



Upgrade Technical FAQ
For
SiteProtector 2.0 Service Pack 5

Introduction

SiteProtector 2.0 Service Pack 5 introduces some new architecture and changes in SiteProtector. This document is intended to highlight these changes that users should be aware of prior upgrading from SP4 to SP5.

Table of Contents

1.	What is new in SiteProtector 2.0 SP5?	1
•	Central Responses	1
•	Asset Protection View.....	1
•	SiteProtector User Auditing.....	1
•	New Policy editor for Proventia G400 and Proventia G2000.....	2
•	VPN wizard for Proventia M-Series appliances	2
•	Desktop Controller Renamed to Agent Manager.....	2
•	New X-Press Update Server Component.....	2
•	New Analysis columns	2
•	New Analysis views.....	2
•	Event loading process enhancements.....	2
•	New Database Maintenance functions.....	2
•	New Reports.....	2
2.	What is different about the Sp5 upgrade from SP upgrades in the past?.....	2
3.	What Database Schema changes have been made which effect custom event extraction?.....	2
4.	What changes are being made to the event loading process?	3
5.	What actions are being audited in the new User Auditing functionality?	3
6.	What is the Agent Manager?.....	4
7.	How does the X-Press Update Server work?	4

1. What is new in SiteProtector 2.0 SP5?

There are several new features and functions in SP5 such as:

- **Central Responses** – Responses such as email and SNMP can be sent centrally from SiteProtector instead of from the agents themselves. The response rules that can be created at the management level are much more flexible and advanced than previously possible through the agents. Additionally thresholds can be performed on the responses so that you can control how many events are required prior to sending an email response. For example, you only want an email sent if 5 instances of these events occur within a 15 minute interval and only three of these emails in a given hour.
- **Asset Protection View** – Two new columns in the asset tab have been added to reflect a protection level that you currently have with the assets in your environment. The protection column will display what type of protection agents exist on the asset. The Risk index column will reflect the dynamically updated list of vulnerabilities from the latest CRI as well as other important threats which are identified by X-Force.
- **SiteProtector User Auditing** – Auditing for users within the SiteProtector system has been added. A report by user or activity is available to enable the tracking of user's activity within SiteProtector.

- **New Policy editor for Proventia G400 and Proventia G2000** – The policy editor for the newest Proventia G-Series appliances takes advantage of a new policy editor for IPS events. This editor supports the latest functionality and provides flexibility in rule creation and sensor specific response configuration.
- **VPN wizard for Proventia M-Series appliances** – Creating VPN's and VPN Mesh's has been greatly simplified with the new wizards added for use with the Proventia M-Series appliances.
- **Desktop Controller Renamed to Agent Manager** – The Desktop Controller has been enhanced and the name was changed to Agent Manager to reflect that SiteProtector Components (such as the X-Press Update Server) and appliances also communicate using the Agent Manager and it is not just the desktops.
- **New X-Press Update Server Component** – A new component was added to facilitate the updating process for agents throughout the SiteProtector infrastructure. This component downloads the latest updates from ISS and disperses them throughout your enterprise independent of other process providing flexibility and scalability. The Update Server requires the use of an Agent Manager component to communicate to SiteProtector.
- **New Analysis columns** – Seven new columns have been added to the analysis tab to facilitate better analysis for Proventia appliances and Desktop. The new columns are: Sensor NetBIOS Name, Source NetBIOS name, Target NetBIOS name, User count, User Name, Virtual Sensor Name, VLAN
- **New Analysis views** – New default analysis views have been added for the inclusion of Application monitoring functionality added in Proventia Desktop.
- **Event loading process enhancements** – The event loading process has been modified to provide greater scalability and removes the previous limit of five (5) event collectors and increases it to 255. This does change the database structure associated with events, therefore any custom processes that directly access the event data from the database should be reviewed the new structure prior to upgrading to SP5.
- **New Database Maintenance functions** – New event purging options have been added for cleared events and audit trail data. Also an option for daily purging has been added which allows purging and other maintenance items to be done on a daily basis rather than a weekly basis.
- **New Reports** – There are five (5) .new reports added in SP5. Reports include Audit detail, Content Filtering Report (Top Web Categories and Web Requests), Assessment Reports (Operating Summary, and Vulnerability Counts)

2. What is different about the Sp5 upgrade from SP upgrades in the past?

There are a few architectural changes which have an effect on the upgrading process. There are database schema changes which could affect customized processes which extract data from the database. There are event loading changes which require the event collectors to be upgraded prior to applying Service Pack 5. The X-Press Update Server will be installed by default on the application server and will require an Agent Manager to be managed. If there is not a desktop controller currently in the SP4 instance of SiteProtector it will be necessary to add an Agent Manager to the SiteProtector SP5 instance after the upgrade from Sp4.

3. What Database Schema changes have been made which effect custom event extraction?

If you use a third party product or a custom extraction process to pull events out of the SiteProtector Database there have been some changes made to the event tables which may affect this process. Prior to SP5 in the SensorData table the SensorDataID field was sequential. This field is often used to determine what events have been extracted and which ones have not. In SP5 a new field has been added that is sequential called the RowID. The SensorDataID is no longer guaranteed to be sequential if you have more than one Event Collector. There were other minor changes which may effect a custom process therefore

validate how these changes could effect your database prior to upgrading if you use custom or third party tools to interoperate with the SiteProtector Database.

