IBM Proventia® Server Intrusion Prevention System for Windows® Technology

Guide to Migrating RealSecure® Server Sensor to Proventia Server IPS for Windows

May 22, 2009

Overview

Introduction

The Proventia Server Migration Utility simplifies the migration from RealSecure Server Sensor to Proventia Server IPS for Windows, Version 2.0 and later. The utility converts many of the settings you have in your server sensor policy to the format used by the Proventia Server IPS for Windows agent.

In this document

This document contains the following topics:

Before You Migrate

Introduction

Before you migrate your server sensor policy settings to a Proventia Server IPS agent, you should consider the information in this topic.

Install XPU 28.010

X-Press Update 28.010 adds functionality that silently uninstalls server sensor when the installation of the Proventia Server IPS agent begins. If you install this update, you do not need to manually uninstall server sensor before you install the Proventia Server IPS agent.

Record settings that will not migrate

The migration utility does not migrate all of the settings you have configured for your server sensor. If you want the Proventia Server IPS agent to use settings that are not migrated by the utility, you must manually record those settings before you uninstall the server sensor.

Reference: "What Settings Does the Utility Migrate" on page 3.

Imported policies overwrite existing policies

When you import a migrated policy, the imported policy overwrites the current policy settings. Import the migrated server sensor policy settings before you configure any Proventia Server IPS policies.

Download the migration utility

To download the migration utility:

1. Sign in to the Download Center at http://www.iss.net/download/.
2. In the **Select a Product** list, select **Proventia Server**.
3. Click **Go**.
4. In the **Version** list, select **Proventia Server for Windows**.
5. Click **Go**.
6. Click the **Other Updates** tab.
7. In the Proventia Server 2.x Policy Migration Utility section, click **Continue**.

   Note: Be sure to select the Migration Utility for the version of Proventia Server for Windows that you are migrating to.
8. Accept the license agreement.
9. Click **Submit**.
10. Click **Download**.
11. Browse to the location where you want to store the .zip file and click **Save**.
12. Extract the .zip file.

Next step

Review "What Settings Does the Utility Migrate" on page 3.

What Settings Does the Utility Migrate

Introduction

The migration utility migrates certain policy settings from your server sensor deployment. The utility does not migrate all of the settings that determine how your server sensor protects your system.

Policy settings that are migrated

The utility migrates the following server sensor policy settings:

- pre-defined network event signatures
- audit event rules
- registry event rules

Important: When you import the migrated server sensor policy settings to the appropriate Proventia Server IPS for Windows policy, the imported policy settings overwrite any current policy settings.

Settings that are not migrated

The migration utility does not migrate the following server sensor settings:

- user-defined network event signatures
- firecell rules
- buffer overflow exploit protection rules
- network monitoring setting

  Note: When you migrate to Proventia Server IPS for Windows, network monitoring will be enabled regardless of the setting you had in server sensor.
- fusion scripts

  Important: Signatures that use fusion scripting may no longer function as expected after the migration.
- Enforce Audit Policy setting
- packet logging settings
- evidence logging settings
- pcd.packetfilters tuning parameter setting to exclude packets from analysis
- AllowAllAcknowledgementPackets tuning parameter setting

Reference: See Table 1, "Guidelines for settings not migrated by the utility" on page 6 for guidance on how to migrate these settings.

Next step

"Exporting and Migrating the Server Sensor Policy" on page 4

Exporting and Migrating the Server Sensor Policy

Introduction

Before you can run the migration utility on the server sensor policy, you must export the policy to the directory where you saved the migration utility.

Exporting the server sensor policy

To export the policy:

1. Right-click a group, and then select **Manage Policy**.

   The Policy tab appears.
2. Select the policy to export.
3. Click **Action→Export**.
4. Navigate to the location where you saved the migration utility, and then click **Export**.

   Note: You can change the name of the file when you export it.

Running the migration utility

To run the migration utility:

- From the command line on the SiteProtector system, run the following command:

  migrate *your_server_sensor_policy_name*

  The migration utility creates the following files:

  - audit.xml
  - ips.xml
  - regintegrity.xml

Next step

"Importing the Migrated Policy Settings" on page 5

Importing the Migrated Policy Settings

Introduction

After you have run the server sensor policy through the migration utility, you must import the policies to the groups that you want to use those policy settings.

Importing the new policy

To import a policy:

1. In SiteProtector, select the applicable group, and then select the **Policy** view.
2. In the **Agent Type** list, select **Proventia Server for Windows**.
3. In the **Agent Version** list, select **2.x**.

   Note: Be sure to select the version of Proventia Server for Windows that you are migrating to.
4. In the navigation pane, select the group.

   The Policy Inventory window for the group appears in the right pane.
5. In the right pane, do the following:

Right-click this policy...	then...	Browse to...	to import...
System Integrity Monitoring	click **Import**	audit.xml	audit rule settings
Registry Integrity Monitoring	click **Import**	regintegrity.xml	registry rule settings
Security Events	click **Import**	ips.xml	network signature settings

Next step

"Reconfiguring Settings that were not Migrated" on page 6

Reconfiguring Settings that were not Migrated

Introduction

The migration utility does not migrate all of the settings from your server sensor configuration. You must manually configure those settings that were not migrated, if you want the Proventia Server IPS agent to use them.

Manually migrating settings

The following table lists the settings that are not migrated by the utility and provides guidance on how to manually migrate those settings:

Server Sensor Setting	Proventia Server IPS Setting	Comments
User-defined network event signatures	Not currently supported	
Firecell rules	Firewall policy	The Proventia Server IPS firewall does not process firewall rules in the same way as the server sensor firewall. Review the *Administrator Guide for Proventia Server for Windows* to determine how to configure the Proventia Server IPS firewall to achieve the same protection provided by server sensor.
Buffer overflow exploit protection rules	Set policy level BOEP settings in the BOEP policy Set agent level BOEP settings from the local user interface for the agent	
Network monitoring component	In version 2.0, not supported In version 2.1, Administration policy ->Management tab	In Proventia Server IPS, the network monitoring component is enabled by default.
Fusion scripts	Not currently supported	Signatures that use fusion scripting may no longer function as expected after the migration.
Enforce Audit Policy	System Integrity Monitoring policy	
Packet logging	Security Events policy->Packet Logging tab	
Evidence logging	Security Events policy->Evidence Logging tab	
pcd.packetfilters tuning parameter	Bypass filter policy	This parameter excludes packets from a specified IP address from analysis.
AllowAllAcknowledgementPackets tuning parameter	Not currently supported	This parameter configured server sensor to allow inbound TCP reply traffic to pass through the firewall.

Table 1: *Guidelines for settings not migrated by the utility*

Next step

Review Chapter 2 in the *Administrator Guide for Proventia Server for Windows* for instructions on how to create an agent build to install Proventia Server IPS agents.