IBM Proventia Network IPS

IBM Proventia Network Intrusion Prevention System Appliance Migration Guide

Version 4.1

Publication Date: July 2010

Contents

About this publication

Scope

This guide describes how to update the firmware and how to migrate your policies for the IBM Proventia® Network Intrusion Prevention System (IPS) appliance.

Additional documentation is located on the IBM® ISS Web site at http://www.iss.net/support/documentation/.

Intended audience

This guide is intended for network security system administrators who are responsible for installing and configuring IPS systems. This guide assumes that you are familiar with network security policies and IP network configuration.

Technical Support Contacts

IBM Internet Security Systems (IBM ISS) provides technical support to customers who are entitled to receive support. You can find information related to Customer Support hours of operation, phone numbers, and methods of contact on the IBM ISS Customer Support Web page.

The IBM ISS Customer Support site

The IBM ISS Customer Support Web page at http://www.ibm.com/services/us/iss/support/ provides direct access to online user documentation, current versions listings, detailed product literature, white papers, the Technical Support Knowledgebase, and contact information for Customer Support.

Contact information

For contact information, go to the IBM ISS Contact Technical Support Web page at http://www.ibm.com/services/us/iss/support/contacts.html.

Chapter 1. Planning The Firmware Update And Policy Migration

Firmware version 4.1 is a major feature update for the Proventia® Network Intrusion Prevention System product line. This update offers many new features and changes from previous releases. Please read through this document in its entirely and follow the procedures carefully *in the order in which they appear*.

Important: The firmware update processes provide important notifications and messages as you progress. Please take time to read the messages rather than dismissing them without reading them. The information provided can help ensure a successful update.

Supported appliance models

Proventia Network IPS firmware version 4.1 is available for the following appliance models:

- GX3000 series
- GX4000 series
- GX4000 series, V2
- GX5000 series
- GX5000 series, V2
- GX6000 series
- GV200
- GV1000

Two firmware updates

Two firmware updates are required to update your appliance to firmware version 4.1. The SiteProtector Database Service Pack (DBSP), provided contains changes to support both firmware updates.

Before you start the upgrade process, your appliance should be running one of the following firmware versions: 1.7, 2.4, 3.1, or 3.2. The next available firmware version (1.8, 2.5, or 3.3) prepares currently supported hardware models to receive the major firmware update, version 4.1.

Firmware updates are available on the Manual Download Center http://www.iss.net/download/ before they become available for automatic discovery and download.

Notes:

- You can download both firmware update packages during the same session. However, you must apply the updates in order. That is, you must update to the next available version for your appliance model before you can update to firmware version 4.1. If you use SiteProtector 2.0, Service Pack 7.0 or Service Pack 8.0, to manage your appliances, you must complete some important migration steps between updating to the next available update and updating to firmware version 4.1.
- If your appliance is not running current firmware, you may need to install additional firmware to bring your appliance to the current firmware level.

Available update paths

The correct update path depends on the appliance model and the firmware version it is running. Refer to the table to see your options.

Table 1. Models and available update paths

Model	Current® version	Update path
• **GX3000 series** • **GX4000 series** • **GX5000 series**	**1.7**	**1.8 → 4.1**
GX6116	**2.4**	**2.5 → 4.1**
• **GV200** • **GV1000** • **GX4000 series, V2** • **GX5000 series, V2** • **GX6116**	**3.1**	**3.3 → 4.1** **Note:** Appliances running firmware version 3.1 must update directly to 3.3.
• **GX4000 series, V2** • **GX5000 series, V2** • **GX6116**	**3.2**	**3.3 → 4.1**

Merged update paths

After you have completed the update for firmware version 4.1, all currently supported appliance models are on the same firmware version and share the same update stream for future updates. In addition, this change removes limitations related to grouping similar hardware models into their own groups in SiteProtector. That is, you can include a variety of appliance models in the same SiteProtector group.

Because all supported appliance models can run the same firmware version, you can now manage different appliance models in the same SiteProtector group because they all use the same policy versions.

Example:
Before this release, GX6116 appliances could not be in a group with other appliance models because of policy differences. This restriction no longer applies.