4. What changes are being made to the event loading process?

Prior to SP5 the events were loaded into a single database table for all event collectors. In SP5 the process has been changed so that the Event Collector components place detailed event data into their own tables directly. For each Event Collector in the site you will see a detail event data table. If there are customized processes that you have developed to pull event data from the single tables prior to SP5 then these procedures will have to be changed to access events from the multiple new detail event tables. For more details on specific changes contact your sales representative for more information.

5. What actions are being audited in the new User Auditing functionality?

The following actions are being audited in service pack 5.

- Sensor Controller Started
- Sensor Controller Stopped
- Application Server Started
- Application Server Stopped
- Console User Login
- Console User Logout
- Site created
- Site updated
- Site deleted
- Group created
- Group updated
- Group deleted
- Group policy updated
- Group rules added
- Group rules updated
- Group rules deleted
- Group host added
- Group host deleted
- Group tree deleted
- Sensor added
- Sensor deleted
- Sensor started
- Sensor stopped
- Sensor paused
- Sensor resumed
- Sensor property changed
- Sensor response file changed
- Sensor policy changed
- Sensor XPU installed
- Sensor XPU uninstalled
- Sensor has error (such as license expire, communications error)
- Database auto maintenance updated
- User group permissions updated
- Scan command issued
- Policy updated
- Policy deleted
- License added
- License deleted

6. What is the Agent Manager?

The Agent Manager component collects events and heartbeats from the agents and sends down policy updates to agents. Historically agents reported events to the EC and received their policies, security content and product upgrades from the application server. In the future agents will begin reporting events and getting their policies from Agent Managers and content and product updates through the X-Press Update Server

As of SiteProtector 2.0 SP5 the following is effective:

Agents or components that report events and receive their policy via an Agent Manager:

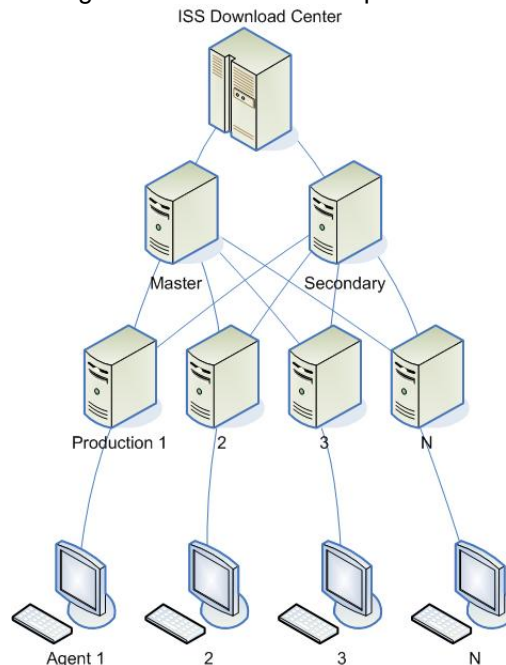
- RealSecure Desktop Protector
- Proventia Desktop
- Proventia M Series Appliances
- Proventia G2000, G400 Appliances
- X-Press Update Server

Agents that receive content or product updates from an Agent Manager

- RealSecure Desktop Protector
- Proventia Desktop

7. How does the X-Press Update Server work?

The X-Press Update server mirrors the ISS download center. Agents are configured through group settings to heartbeat up to an X-Press Update Server (XP-US) to determine if there are any available updates for the agent. If new security content or upgrades for the agent are available the XP-US it will check to see if it has already downloaded the update to send to the agent. If not it will request the update from either the download center or another XP-US. Because XP-US can request updates from other XP-US it is possible to have multiple XP-US requesting updates from one central XP-US which in turn requests updates from the ISS Download Center. See the diagram below for an example.



About Internet Security Systems (ISS)

Internet Security Systems, Inc. (ISS) is the trusted expert to global enterprises and world governments providing products and services that protect against Internet threats. An established world leader in security since 1994, ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise for more than 11,000 customers worldwide. ISS products

and services are based on the proactive security intelligence conducted by ISS' X-Force™ research and development team – the unequivocal world authority in vulnerability and threat research. Headquartered in Atlanta, Internet Security Systems has additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at www.iss.net or call 800-776-2362.

Copyright © [2003 -2004], Internet Security Systems, Inc. All rights reserved worldwide.

Internet Security Systems, the Internet Security Systems logo, Proventia, System Scanner, Wireless Scanner, SiteProtector, ADDME, AlertCon, ActiveAlert, FireCell, FlexCheck, SecurePartner, SecureU, X-Force, Virtual Patch, and X-Press Update are trademarks, and Secure Steps, SAFEsuite, RealSecure, Internet Scanner, Database Scanner and Online Scanner registered trademarks and service marks, of Internet Security Systems, Inc. Network ICE, the Network ICE logo and ICEpac are trademarks, BlackICE a licensed trademark, and ICEcap a registered trademark, of Network ICE Corporation, a wholly owned subsidiary of Internet Security Systems, Inc. Other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.