ManageEngine

Security Manager Plus

User Guide

Network Security Scanner with Patch Management

support@securitymanagerplus.com

AdventNet
Excellence Matters

Table Of Contents

Introduction

With increasingly sophisticated attacks on the rise, the ability to quickly mitigate network vulnerabilities is imperative. Vulnerabilities if left undetected pose a serious security threat to enterprise systems and can leave vital corporate data exposed to attacks by malicious hackers. Fororganizations, it means extended system downtimes and huge loss of revenue and productivity.

The goal of a vulnerability management system is to identify such security holes in your network infrastructure and remediate them before they are exploited. Vulnerability management systems, or vulnerability scanners as they are popularly known, help you in performing the following tasks:

- Cataloging network assets or resources through network discovery.
- Assessing the network health by scanning the discovered assets for vulnerabilities.
- Identifying the vulnerabilities or potential threats to each resource.
- Categorizing the risk level based on vulnerability severity.
- Providing remediation solutions to mitigate the risks.
- Regularly updating itself to keep track of the latest vulnerability signature.

Security Manager Plus is a web-based, enterprise vulnerability management software that proactively reports on network vulnerabilities and helps to remediate them and ensure compliance. Its open ports detection, vulnerability scanning and patch management capabilities protect your network from security threats and malicious attacks.

Security Manager Plus Features

- Completely web-based enterprise vulnerability scanner
- Accurate, fast, non-intrusive and customizable discovery and scanning.
- Advanced scheduling and scan automation capabilities.
- Intelligent scan completion notification.
- Remediation for Windows systems by deploying missing patches and service packs
- PCI DSS Compliance Reporting
- Windows Change Detection & Baselining
- Frequently updated, comprehensive vulnerability database.
- Comprehensive reports to capture the health of your enterprise network
- Vulnerability management over the internet
- Template based report customization.
- CVE cross-references.
- Trouble ticket mail generation.
- Cross platform product installation.
- Secure architecture

Supported Systems and Services

Some of the many systems and services vulnerabilities that Security Manager Plus assesses are as follows .

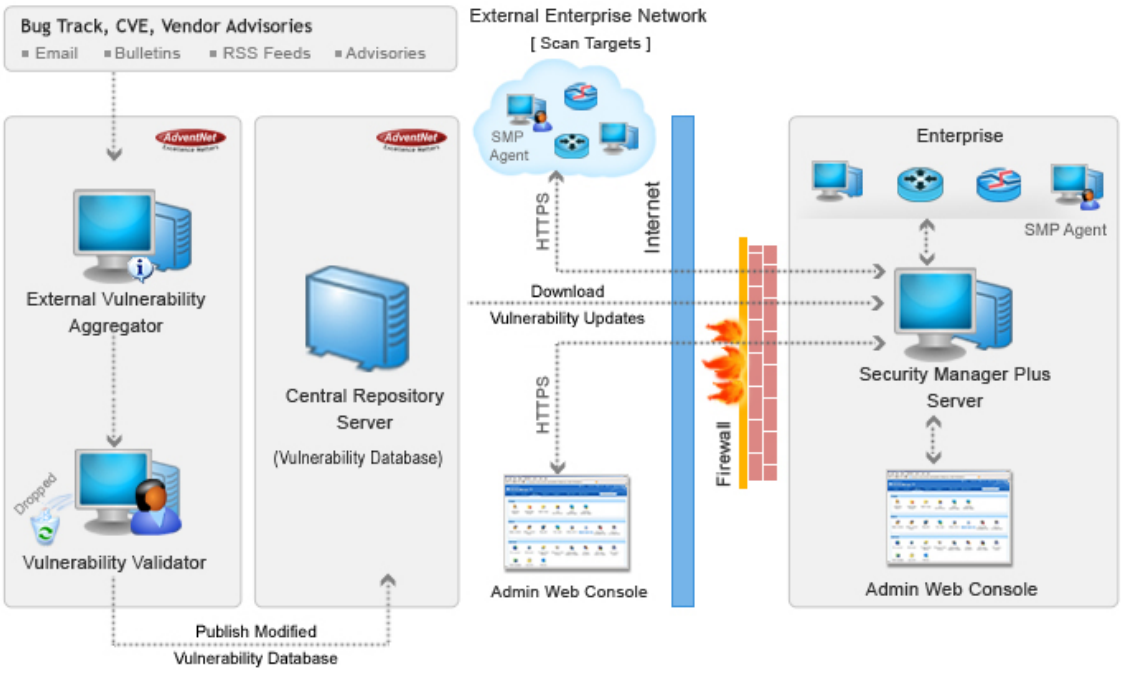
• Web Servers • Database Servers • Application Servers • RPC Services • CGI Scripts • FTP • DNS • POP3 • SNMP	• SMTP • IMAP • SSH • SSL • Proxy Servers • UDP • TCP/IP • Registry	• User Accounts • Dos Vulnerabilities • SQL Injection vulnerabilities • Trojans and Viruses • Switches • Routers • Windows • Linux • VPNs and many more...

About Security Manager Plus

Security Manager Plus Architecture

To understand how Security Manager Plus functions, you will need to know about the various components in Security Manager Plus architecture. The primary components of Security Manager Plus (SMP) are :

- External Vulnerability Aggregator
- Central Repository Server
- Security Manager Plus Server
- Security Manager Plus Agents (optional)



External Vulnerability Aggregator

The External Vulnerability Aggregator resides at the AdventNet site and draws vulnerability information from various security advisories - mainly advisories from the CVE and SecurityFocus websites, bulletins from the Microsoft website, and other vendor specific advisories, through Email and RSS Feeds.

Vulnerability and Windows patch information consolidation,assessment for information authenticity and testing for functional correctness is also carried out by the Security Manager Plus Enterprise

Security Team. The final analysis and data are correlated to obtain a consolidated repository of vulnerability information - a vulnerability database, which serves as a baseline for vulnerability assessment in the enterprise (customer site). The modified vulnerability database is then published to the Central Repository Server for further use. The whole process of information gathering, vulnerability assessment, patch analysis and publishing the latest vulnerability database occurs periodically.

Central Repository Server

The Central Repository Server is a highly secure comprehensive database of all thoroughly analyzed vulnerability and patch information, residing at the AdventNet site. Any update to the Central Repository Server is automatically *recognized* by the Security Manager Plus server, situated at the customer site.

Security Manager Plus Server

Security Manager Plus Server is located at the enterprise (customer site) and subscribes to the Central Repository Server, to periodically download the vulnerability updates. It performs device discovery and assesses/scans the devices in the heterogeneous enterprise network and lists the open ports, vulnerabilities and missing patches, and generates reports to effectively manage the vulnerability assessment process in your enterprise. All these actions can be initiated from a universally accessible, web-console in a few simple clicks.

Security Manager Plus Agents

The Security Manager Plus Agent is a light-weight software that is installed in a target machine. It acts as a worker to carry out the management operations as instructed by the Security Manager Plus server. The agent-based mode of management is an option that you can adopt, based on your enterprise network infrastructure set-up and requirements. It is an optional component that can be employed in target machines that are locked down or behind a firewall (or) to manage systems in present in remote geographical locations where a dedicated network tunnel is not feasible.