Three supplemental steps for a smooth update

Because this is a major firmware update, you must complete some steps in addition to the process you normally use to upgrade your appliances.

- Backup your current firmware and settings and save the backup copy to a safe location on a different piece of hardware. This step is optional, but it is a good practice. Chapter 2, “Backing Up Current Settings,” on page 5
- Migrate your SiteProtector policies to use the new policy structure. Chapter 3, “Updating Firmware and Migrating SiteProtector Policies,” on page 7

  Note: If you do not use SiteProtector to manage your appliances, you do not need to complete the policy migration steps. If you use SiteProtector 2.0, Service Pack 8.1, deploy only the Web Application Protection policy since all other policies migrate automatically.
- Update security content to the latest protection level. Chapter 4, “Getting The Latest Security Content,” on page 11

Follow the steps outlined in this guide in the order in which they are presented to help ensure a successful update.

Process overview

This section provides a high-level overview of necessary migration steps. Detailed procedures are included later in this guide. Please refer to the steps and follow them in order.

1. Backup your current firmware and settings, and save the backup copy to a safe location on a different piece of hardware. This step is optional, but it is a good practice.
2. Install the Database Service Packs (DBSPs) required to support the updates to the next available version and to firmware version 4.1.
3. Update your appliance to firmware version 1.8, 2.5, or 3.3 (as appropriate for your appliance model).
4. Migrate your SiteProtector policies to use the new policy structure.

   Note: If you do not use SiteProtector to manage your appliances, you do not need to complete the policy migration steps. If you use SiteProtector 2.0, Service Pack 8.1, deploy only the Web Application Protection policy since all other policies migrate automatically.
5. Update security content to the latest protection level.

Remember, the order in which you complete these steps is important.

Other considerations

- Updating to firmware 4.1 re-images and re-partitions the appliance. Any custom changes or third-party software solutions you are using on the appliance are lost.
- Local tuning parameters that were set on the appliance will be lost. Only the global tuning parameters (set in SiteProtector) are migrated.
- Use only the supported Java™ Runtime Environment (JRE) listed in the readme document.
- Executable routines for user specified responses may not work after you update the appliance to firmware version 4.1. If you are updating from firmware version 2.4, your executable routines will not work.

Note: Use this guide in conjunction with **Technote 1437344**. Check there for latest updates.

Use the Knowledgebase

The knowledgebase, at http://www.ibm.com/support/entry/portal, is the source of the latest information available about migration and other subjects. Use this guide in conjunction with **Technote 1437344**. Check there for the latest updates.

Chapter 2. Backing Up Current Settings

Firmware 4.1 is a major firmware update. This update re-partitions the appliance's hard drives during the update process. To keep configurations and settings, copy backup files off of the appliance to a safe, convenient place on your network. You can retrieve these files to restore a backup version.

This chapter describes how to back up your current settings and configurations. This is a precautionary measure and the backup will probably not be needed.

Backing Up Using Remote Installation

You can use this method to back up a working version of your settings using remote installation, either SSH or serial console connection.

Procedure

1. Log on to the appliance as `admin` using SSH or serial console.
2. From the Configuration Menu, select **Appliance Management**.
3. Select **Backup Current Configuration**.
4. Select **OK**.

   The appliance could be offline for several minutes while it completes the restart.
5. When the appliance comes back online, copy files from one of the following appliance drives to a designated place off the appliance. The drive you copy from depends on the firmware version running on the appliance.
   - `/backup/0/images`
   - `/backup/images`
   - `/restore/0/images`
   - `/restore/images`

Chapter 3. Updating Firmware and Migrating SiteProtector Policies

Firmware 4.1 introduces new policies and policy structures. This chapter explains how to update to these new policies, as well as how to save and migrate existing policies into the new 4.1 structures for appliances managed in SiteProtector.

Important: If you do not use SiteProtector to manage your appliances, your policies are migrated automatically. You can move onto updating your security content. Chapter 4, "Getting The Latest Security Content," on page 11.
If you use SiteProtector 2.0, Service Pack 8.1, deploy only the Web Application Protection policy since all other policies migrate automatically.

