure stop`.
   - On Nokia, run `/opt/ISS/issDaemon/issd -all`.
2. Open the iss.access file on the sensor.
   - On Windows, the file is located in `\Program Files\ISS\issDaemon\iss.access`.
   - On Linux/Solaris/Nokia, the file is located in `/opt/ISS/issDaemon/iss.access`.

   **Example:** The following is an example of the file:

   ```
   [\];
   [\Roles\];
   [\Roles\MasterStatusManager\];
   [\Roles\MasterStatusManager\hostname\];
   [\Roles\KeyAdministrator\];
   [\Roles\KeyAdministrator\hostname\];
   ```

   Some lines might include hostnames. These hostnames are the hostnames of management consoles that you use to manage the agent.

3. Directly below the `[\Roles\KeyAdministrator\];` line, add the following line to the file:

   ```
   [\Roles\KeyAdministrator\RSSP_appserver_hostname\];
   ```

   *`RSSP_appserver_hostname`* should be the hostname of the SiteProtector system Application Server machine.

   **Example:** The following is an example of the file after you add the key administrator role:

   ```
   [\];
   [\Roles\];
   [\Roles\MasterStatusManager\];
   [\Roles\MasterStatusManager\otherhostname1\];
   [\Roles\MasterStatusManager\otherhostname2];
   [\Roles\MasterStatusManager\otherhostname3_username\];
   [\Roles\KeyAdministrator\];
   [\Roles\KeyAdministrator\RSSP_appserver_hostname\];
   [\Roles\KeyAdministrator\otherhostname1];
   [\Roles\KeyAdministrator\otherhostname3_username];
   ```

4. Save the file.
5. Restart the issDaemon.
   - On Windows, start the issDaemon service
   - On Linux/Solaris, run `/etc/init.d/realsecure start`.
   - On Nokia, run `/opt/ISS/issDaemon/issd &`.

# Issues Related to Exporting Data

### Services not allowed to access shared folder

**Description:** The data export job fails because you are using a shared folder for data archives, and either the Sensor Controller service, the SQL Server service, or both services are not configured to log on as a user with permission to access the shared folder.

**Solution:** You should verify that the Sensor Controller and SQL Server service are both configured to log on as a user with permission to access the shared folder.

- See "Setting Up a Shared Folder for Data Archives" on page 22.
- See "Configuring Services with Shared Folder Permissions" on page 24.

### Not enough space

**Description:** The export job fails because the destination folder for the data archive file does not have enough temporary space to run the job or drive space to store the archive file.

**Solution:** You should verify that the destination folder has enough temporary space and drive space. See "Setting Up a Shared Folder for Data Archives" on page 22.

# Issues Related to Importing Data

### Application Server does not have database permission

**Description:** The import job fails because the Application Server user account called IssApp does not have “bulkadmin” permission. This permission allows the Application Server to insert data into the Site Database.

**Solution:** You should verify that Application Server user account called IssApp has “bulkadmin” permission. See “Configuring Application Server Permissions” on page 20.

### Database full

**Description:** The import job fails because the Site Database where you are trying to import data is full.

**Solution:** You should create more space in the Database. See the *SiteProtector System Configuration Guide*.

### Component versions do not match

**Description:** The import job fails because you are trying to transfer data between Sites that contain components with different version numbers.

**Solution:** You should verify that the components on both Sites are at the same XPU and Service Pack levels. If not, then you should update the components on both Sites to the same level, run the data export job again, and the run the data import job again.

**References:**

See “Secondary Site Requirements and Considerations” on page 16.

See “Requirements for the Reinstalled Site” on page 47.

# Issues Related to Disaster Recovery

### Licenses do not exist

**Description:** The required licenses do not exist on the reinstalled primary Site.

**Solution:** Copy the LicRep.xml repository file from the secondary Site to the reinstalled Site. You can also remove all the license files, and then re-add all the license files to correct this problem.

### Cannot locate the original Site information

**Description:** You cannot locate the original IP addresses, host names, and Site Group Name for the original primary Site. When you reinstall the primary Site, you must use the same IP addresses, host names, and Site names that were used in the original Site.

**Solution:** You can locate this information in the Failover_SiteInfo.txt file. To create this file, you should run an export configuration data job on the primary Site. This job automatically creates the Failover_SiteInfo.txt and includes it in the data archive file. You can open the archive file using a file compression utility such as WinZip.

# Downloading Log Files

**Introduction**

The SiteProtector system creates log files for each SiteProtector - SecureSync job. The entries in the log file indicate whether the job completes successfully and also provide other information, such as the following:

- The date and time of the job
- The types of data exported or imported
- The amount of data exported or imported

**Log file descriptions**

Table 24 describes the log files that the SiteProtector system creates when it runs a data import or export job:

| Log file | Description |
|---|---|
| SMTAgentExport.out | The SiteProtector system creates this file each time it runs an export data job and saves the file to the following directory:<br>`Application Server\bin\failover\` |
| SMTAgentImport.out | The SiteProtector system creates this file each time it runs an import data job and saves the file to the following directory:<br>`Application Server\bin\failover\` |

**Table 24:** *Log files for data import and export jobs*

**Sensor Controller log file**

The SiteProtector system also creates entries in the Sensor Controller log file when it runs jobs related to failover and failback. The Sensor Controller log file provides detailed information that can be helpful in troubleshooting the following jobs:

- Data export jobs
- Data import jobs
- Key distribution jobs
- Manage agent jobs
- Release agent jobs

**Procedure**

To download a log file:

1. Select the Site Node.
2. Click **Tools**→**System Logs**→**Download System Logs**.
3. Expand **Sensor Controller**, and then expand **SecureSync@***`your_site_IP_address`*.
4. Expand the folder for a job, and then select the log file.
5. Click **Download**.

# Index