How Security Manager Plus works

Vulnerability Assessment using Security Manager Plus can be broadly considered as a three step process.

Detect

Security Manager Plus discovers all assets on a given network, and provides detailed information, including operating system, IP address, DNS Name, Mac Address and IF Descriptor , of the discovered asset. IT Administrators are provided with a variety of options to customize the discovery of enterprise resources., like using TCP ping or ICMP ping for host discovery, Nmap or SNMP for OS detection.

Once the network resources have been discovered scan is performed on open ports for identifying which services or applications are listening in these ports. On identifying the service, tests are run to identify the service specific vulnerabilities and Windows specific missing patches. When a scan is complete, vulnerabilities are displayed in a color-coded list that indicates the severity of each potential problem.

Report

Reports can be generated automatically from Security Manager Plus web-console in HTML formats and exported to PDF/CSV formats and even can be e-mailed to any number of recipients in PDF/CSV formats. Customization is simple as Security Manager Plus provides report customization templates, whereby report sections can be added, removed or re-ordered. The amount of technical detail can be adjusted, allowing reports to be tailored for any target audience.

Not only are Security Manager Plus reports flexible, but they also provide the required vulnerability information efficiently in color-coded and graphical format.

Remediate

Remediating vulnerabilities comprises of many aspects like notifying IT personnel so that they can fix them, effecting configuration changes in systems, routers or firewalls, deploying missing patches and service packs in desktops and servers etc.

Security Manager Plus offers two forms of remediation :

1. **Patch Deployment :** Once the missing patches are detected for Windows systems, Security Manager Plus allows you to install the missing patches and service packs in these systems, thereby remediating all such vulnerabilities for software products from Microsoft that have patches released by the vendor.

2. **Trouble-ticket system integration :** Vulnerability reports contain information to quickly understand what the problem is and provide supporting evidence that the system is vulnerable. You can generate trouble tickets from the Security Manager Plus generated vulnerability notification mails provided you have a Helpdesk system, like ManageEngine™ ServiceDesk Plus, in your enterprise which recognizes notification mails generated by Security Manager Plus and converts them to trouble tickets. URL links to vendor advisories and downloadable patches make remediation straightforward.

Release Notes

Build 5100

New Features

- Linux patching support - Provision to deploy updates for Linux distributions, with out-of-the-box support for Red Hat, CentOS and Debian. Support for other Linux distributions can be added by editing patch management scripts from the web console.
- Windows Change Management - Provision to track changes in Windows files, folders and registry settings & to compare against a set baseline.
- Patching support for Windows x-64 bit systems. Patches released from year 2008 are supported.

Bug Fixes

- When an asset being managed by an SMP Agent was deleted from the web console, the SMP Agent shutdown automatically. This has been fixed.
- In Hardware inventory, there was an error displaying the keyboards, when 2 keyboards were detected on an asset. This has been resolved to identify and display only one primary keyboard device.
- While configuring MS Office media path for MS Office patches deployment, there was no provision to supply a hidden share ($ at the end of Windows path). This has been fixed and $ paths can now be specified.

Build 5010

New Features

- PCI DSS Compliance Reports - Security Manager Plus can help corporate networks adhere to PCI DSS, by assessing many key requirements of the PCI DSS and furnishing compliance reports.
- Latest NMap (version: 4.22SOC7) integrated in this build

Bug Fixes

- There were some junk characters being sent in the SMP Agent's response for a task, to the SMP server, which caused the task execution to fail. This has been fixed.
- A gradual overflow in the PageFaults parameter for the SMP Agent process was noticed. This has been addressed.
- The trouble ticket e-mail address field in the SMP web interface did not support certain e-mail address formats. Validation checks for this have been handled properly now.

Installation and Setup

System Requirements

Minimum system requirement for Security Manager Plus

Hardware	Operating Systems	Web-Client
Processor 1.8 GHz Pentium® processor **RAM** 512 MB **Hard Disk*** 200 MB for product 10 GB for database	• Windows Vista (Business & Ultimate) • Windows Server 2003 • Windows XP Professional • Windows 2000 Server/Professional • Red Hat Linux 7.2 • Red Hat Linux 8.0 • Red Hat Linux Advanced Server 3.0 • Red Hat Enterprise Server 3.0 • Debian GNU/Linux 3.0 (Woody)	HTML client requires one of the following browsers** to be installed in the system: • IE 6.0 and above (on Windows) • Firefox 2.0 and above (on Windows and Linux) Security Manager Plus is optimized for 1024 x 768 resolution and above.

The system in which Security Manager Plus server is installed should have access to the Internet, with minimum connection speed of 56 kbps.

***** - Hard Disk space requirement is dependent on the number of scans stored in the Security Manager Plus server.
****** - Browsers must have JavaScript and Cookies enabled.

Prerequisites

Prior to installing and starting Security Manager Plus in your enterprise, ensure that the following are taken care of :

Ports Used

1. The web server port of Security Manager Plus server for HTTP access (Standard Mode), by default, is **6262**.
2. The web server port of Security Manager Plus server for HTTPS access (Secured Mode), by default, is **6767**.

If these ports are occupied, you can alter them in the **server.xml** file located in the <*Security Manager Plus_Install_Dir>/conf* directory.

3. The MySQL database server port is **33300**. If this port is occupied, you can alter it in the **database_params.conf** file located in the <*Security Manager Plus_Install_Dir>/conf* directory.

4. The Security Manager Plus Server listener port is **9004** by default. It is used for server to agent communication only. The Security Manager Plus Agent communicates to the server through this port number.

If this port is occupied, the server will not start up. This port can be altered from the **ports.properties** file located in the <*Security Manager Plus_Install_Dir>/conf* directory.

Internet Connection

An internet connection, with a minimum speed of 56 kbps, should be available in the machine running the Security Manager Plus server. This is to ensure that you receive updates of the latest vulnerabilities added to our Central Repository Server (CRS), hosted at our AdventNet site.

If you are using a proxy server to connect to the Internet then the Security Manager Plus proxy settings have to be configured in Security Manager Plus server without fail during first login.

Machine access rights

- If you install Security Manager Plus in a Windows system, ensure that the system is in the Windows domain of your enterprise.
- Administrator rights for target Windows machines is to be made available for Security Manager Plus server to remotely login to target Windows machines and execute vulnerability assessment tasks involving registry checks and detecting missing patches.

NMap Configuration for Security Manager Plus server running in Linux systems

In Linux systems, for Security Manager Plus server to use NMap OS detection, proper privileges need to given to the NMap executable, before starting the Security Manager Plus server.

In order to do so, please execute the script file **nmaposdetect.sh** located in <*Security Manager Plus_Install_Dir>/scripts* directory in "superuser mode".

Recommended Additional Software

- ### Samba-Tng

  If you intend to run the Security Manager Plus server in Linux OS, ensure that Samba-TNG software (version 0.4.99 and above) is installed. This software facilitates communication between the Linux server and target Windows machines. Useful while identifying missing patches in target Windows machine (**only in agentless mode**).