Process Overview

This topic offers an overview of the steps required to update and migrate IPS policies to firmware 4.1 structures for an appliance managed in SiteProtector.

Important: You must follow the exact order of steps or your firmware update may be unsuccessful.
The steps for migrating policies and updating firmware are:

1. Apply the applicable DBSP to SiteProtector.
   - DBSP 7.37 for SiteProtector 2.0, Service Pack 7.0
   - DBSP 8.12 for SiteProtector 2.0, Service Pack 8.0
   - DBSP 9.1 for SiteProtector 2.0, Service Pack 8.1

   Note: For Service Pack 8.1, deploy only the Web Application Protection policy since all other policies migrate automatically.
2. Choose one IPS appliance from each SiteProtector group.
3. Update that appliance to the first update (1.8, 2.4, or 3.3) using Proventia Manager (the appliance LMI).
4. Locate the new .zip file created by the update and put it on the computer that runs the SiteProtector Console.
5. Extract the files.
6. Using SiteProtector, import, save, and deploy the extracted policy files.
7. Verify your policies have been migrated and deployed successfully.
8. After verification, update your IPS appliances to firmware version 4.1.

Applying The Database Service Pack

Apply the applicable Database Service Pack (DPSP). The DBSP contains SiteProtector updates that must be in place before you start the update process.

Applicable DBSP's are:

- DBSP 7.37 for SiteProtector 2.0, Service Pack 7.0
- DBSP 8.12 for SiteProtector 2.0, Service Pack 8.0
- DBSP 9.1 for SiteProtector 2.0, Service Pack 8.1

Updating The Appliance To The First Update

The first update saves your current policy configurations and puts them in a .zip file.

Update one appliance in every IPS group.

In Proventia Manager go to **Updates → Available Installs** and **Updates → Available Downloads** and update the appliance to the appropriate firmware version. The appliance recognizes the applicable firmware. To apply the update, the appliance must restart.

Getting The Files

This topic describes what to do with the migration file created by the update.

About this task

Note: Perform this task on one appliance in each IPS group.

Procedure

1. When the appliance is back online, log into Proventia Manager and go to **System → Logs** and download **migrated_policies_4.1.zip**.

   Note: On appliances that are already updated to firmware 4.1, the file is entitled **migrated_policies_4.1.tgz**.
2. Place the migration file on the computer that runs the SiteProtector Console.
3. Extract the files onto the computer that runs SiteProtector using a preferred method.

Importing 4.1 Policy Structures For Shared Objects

This topic explains how to import, save, and deploy the firmware 4.1 policy structures for shared objects into SiteProtector.

About this task

Important: You must select **Agent Version 4.1** or the policy migration will fail.

In SiteProtector:

Option	Setting
Go to	Policy
Agent Type	Network IPS
Agent Version	4.1

The shared objects are:

- **Protection Domains**
- **Response Objects**
- **Trust X-Force Settings** or **X-Force Virtual Patch**

Note: The **Management and TCP Reset Interfaces** and **Security Interfaces** policies are device level policies. After you update to firmware 4.1, you will see these policies at the device level in SiteProtector.

Procedure

1. In the navigation pane, select **Default Repository**.

   Note: If you are using a repository other than the default, select that repository.
2. Select **Shared Objects** in the navigation pane.
3. Select the policy in the details pane.
4. Go to **Action** and select **Import**.
5. Browse to the location of the unzipped policies and select the appropriate file to match the policy you are working with.
6. **Open** the policy and click **Save**.
7. In the Save Policy Version window, select the **Force affected components/appliances to contact SiteProtector when save completes** checkbox, and click **OK**.
8. Close the policy and repeat the procedure for the remaining shared objects.
9. Verify that the 4.1 policy structures migrated successfully. In SiteProtector, go to the default repository and look for the deployed policies.

Importing 4.1 Policy Structures For Groups

This topic explains how to import, save, and deploy the firmware 4.1 structures for group level policies into SiteProtector.

About this task

Important: You must select **Agent Version 4.1** or the policy migration will fail.