  You can download the software from : http://download.samba-tng.org/tng/0.4.99/ .

  For more information on Samba-TNG, refer to : http://www.samba-tng.org .

  Note: Please ensure that SAMBA_HOME environment variable is pointing to the Samba TNG Home directory.

Server Installation

Installing Security Manager Plus Server on Windows

The Windows edition of Security Manager Plus is available as an executable file. (.exe). Download the **ManageEngine_SecurityManagerPlus.exe** on the system you want to install Security Manager Plus, execute the file and follow the instructions as they appear on screen. Security Manager Plus will be installed as a Windows service from the installer.

Important Note : Ensure that you have 'administrator' privileges before you proceed with the installation.

Security Manager Plus server startup and shutdown will cover on starting and stopping the Security Manager Plus server.

Installing Security Manager Plus Server on Linux

The Linux edition of Security Manager Plus is available as a zip file (.zip) - **ManageEngine_SecurityManagerPlus.zip** . Steps for installing Security Manager Plus are as follows.

- Download the **ManageEngine_SecurityManagerPlus.zip** to the machine where you will run the Security Manager Plus server
- Create an installation directory (if necessary) and move the zip file to the installation directory
- Unzip the file in the installation directory, which will create a directory named '*AdventNet*' in the installation directory. Here onwards we will refer to the *<installation directory>/AdventNet/SecurityManagerPlus* as ***<Security Manager Plus_Home>***

Security Manager Plus can be installed as a service (daemon) in Linux as well. For server startup and shutdown refer here.

Note : For details on recommended additional software installation, refer here .

Uninstalling Security Manager Plus

Windows

For uninstalling Security Manager Plus from a Windows system, first ensure that the Security Manager Plus server is no longer running. Then click on : Start Menu --> Programs --> ManageEngine Security Manager Plus 5 --> Uninstall Security Manager Plus

Linux

For uninstalling Security Manager Plus from a Linux system, you just need to remove the Security Manager Plus directory.

Note : Uninstalling Security Manager Plus does not uninstall the recommended additional software. Please follow the instructions mentioned in the corresponding websites to uninstall these additional software.

Agent Installation

Windows systems can be managed using an agent, as an option. The Security Manager Plus Agent edition is available as an executable file (.exe) in the Security Manager Plus Server installation. Once the Security Manager Plus Server is installed, copy the Security Manager Plus agent executable from the location : *<Server_Install_Dir>/AdventNet/SecurityManager/agent/windows* to the target machine. Execute the file and follow the instructions as they appear on screen.

Please ensure that you have 'administrator' privileges before you proceed with the installation.

Security Manager Plus 5 is powered with an agent which can function in either HTTPS mode or SSL/TCP mode. You can choose your desired mode of installation based on the scenario in which your systems are going to be managed.

Refer to the following sections of the help documentation to know more about installing and working with the agents in each of these modes.

S.No		Security Manager Plus Agent in HTTPS Mode	Security Manager Plus Agent in TCP Mode
1	Usage scenario	To manage systems in remote locations without a dedicated network connection (over internet), systems in the LAN, laptops that are often disconnected from the network	To manage systems in the LAN, systems with restricted access, systems accessible over a VPN tunnel
2	Communication protocol	HTTP (Over the web)	Port to port (TCP)
3	Security	Data encrypted. Communication secured using SSL over HTTP (HTTPS)	Data encrypted. Communication secured using SSL over TCP.
4	Ports to be open for the Agent in the firewall (if any)	None. Web access (HTTP) must be allowed.	9001 (default, but configurable)
5	Ports to be open for the Server in the firewall (if any)	8443 (PQ server web port - default, but configurable)	9000 (default, but configurable)
6	PQ Server location	Can be located in an internal network with IP & port mapping done to the NAT's external IP address	Located in the internal network
7	Agent Configurations required	External IP address of the PQ Server, PQ server web port & proxy server info (if required), polling interval for agent	Name/IP address of the PQ Server, PQ Server TCP port
8	Communication Flow between Server and Agents	One-way (Agent polls Server)	Two-way
9	Response time of Agent	At every agent poll interval	Instant (no polling!)
10	Operating System supported	Windows only	Windows & Linux

Note : After the installation is complete, the agent **starts** as a Windows service automatically. To simply install the agent but start it up at a a later point, un-check the "Yes, I want to start the agent service" option. Refer to the ReadMe file in the agent installation for more information.

Downloading from the web-client and installing

You can connect to the Security Manager Plus server using a browser from the machine you want the agent to be installed. Select the '**Download Windows Agent**' link option from the '**Admin**' tab. Once the download is complete, proceed with the installation.

Agent in HTTPS Mode

HTTPS Mode Overview

HTTPS mode of agent installation is suitable to manage

- systems that are spread across different geographical locations or offices over the internet,
- laptops that are often disconnected from the network
- systems situated behind a NAT/PAT firewall or router

This mode is helpful in cases where maintaining a dedicated network tunnel is not feasible; therefore allowing the communication over the internet.

Note : The most important prerequisite is that the Security Manager Plus(SMP) agents should be able to contact the Security Manager Plus server over HTTP.

The Security Manager Plus Server needs to be running on a system exposed to the internet (with an IP that is accessible by the external world). The web server port of Security Manager Plus (default:6767) needs to opened up to allow HTTP traffic to the server from the Security Manager Plus Agent. A management task (scan, patch deployment, agent configuration) will be initiated in the server via the web interface. The agent will check-in (poll) periodically to the Security Manager Plus Server (over the internet over HTTP secured using SSL), authenticate itself and fetch the tasks. The tasks will be executed and the response will be submitted to the server at the next check-in interval (default: 5 minutes).

This apparently means that it is the 'SMP Agent', that always communicates with the SMP Server (one-way) using HTTP protocol over the web. It either submits responses to previous tasks or fetches new tasks to execute. The SMP Server is just a provider in this case. This implies that the agent machine should be allowed web access. If a proxy server is required to access the internet for the agent machine, it can be configured during agent installation or from the agent system tray icon.

Note : The HTTPS Agent can also be used in the LAN! But the TCP agent cannot be used over the internet.

Enterprise Setup

Consider a scenario where a Service Provider say SerPro in Washington, has a requirement to manage systems for 3 of his enterprise clients - AXZ Car wash in California, BNF Bank in Texas, Colt Freightliners in New York, who situated in different locations in the USA. These 3 networks are in no way interconnected and neither are they accessible by the SerPro network.

The Security Manager Plus Server will reside in the SerPro network in Washington. The Security Manager Plus Agents (in HTTPS mode) will be deployed in the systems in these 3 client networks spread across the US. The agents will contact the Security Manager Plus Server over the internet and fetch management tasks that need to be performed. On task completion they will report back periodically to the Security Manager Plus Server with the status update. Thus the systems in these independent enterprise networks will be managed by a single console with just internet accessibility.