In SiteProtector, select a group and the following options:

Option	Setting
Go to	Policy
Agent Type	Network IPS
Agent Version	4.1

The group policies are:

- **Alerts Settings**
- **Connection Events**
- **Data Loss Prevention**
- **Firewall Rules**
- **Open Signatures**
- **Remote Access**
- **Response Filters**
- **Rolling Packet Capture Settings**
- **Security Events**
- **SNMP**
- **Tuning Parameters**
- **User Defined Events**
- **Web Application Protection**

Note: The **Management and TCP Reset Interfaces** and **Security Interfaces** policies are device level policies. After you update to firmware 4.1, you will see these policies at the device level in SiteProtector.

Procedure

1. In the navigation pane, select **Default Repository**.

   Note: If you are using a repository other than the default, select that repository.
2. Select the policy type.
3. Go to **Action** and select **Import**.
4. Browse to the location of the unzipped policies and select the appropriate file to match the policy you are working with.
5. **Open** the policy and click **Save**.
6. In the Save Policy Version window, enter any comments and select the **Deploy this New Version** checkbox.
7. In the Deploy Policy window, select the appropriate target group, select the **Force affected components/appliances to contact SiteProtector when save completes** checkbox, then click **OK**.
8. Close the policy and repeat the procedure for the remaining group level policies.
9. Verify that the 4.1 policy structures migrated successfully. In SiteProtector, in the policy view, go to the IPS group and look for the deployed policies.

What to do next

After the successful update and migration of all shared objects and group level policies, update the firmware to 4.1. You can then update all appliances in the group to firmware version 4.1.

Chapter 4. Getting The Latest Security Content

IBM X-Force® regularly releases security content as new vulnerabilities are discovered. The security content is current at the time that the firmware versions are available.

For most firmware updates, this step is not required because the latest security content is still available after the update. Firmware 4.1 re-partitions the appliance's hard drives. Any security content on the appliance is lost. You must update to the latest security content to ensure the highest level of security.

In Proventia Manager, go to **Manage System Settings** → **Updates and Licensing** → **Administration**.

In SiteProtector, select the **Update Settings** policy.

Chapter 5. Migrating Undeployed IPS Policies In SiteProtector

This topic is designed to help you migrate undeployed IPS policies in SiteProtector that you may need to deploy later to a firmware 4.1 appliance. Consider migrating undeployed policies to firmware 4.1 now in case you decide to use them later.

Migrating Procedure

Before you begin

Upgrade or re-image appliances to firmware 4.1 and migrate all deployed policies in SiteProtector.

About this task

You do not need to complete these steps if you do not use SiteProtector to manage policies or if you are using SiteProtector 2.0 Service Pack 8.1 with Database Service Pack 9.1 or later installed.

Procedure

1. Copy the TGZ file entitled **migrate_post_41_install.tgz** from the IBM ISS Download Center at http://www.iss.net/download/ to an appliance that has been upgraded to firmware 4.1.
2. Install the script using the following command: `tar -C / -xzvf migrate_post_41_install.tgz`
3. From a shell prompt logged in as `root`, create a temporary directory in which to copy the undeployed policy files (XML files) to be migrated. **Example**: The command `mkdir -p /home/admin/xml_migrate` would create a directory called `/home/admin/xml_migrate`.
4. Use the **Export** feature in SiteProtector to export the undeployed policy files.
5. Copy the policy (XML) files to be migrated to the temporary directory that you created.
6. From the shell prompt logged in as `root`, run the migration script: `migrate_post_41.sh [source policy directory] [zip file name]` **Example**: `migrate_post_41.sh /home/admin/xml_migrate my-migrated-policies` This sample command would take all of the xml policy files in `/home/admin/xml_migrate`, migrate them to 4.1 policy files, and compress them into a file named **my-migrated-policies.zip**.

   Note: The zip file will be located in the `/cache/iss` directory.
7. Copy the zip file from the appliance (`/cache/iss`) to your SiteProtector computer.
8. Extract the files from the zip file.
9. Import the new policies into SiteProtector at **Agent Type: Network IPS** and **Agent Version: 4.1**.