Setting Up Security Manager Plus Server in the Service Provider Network

1. On a system which is in the Internet Data Center (IDC), with a public IP address

Security Manager Plus Server can be installed on a server in the IDC of the service provider. This server must have a unique public IP address and must be accessible over the web. Port 8843 (default web server port of Security Manager Plus server) must be open allow Security Manager Plus agents to communicate to this server.

Administrators can login to the web interface of Security Manager Plus either from the SerPro data center, SerPro internal network or from anywhere else if web access is allowed.

2. On a system in the internal network of the service provider, with internet access with a NAT/PAT router

Security Manager Plus can be installed on a system with an internal IP address, within the SerPro network. The NAT router in the service provider IDC will have the public IP address for external internet traffic, and this will redirect all traffic to and from the internal IP addresses. The NAT router must be configured (mapping in the routing table) in such a way that it routes all HTTP (web) traffic coming through port 6767 (default web server port of Security Manager Plus server) to the internal IP address of the system which has Security Manager Plus Server installed.

The SMP agents will have the **external IP** of the SerPro NAT router configured as the **SMP Server name** and will establish contact over the web on port 6767 (default). The NAT router at SerPro will take care of redirecting the requests/responses to the internal IP address of the SMP Server machine

Setting Up Security Manager Plus Agents at the customer sites

This process is very much simple and does not involve any major configurations at the customer sites.

- Access the web interface of the SMP Server in SerPro using the public IP address : https://<publicIP>:6767/
- Login and download the SMP Agents (Windows) from the Home tab
- Copy and install the SMP Agents on systems that need to be managed
- Provide the public IP address of the SMP server machine as Server Name to the agent during installation
- If web access from the SMP Agent machine happens via a proxy server, this can be configured during installation or later from the System Tray Icon of SMP Agent

- Start the agent at the end of the installation screen
- Login to the web interface of SMP, visit the Assets tab and see your agents listed there

Note : If the customer site cannot access the SMP server web interface, you can copy the SMP Agent installable on to the customer network by some other means, and proceed with the installation.

Installation

The SMP agent is available as an executable file (SecurityManagerPlusAgent.exe) in the <Server_Install_Dir>/AdventNet/SecurityManager/agent/windows directory of the Security Manager Plus Server. Copy the agent to your target machines, execute the file and follow the instructions. Choose HTTPS mode when prompted for during the installation.

Alternatively, you can connect to the Security Manager Plus Server from a browser in the target machine, using the URL : https://server_name:portnumber. (e.g. https://localhost:6767). Login and visit the 'Admin' tab.

Use the '**Download Windows Agent**' link from **Admin** tab, to download and install the Security Manager Plus agent (.exe file) in that particular system. Carry out the same step for the desired number of target machines. Choose HTTPS mode when prompted for during the installation.

Agent Configurations for HTTPS Mode

There are some parameters that need to be configured for this mode. These configurations are effected in any of the following ways:

- During Agent Installation
- By editing two config files - **agent.ini** & **server.ini** in the agent installation
- From the web interface of Security Manager Plus --> Admin tab --> Agent Administration link for the agent system listed

Here are the parameters :

- Mode: Property to be changed in **agent.ini** & **server.ini** file: **transport=https**
- Polling Interval (jn minutes) : Default 5 minutes. The time interval in which the agent polls the SMP server for tasks to be executed. Property in **agent.ini** file: **pollinterval**
- Server Name: The System Name or IP address of the Security Manager Plus server machine to which agent communicates. Property in **server.ini** file: **server**
- Security Manager Plus Server Web Port: Default 6767. The web port on which the SMP server communicates to the agent. Note that the SMP server now runs in the HTTPS mode. Property in **server.ini** file: **webport**

  Do not alter Server Port value unless and until this has been changed accordingly during Security Manager Plus Server installation.

- Proxy Configurations - Proxy server name, port, username & password can be provided if the agent requires to access the internet via a proxy. This can be configured from the Security Manager Plus Agent System Tray Icon as well at any point after installation.

Agent in TCP Mode

TCP Mode Overview

TCP mode of agent installation is suitable to manage systems that are in a LAN or for those systems that can be communicated to, by the Security Manager Plus (SMP) server over a secure VPN tunnel.

The two-way communication between the Security Manager Plus server and the agent is via a TCP connection (port to port). The agent will have a TCP port (default:9005) open in the system and talk to the server on its own TCP port (default port:9004). Data is encrypted and the communication is secured using SSL. Vulnerability management tasks are initiated from the web interface of Security Manager Plus. The SMP Server contacts the agent and assigns the tasks. SMP Agent will perform the tasks on the system and send the response back to the server on the same connection.

Enterprise Setup

Consider a scenario within an enterprise network where a few systems are "highly" secured or present in a DMZ (De-Militarized Zone) - wherein remote access is not permitted, ADMIN$ shares are disabled, remote registry service is disabled or systems have a firewall enabled which blocks external access. It becomes practically impossible to manage such systems in the remote or agentless mode as they cannot be easily contacted by the Security Manager Plus Server. In such cases, installing Security Manager Plus Agents on these systems and enabling TCP port 9005 in the firewall for access by the Server will making patch management permissible.

Setting up Security Manager Plus Server in the enterprise

The Security Manager Plus Server will be installed on a high-end machine in the internal network / server data center. TCP port 9004 must be open in this machine for SMP Agents to communicate to the Server over TCP.

Administrators can login to the web interface of Security Manager Plus either from the server data center or enterprise internal network.

Setting Up Security Manager Plus Agents in the enterprise network machines

- Access the web interface of the SMP Server as : https://<server-name>:6767/
- Login and download the SMP Agents from the **Admin** tab --> **Download Windows Agent** link
- Copy and install the SMP Agents on systems that need to be managed
- During the installation, configure the agent's TCP port (default 9005)
- Provide the name or IP address of the SMP server machine as Server Name to the agent during installation

- Change the Server TCP port (default:9004) if and only if this value has been changed during Server installation.
- Start the agent at the end of the installation screen
- Login to the web interface of SMP, visit the Assets tab and see your agents listed there
- Carry out vulnerability management operations on the agents from the web interfaces

Installation

The SMP agent is available as an executable file (SecurityManagerPlusAgent.exe) in the <Server_Install_Dir>/AdventNet/SecurityManager/agent/windows directory of the Security Manager Plus Server. Copy the agent to your target machines, execute the file and follow the instructions. Choose TCP mode when prompted for during the installation.

Alternatively, you can connect to the Security Manager Plus Server from a browser in the target machine, using the URL : https://server_name:portnumber. (e.g. https://localhost:6767). Login and visit the 'Admin' tab.

Use the '**Download Windows Agent**' link from **Admin** tab, to download and install the Security Manager Plus agent (.exe file) in that particular system. Carry out the same step for the desired number of target machines. Choose TCP mode when prompted for during the installation.