Notes For Migrating Undeployed IPS Policies

- Only one copy of each policy file should be stored in the directory to be migrated. If you need to migrate multiple versions of the same file, create multiple directories and place one copy in each directory.
- The script migrates all polices found in the source directory. You get a warning message in the output if any expected policy files are not found.
- If you migrate Global Tuning Parameters, you get four migrated policies:
  - **RollingPacketCaptureSettings_1.0.xml**
  - **TuningParameters_5.0.xml**
  - **TrustXForceSettings_1.0.xml** (This policy file is for SP 7)

– **XForceVirtualPatch_1.0.xml** (This policy file is for SP 8)

Note: TrustXForceSettings_1.0.xml and **XForceVirtualPatch_1.0.xml** are different versions of the same policy. The policy names are different to accommodate different versions of SiteProtector.

Chapter 6. Frequently Asked Questions

What models can be updated to 1.8?=

- GX3000 series
- GX4000 series
- GX5000 series

What models can be updated to 2.5?

GX6116

What models can be updated to 3.3?

- GV200
- GV1000
- GX4000 series, V2
- GX5000 series, V2
- GX6116

What models can be updated to 4.1?

- GX3000 series
- GX4000 series
- GX4000 series, V2
- GX5000 series
- GX5000 series, V2
- GV200
- GV1000

What Database Service Packs are required to support the firmware?

- DBSP 7.37 for SiteProtector 2.0, Service Pack 7.0
- DBSP 8.12 for SiteProtector 2.0, Service Pack 8.0
- DBSP 9.1 for SiteProtector 2.0, Service Pack 8.1

Is it necessary to import policies you manage at the device level into an IPS group for the firmware version 4.1 update?

No. If you have policies that you manage at the device level, you do not need to import them into a group for the update. After you update to firmware version 4.1, you will see these policies at the device level in SiteProtector.

Appendix. Policy Changes For Firmware 4.1

Table 2. New firmware 4.1 policies

Policy name	Description
Alerts Settings	Specifies settings for sensor and health alerts. In previous versions, this information was at the device level in local tuning parameters. This policy is now a group level policy.
Data Loss Prevention	Specifies settings to inspect and analyze packets for Personal Identifiable Information (PII) and other confidential information on the network.
Management and TCP Reset Interfaces	Specifies the management and TCP reset interface (formerly called ports) settings. This policy includes setting the host name, assigning a DNS search path, and setting the speed and duplex.
Rolling Packet Capture Settings	Specifies settings to capture and store network packet information for use in troubleshooting or general network analysis.
Security Interfaces	Specifies the adapter list and high availability settings.
Trust X-Force Settings or **X-Force Virtual Patch**	Specifies functionality to automatically set the block response for events that X-Force recommends. In previous versions, this information was in the global tuning parameters section.
Web Application Protection	Specifies the use of attack signatures, audit signatures, and parameter names (keywords) from the IBM® ISS Protocol Analysis Module (PAM) engine to provide overall protection against Web application security attacks. **Note:** Signatures including SQL Injection and Cross Site Scripting are located in the Web Application Protection policy.

Table 3. Policies that are no longer applicable

Policy name	Description
Local Tuning Parameters	Specified system settings such as: • Sensor error, warnings, and informational alerts • Network adapter cards • Alert queue size • Advanced parameters

Table 4. Policies and levels

Policy name	Level
Alerts Settings	Group
Connection Events	Group
Data Loss Prevention	Group
Firewall Rules	Group
Management And TCP Reset Interfaces	Device
Open Signatures	Group

Table 4. Policies and levels (continued)

Policy name	**Level**
Protection Domains	Shared object
Remote Access	Group
Response Filters	Group
Response Objects	Shared object
Rolling Packet Capture Settings	Group
Security Events	Group
Security Interfaces	Device
SNMP	Group
Tuning Parameters	Group
Update Settings	Group
User Defined Events	Group
Trust X-Force Settings or **X-Force Virtual Patch**	Shared object
Web Application Protection	Group

Notices

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

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

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

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

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

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

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

IBM Corporation
Project Management
C55A/74KB
6303 Barfield Rd.,
Atlanta, GA 30328
U.S.A

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

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

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

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

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

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

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

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

Printed in USA