Agent Configurations for TCP Mode

There are some parameters that need to be configured for this mode. These are configurations are effected in any of the following ways:

- During Agent Installation
- By editing two config files - **agent.ini** & **server.ini** in the agent installation, if required at a later point
- From the web interface of Security Manager Plus --> Admin tab --> Agent Administration link for the agent system listed

Here are the parameters :

- Mode: Property to be changed in **agent.ini** & **server.ini** file: **transport=ssl**
- Agent Port : Default is 9005. This is the port on the agent machine through which the SMP agent communicates with the Security Manager Plus Server. Property in **agent.ini** file: **requestport**
- Server Name : The System Name or IP address of the Security Manager Plus server machine to which agent communicates. Property in **server.ini** file: **server**
- Server Port : Default is 9004. The TCP port on which the SMP server communicates to the agent. Property in **server.ini** file: **sslport**

  Do not alter Server Port value unless and until this has been changed accordingly during Security Manager Plus Server installation.

Getting Started

Security Manager Plus Server Startup and Shutdown

As has been already mentioned in Security Manager Plus server installation , Security Manager Plus product comes as an executable (.exe) file for Windows and as a zip file for Linux. Below you will find instructions for starting or stopping the Security Manager Plus server in Windows and Linux .

Security Manager Plus Server Startup and Shutdown in Windows

You can use either of the following approaches for Security Manager Plus server startup and shutdown in Windows.

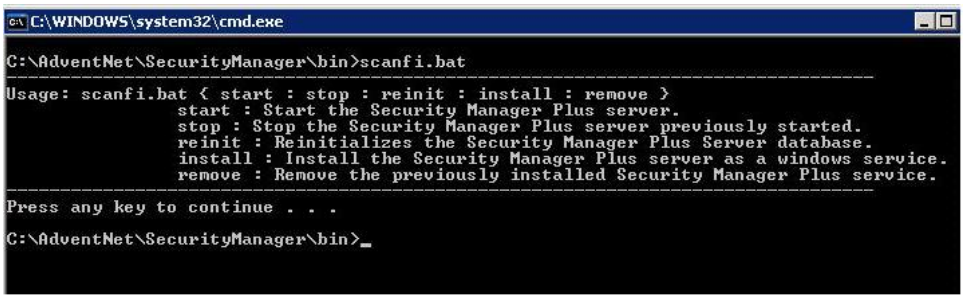
- **using System Tray Icon menu (or) Programs menu options (Recommended)**
    1. The Security Manager Plus Windows installation wizard will automatically install and start the Security Manager Plus System Tray Icon.
    2. Right click on the Security Manager Plus Tray Icon to see the following menu actions, and start Security Manager Plus :
        - **Start Service** - to start Security Manager Plus in service mode. This is the default and **recommended** mode of starting Security Manager Plus. This option will appear when Security Manager Plus is not running
        - **Stop Service** - to stop the Security Manager Plus service. This option is enabled when Security Manager Plus is running
        - **Security Manager Plus WebConsole** - to start the web interface of Security Manager Plus. This option will appear only when Security Manager Plus is running.
        - **Show Startup Logs** - Log file located in the ***<Security Manager Plus_Home>/logs/wrapper.log***. This log filewill keep track of activities related to Security Manager Plus service startup and shutdown.
        - **StartUp Options**
            - Load this tray icon on Windows Startup - Launch the Security Manager Plus tray icon when the machine is started or rebooted. This option is checked by default
            - Start Web Console on Service Startup - Open the web interface of Security Manager Plus immediately after Security Manager Plus starts up. This option is checked by default
            - Show Splash Screen on Service Startup - Launch the Splash Screen which indicates startup progress, every time Security Manager Plus is started. This option is checked by default

Note : A status message is displayed in a balloon on the Tray Icon whenever Security Manager Plus is started or stopped from there.

3. The Security Manager Plus Windows installation wizard will also activate Security Manager Plus menu options from Windows Start Menu (**Start >> Programs >> ManageEngine Security Manager Plus 5**).
4. The various menu options provided for Security Manager Plus and their actions are listed below :
    - **Start Security Manager Plus Service -** to start Security Manager Plus (will start in Windows Service mode)
    - **Stop Security Manager Plus Service -** to stop / shutdown Security Manager Plus (will shutdown Security Manager Plus Service)
    - **Security Manager Plus Web Console** - to start the web interface of Security Manager Plus
    - **Uninstall Security Manager Plus -** to uninstall Security Manager Plus from your machine.
    - **Show Tray Icon -** to enable Security Manager Plus system tray icon.
    - **Update Manager -** used for installing patches or service pack. This menu item is available only in Windows Start Menu (**Start >> Programs >> ManageEngine Security Manager Plus 5**).
    - **Help** - User Guide for the Security Manager Plus product

[or]

- **using command line interface (CLI)**
    1. Open a command prompt from ***<Security Manager Plus_Home>\bin*** directory.
    2. Type ***Security Manager Plus*** .
    3. A listing of Security Manager Plus usage commands will be displayed



    4. To start the Security Manager Plus server, type the command ***scanfi start***
    5. A Splash Screen appears indicating the progress of the start-up
    6. Please wait for all the server process to get started, and once you see the message "**Please connect your browser to http://localhost:6262/** " the Security Manager Plus Web Client will open up in your default browser.
       To shutdown the Security Manager Plus server, open another command prompt from ***<Security Manager Plus_Home>\bin*** directory and type the command ***scanfi stop***

7. The command ***scanfi reinit*** should be used to reinitialize the Security Manager Plus MySQL database, whereby all the tables which where created on server startup will be **dropped** (i.e.. will be removed).
8. The command ***scanfi install*** will install Security Manager Plus as a service, (*Control Panel >> Administrative Tools >> Services*) you will receive a command line confirmation message "*wrapper | Security Manager Plus installed*" , whereon you can start and stop the Security Manager Plus server from Windows ***Control Panel >> Administrative Tools >> Services >> ManageEngine Security Manager Plus***
9. The command ***scanfi remove*** will remove Security Manager Plus from Windows service (*Control Panel >> Administrative Tools >> Services*), you will receive a command line confirmation message "*wrapper | Security Manager Plus removed*".
10. To uninstall Security Manager Plus from your machine you just need to delete the Security Manager Plus installation directory, ***<Security Manager Plus_Home>*** .

Note : For installing patches or service pack for Security Manager Plus product, you can use of the **UpdateManager.bat** file, present in ***<Security Manager Plus_Home>\bin*** directory.

Security Manager Plus Server Startup and Shutdown in Linux

1. Goto ***<Security Manager Plus_Home>/bin*** directory.
2. Type **sh *SecurityManager.sh*** .
3. A listing of Security Manager Plus usage commands will be displayed

4. To start the Security Manager Plus server, type the command ***sh SecurityManager.sh start***
5. Please wait for all the server process to get started, and once you see the message "**Please connect your browser to http://localhost:6262/** " in the CLI, now you can start the Security Manager Plus Web Client.
6. To shutdown the Security Manager Plus server , open another command prompt from ***<Security Manager Plus_Home>/bin*** directory and type the command ***sh SecurityManager.sh stop***
7. The command ***sh SecurityManager.sh reinit*** should be used to reinitialize the Security Manager Plus MySQL database, whereby all the tables which where created on server startup will be **dropped** (ie. will be removed).
8. The command ***sh SecurityManager.sh install*** will install Security Manager Plus as a service, (*/etc/rc.d/init.d/*) you will receive a confirmation message "*Security Manager Plus Service*

Installed Successfully ! " ,whereby you can use the various options - *console , start, stop, restart, status, dump* from */etc/rc.d/init.d/securitymanager-service [options]* .

9. The command ***sh SecurityManager.sh remove*** will remove Security Manager Plus from service (*/etc/rc.d/init.d/*), you will receive a confirmation message "*Security Manager Plus Service Removed Successfully !* ".
10. To uninstall Security Manager Plus from your machine you just need to delete the Security Manager Plus installation directory, ***<Security Manager Plus_Home>*** .

    Note : For installing Security Manager Plus as a service in Linux you need to have Super User privileges.

Running Security Manager Plus Server 'only' in Secure Mode

By default, the Security Manager Plus has its web server accessible via ports 6262 & 6767.

You can access the web interface of Security Manager Plus from a browser over HTTP by connecting to port 6262 (Standard Mode as http://localhost:6262) & over HTTPS connecting to port 6767, which is the Secure Mode as https://localhost:6767.

Now if you wish to run and access Security Manager Plus only in the Secure Mode (HTTPS access only), you can carry out the following steps :

- Traverse to **<Security Manager Plus_Install_Dir>/webapps/Security Manager Plus/WEB-INF/** directory
- Edit **web.xml** file
- Uncomment the following lines in this file as :

```
<!--user-data-constraint>
transport-guarantee>INTEGRAL</transport-guarantee>
</user-data-constraint-->
```

- Restart the Security Manager Plus server
- Security Manager Plus will now be accessible only in the Secure Mode from the login screen

Starting the Web Client

- On successful server start-up, open a browser window of your favorite browser (refer to System Requirements for the browsers supported).
- Connect to the URL **http://<Security Manager Plus ServerName>:port_number/**. (default web server port is 6262). e.g http://localhost:6262/
- You can also access the web interface using the secure https port 6767, using the URL: **https://<Security Manager Plus ServerName>:6767/**
- In this case, since the web-client connects to the Security Manager Plus server through a secure connection (**https**), your browser will pop-up a Security Alert which would require you to accept the **security certificate**. This is perfectly safe and necessary to access the Security Manager Plus web client.
- To know further about accessing Security Manager Plus web client , refer here.

Starting the Agent

Just after the Security Manager Plus agent is successfully installed, the default behavior is that it automatically starts up as a service in Windows machines.

In case you have not chosen this option during installation, you can start the agent using the options below :

On Windows

Starting Agent Service

You can run the agent as a service from either from **Start » Programs » ManageEngine Security Manager Plus Agent 5 » Control Agent » Start** or from the Service Applet (Service Name : Security Manager Plus Agent). A taskbar tray icon indicates that the SMP Agent service is running.

Stopping Agent Service

There are 2 ways to stop the SMP Agent service. Any **one** of them can be adopted :

- Click **Start » Programs » ManageEngine Security Manager Plus Agent 5 » Control Agent » Stop**
- Visit the Service Applet (Settings » Control Panel » Administrative Tools » Services) and stop the service : Security Manager Plus Agent)

Accessing the Web Interface

From the login screen that is displayed after you connect to the Security Manager Plus server, provide the username and password to access the user interface of Security Manager Plus. For first time users, both the username and password are **admin** by default, the password for 'admin' can be reset by using the **Change Login Password** option available in the '**Admin**' screen after logging in.

License Information

After you login to the user interface of Security Manager Plus, you can click on the 'License' link on the top of the screen to view the license information of the current Security Manager Plus server installation.

This screen will indicate the following information :

- what type of License (Free or Professional) that you are holding currently
- the product name
- the product version number
- number of days for license expiry

Upgrading the License

In order to upgrade the current license, you must obtain a **valid license file** from AdventNet. Browse for the file in your system and click the '**Upgrade**' button. Any invalid files will not be accepted.

Contact sales@adventnet.com for more information on Security Manager Plus Licensing terms and upgrade requirements.

Setting System Parameters

Setting System Parameters

Before you proceed with the vulnerability assessment & patching of your network resources, it is imperative that you effect certain configurations in the Security Manager Plus system so as to ensure smooth and efficient functioning. Some of them are as below :

- Setting Proxy
- Mail Server Settings
- Configuring Vulnerability Database

Setting Proxy

Internet access is essential to update the vulnerability database information from AdventNet site. In your enterprise network setup, you might need to go through a proxy server to access the internet. In this case, you can configure the username and password that is provided for internet access, from this screen : **Admin** tab **» Configure » Proxy Server**. This configuration is essential for the system in which the Security Manager Plus server is installed.

The different parameters to be configured are :

1. **HTTP Proxy Host** : Host name of the proxy server (eg: proxy-server)
2. **HTTP Proxy Port** : Port number at which the server is running (eg: 80)
3. **Username** to access the internet. This can be in the format : firstname.lastname@domain.com
4. **Password**

Specify values for these parameters and click '**Save**'. You can even test to see if a connection to the specified proxy server is established, by clicking on the '**Test**' button. You can also save the proxy settings and update the vulnerability knowledge base immediately from here, by selecting the 'Update Database' checkbox.

If you have not configured the above parameters correctly then the Security Manager Plus server will be unable to contact Central Repository Server, you will see the message "**Unable to contact Central Server**" posted in **Home** tab.

Removing proxy parameters

To remove the proxy configurations permanently from the system, click on the '**Remove**' button. This will mean that the Security Manager Plus server will not have access to the proxy server anymore, to connect to the internet.

Note: The 'Remove' button appears only after a configuration has been made.

Mail Settings

Mails can be sent to desired recipients to report completion of certain vulnerability assessment tasks like scheduled scanning of network resources for vulnerabilities, sending generated reports, sending feedback to Security Manager Plus technical support through Instant Feedback.

In order to enable this functionality, your enterprise's mail server parameters need to be configured in Security Manager Plus. You can access this configuration from : **Admin » Configure » Mail Server**

The parameters required for Mail Server Configuration are :

- **Server Name,** the SMTP (Simple Mail Transfer Protocol) server hostname/IP Address for the field
- **Port** (default port number : 25)
- Select the option **Requires Authentication** only if your mail server requires you to authenticate yourself, in which case you need to supply the **Username** and **Password**.
- **Sender E-Mail ID -** the email address provided will be the default from address which will be used while sending scan completed notification mails and sending vulnerability reports.

Setting the Trouble Ticket E-mail ID

Security Manager Plus can be configured to Generate Ticket on Scan Completion by sending mail to the supplied mail-id provided you have a Helpdesk system, like ManageEngine™ ServiceDesk Plus, in your enterprise which recognizes notification mails generated by Security Manager Plus and converts them to trouble tickets.

To configure the e-mail ID, visit the **Admin** tab **» Configure » Trouble Ticket Settings**. Specify the e-mail ID here and click the 'Save' button.

Vulnerability Database Configuration

What is Vulnerability Database ?

The vulnerability database is a baseline against which the enterprise network vulnerabilities, are determined. This database is collated by acquiring information from security bulletins/errata from many of the Internet's largest and most comprehensive databases for security exposures and vulnerabilities. This information is further thoroughly analyzed and filled-up with relevant information for vulnerability assessment.

The vulnerability database is finally published in the Central Repository Server (CRS), from where it is updated to the enterprise site on request from the Security Manager Plus web interface.

The database is periodically updated with latest information and placed in the CRS. Therefore, it is best advised to update the database periodically in order to be in sync with the latest vulnerability and patch related information.

What does the Vulnerability Database comprise of ?

The vulnerability database contains detailed information about publicly known security vulnerabilities and exposures , which are grouped under '**Vulnerability Knowledge Base**' and provides :

- risk based vulnerability prioritization.
- service based vulnerability classification.
- remediation solution URLs.
- common vulnerability exposure (CVE) IDs.
  CVE (Common Vulnerabilities and Exposures) is a list of common names for publicly known vulnerabilities and exposures. The CVE Editorial board determines which vulnerabilities or exposures are included in CVE, through open and collaborative discussions. If the CVE name starts with CAN (candidate), then it is under consideration for entry into CVE.

The Vulnerability Database also contain Windows Patch related information, which are grouped separately under '**Patches Knowledge Base**' and provides :

- severity of the missing patch
- a brief description of the patch
- Bulletin reference link
- the patch to install

When should it be updated ?

- The vulnerability database has to be updated as the first step, after starting the Security Manager Plus server and logging in to the web interface - using the update icon in the **Home** page --> **Security** snapshot tab --> **Latest Vulnerabilities** section.
- Subsequent update intervals can also be scheduled, from **Admin** tab **» Configure » Vulnerability Database Updates**.
- Also, when the CRS at AdventNet site has been updated , your Security Manager Plus **Home** page will indicate  **Vulnerability Updates Available.**

Updating the database immediately

From the web interface of Security Manager Plus, **Home** page --> **Security** snapshot tab --> **Latest Vulnerabilities** section, choose the update icon to update the database. Your Security Manager Plus **Home** page will indicate  **Vulnerability Database is Up-to-date** once the update is complete.

Alternatively, visit **Admin** tab **» Configure » Vulnerability Database Updates**. Click on the '**Update Now**' button to trigger immediate update of Security Manager Plus vulnerability database.

Scheduling Vulnerability Update

Visit the **Admin** tab **» Configure » Vulnerability Database Updates** for automatic scheduling for vulnerability updates.

Viewing Vulnerability Database

You can view the Vulnerability Database either from **Admin** tab **» Actions » Vulnerability Knowledge Base .**

Searching based on CVE ID

The Vulnerability Database can be searched based on CVE ID. In order to perform a CVE ID based search, perform the following steps :

- Visit the **Admin** tab
- Click on the **Vulnerability Knowledge Base** link from here
- From the **CVE ID** column in the Vulnerability Knowledge base table, click on the  icon to invoke the **Search** field
- Specify the CVE ID you would like to view the information for, in the text field provided and hit 'Enter' key
- The search results will display the vulnerability that is mapped to this CVE ID and the corresponding risk information and description
- By clicking on the Short Description link, you can view the details of this vulnerability and also find a link to the CVE article for the vulnerability

Viewing Patch Database

You can view the Patch Database either from **Admin** tab **» Configure » Patches Knowledge Base**

Working with Security Manager Plus

Overview

Security Manager Plus is a web-based vulnerability scanner and patch remediation software which scans your network for vulnerabilities and applies patches for Windows systems. Working with Security Manager Plus mainly involves a few simple steps, as outlined here.

- Discovery - involves addition of the assets / resources present in your enterprise (the servers, workstations, laptops, routers, switches and others) into the Security Manager Plus enterprise setup for vulnerability assessment.
- Scan - involves scanning of desired enterprise resources for vulnerabilities. If asset discovery has not been performed then scan will involve discovering the assets first and then scanning them for vulnerabilities, open ports and missing patches and service packs.
- Remediation - involves fixing issues that cause vulnerabilities in Windows systems by deploying missing patches and service packs detected as a result of a scan on these systems.
- Reports - you can generate standard remediation or executive reports or even customize your reports based on your requirement.

Over and above the afore mentioned main steps, Security Manager Plus also supports :

- Groups - Security Manager Plus facilitates vulnerability scanning based:
    - on discovered Assets , called Asset Groups
    - on published vulnerabilities or vendor specific security bulletins - called Vulnerability Groups
- Scheduler - helps you to automatically perform vulnerability assessment of desired assets or groups at a predetermined time on a hourly, daily, weekly or monthly basis.
- Updating the vulnerability database, to be in sync with the latest vulnerability information from the AdventNet website.
- Configuring settings like mail-server, proxy server parameters, user administration etc. to ensure smooth functioning of Security Manager Plus.
- Manage credentials by supplying username and password that can be applied commonly across a group of network assets.

Follow the instructions given in the "**Before you start**" section before proceeding to work with Security Manager Plus.

Before you start

There are some mandatory configurations that you may need to do before you begin using Security Manager Plus for vulnerability assessment of your network. They are as follows :

1. Configure System Parameters
2. Update Vulnerability Database
3. Manage Credentials

Configure System Settings

Setting Proxy

Proxy server parameters are required to enable download of latest vulnerabilities from the internet and to keep the vulnerability database in sync. Refer to the 'Setting Proxy' section for more details.

Configuring Mail Server

Mail server parameters are required to enable e-mail sending functionality. Refer to 'Configuring Mail Server' section for more details.

Report Mail Settings

For you to automatically receive vulnerability reports immediately after a scan is completed, you need to configure the Security Manager Plus Report Mail Settings .

Update Vulnerability Database

Once you have started the Security Manager Plus server and have logged in to the web interface, you will need to update vulnerability database (for vulnerabilities as well as patches), before you begin any vulnerability management operation. For this, visit **Admin** tab **» Configure » Vulnerability Database Updates**.

A vulnerability database update status indicator is available in the Home tab of the web interface, under Security tab --> Latest Vulnerabilities section. This will denote if the vulnerability database of Security Manager Plus is in sync with the latest vulnerabilities in the Central Repository Server in our site.

Refer to 'Vulnerability Database Configuration' for more details.

Manage Credentials

Why do we need credentials ?

Any username/password combination that can be applied to a number of machines with administrator privileges can be pre-configured and stored in the Security Manager Plus database, these credentials are encrypted before storing them in the Security Manager Plus database. This credential will be used during scan to remotely login and identify the asset details, and perform various registry checks (in Windows) to identify related vulnerabilities and missing patches for the assets for which the scan is being performed.

Adding credentials

Go to tab **Admin » Manage » Credential Library**

- Click on the '**Add Credentials**' button from here
- Select the **Windows** radio button for configuring credentials for Windows systems or **Linux** radio button for Linux systems
- For**Credential Name** provide a unique name & **Description** of your choice.
- **User Name**, this user must have administrator privileges (Windows)
- Provide the correct **Password** used to authenticate to the remote system
- **Retype Password** to confirm.
- For Linux Credentials, provide both the Super User (root user) as well as Normal User details
- Click '**Save**' button to add these details.
- The newly added credentials will immediately appear in the '**Credential Details**' section of the page.
- You can delete the credentials, by clicking on the '**Delete**' icon.
  Public key-based authentication

  SSH keys (specific to hosts) can be supplied to authenticate **Linux hosts** before scanning. This is **optional** to supplying credentials with password.

  In order to use this functionality, under the Linux credentials --> Normal User Login Details, check the 'Public Key Authentication' check-box and provide the User Name and copy-and paste the SSH private key information in the Private Key text-area.

  Note :
  - This feature is optional
  - It is supported for SSH2 (version 2) protocol only

Dashboard

When you login to the web interface of Security Manager Plus, you are presented with a dashboard view of the security posture of your enterprise network and the assets that you are managing. The dashboard gives you an at-a-glance, business view of the hosts that are at risk, vulnerabilities that need to be addressed, missing patches that need to be deployed and also the entities (files/folders/registry entries) that have undergone most changes.

This view is classified into two main aspects that represent the security posture :

- Security snapshot
- Patches snapshot
- Inventory snapshot

Security Snapshot

The Security snapshot for Security Manager Plus captures the following information:

- Most Vulnerable Assets
- Most Vulnerable Asset Groups
- Prevalent Vulnerabilities in the Network
- Latest Vulnerabilities from our vulnerability database

From the snapshot, you can further drill-down to other important views and get detailed information.

Most Vulnerable Assets

A list of most vulnerable assets and the risk levels they are at, is displayed in this section. The risk levels are calculated based on the severity of the vulnerabilities found based on the latest scan done on the assets, with an asset having the maximum number of high risk vulnerabilities being at the highest risk. The risk level is denoted by an increasing progress bar image.

From here, you can drill-down to the Scan Details or Asset Details by clicking on the Asset Name. For viewing other most vulnerable assets, you can click on the 'more' button at the bottom of this section.

Most Vulnerable Asset Groups

This section presents a list of most vulnerable asset groups with the risk levels alongside each asset group name. The risk level for the group is calculated based on the risk levels of all the systems present in each group. So a group having many assets that are at high risk, will obviously show up as one of the most vulnerable Asset group here.

You can drill-down to Group Details by clicking on the name of the group.

Prevalent Vulnerabilities in the Network

A snapshot view of the most wide-spread vulnerabilities in your systems in the network based on the vulnerability scans performed so far, along with the risk severity.

By clicking on the vulnerability name from here, leads to a view which displays :

- the hosts affected by this vulnerability
- the complete details of the vulnerability along with the remediation solution to fix the vulnerability

Latest Vulnerabilities

A list of the latest vulnerabilities that have been updated in our central repository server recently and available in your Security Manager Plus Vulnerability Knowledge Base. Drilling-down by clicking on a vulnerability link from this section will lead to a view which displays affected hosts & vulnerability details with a remediation solution.

Vulnerability Database Up-to-date indication

You will need to update the vulnerability database periodically to be in sync with the latest vulnerabilities that we assess and release in our Central Repository Server. The status indicator icon here & a message in this section, will help indicate whether an update of the Security Manager Vulnerability Database needs to be done. You can do an instant update or schedule an update from here itself.

Patches Snapshot

The Patches snapshot for Security Manager Plus captures the following information :

- Network Patch Status
- Top Patches required for your Network
- Most Vulnerable Hosts by missing patches
- Recently Released Patches

From the Patches snapshot, you can drill-down to other views for assets and patches, and you can deploy relevant patches from thereon.

Network Patch Status

Gives you a count of missing Windows patches in your network, based on patch severity. Clicking on the patches count will lead you to a detailed view displaying the list of patches, the number of hosts each patch is missing from, Microsoft bulletin ID etc.

Deploying missing patches to hosts based on severity

You can deploy missing patches by selecting one or more patches and clicking on the 'Deploy' button in the Network Patch Status section. From the subsequent view, the names of hosts in which the selected patches are missing is displayed. Here you can choose the hosts of interest and proceed with the patch deployment.

Top Patches required for your Network

This section lists the important patches that are missing in the network by patch name. It lists the host count against each patch. Clicking on the patch name shows the affected host and the complete patch details. There is a provision to deploy the chosen patch to the hosts listed by selecting host names shown and clicking on the deploy button.

Deploying all missing patches to all hosts

From the 'Top patches' section, click on the 'more' link to see a list of ALL missing patches in your network based on the scans done using Security Manager Plus. From all the All Missing Patches view, you can select patches and click on the 'Deploy Patch' button to see the list of hosts for which each of the patches is missing.

If you select all patches, then you can deploy all missing patches to the desired hosts that miss them, at one go

Most Vulnerable Hosts by missing patches

Here you can see a list of most vulnerable hosts classified based on the severity and number of missing patches. The risk level is also displayed along side the hostname. The risk level is denoted by an increasing progress bar image.

From here, you can drill-down to the Scan Details or Asset Details by clicking on the hostname. For viewing other most vulnerable assets, you can click on the 'more' button at the bottom of this section.

Recently Released Patches

A list of the latest patches that have been updated in our central repository server recently and available in your Security Manager Plus Patches Knowledge Base. Drilling-down by clicking on a patch name link from this section will lead to a view which displays affected hosts & patch details of the chosen patch. The patch can also be deployed on all or any of the hosts from the list displayed.

Patch Database Up-to-date indication

You will need to update the vulnerability database periodically to be in sync with the latest patches that we assess and release in our Central Repository Server. The status indicator icon here & a message in this section, will help indicate whether an update of the Security Manager Vulnerability Database needs to be done. You can do an instant update or schedule an update from here itself.

Inventory Snapshot

The Inventory snapshot for Security Manager Plus captures the following information:

- OS Distribution
- Software Inventory
- Assets with most changes
- Entities with most changes

From the snapshot, you can further drill-down to other important views and get detailed information.

OS Distribution

A graph depicting the top 5 operating systems from the scanned assets along with the system count, is displayed in this section. The different operating systems can be Windows XP, Windows 2003 Server, Red Hat AS Linux, Red Hat ES Linux etc.

From here, you can drill-down to the asset list for each operating system listed by clicking on the bar graph of each OS. From the asset list you can generate the Reports of your choice from the drop-down menu.

Software Inventory

A graph depicting the top 5 installed software in the scanned assets along with the system count, is displayed in this section. This graph is useful in software inventory & license tracking.

From here, you can drill-down to the asset list, by clicking on the bar graph of each software shown. From the asset list you can generate the Reports of your choice from the drop-down menu.

Assets with most changes

A list of Windows assets in which files, folders or registry entries being monitored, have undergone most number of changes, and the risk levels these assets are at, is displayed in this section. The risk levels are calculated based on the number of changes detected relative to other systems, based on the latest scan done on the assets. This list will be populated only if Windows Change Management profile is configured for the assets.

Clicking on the asset name from here, leads to the Changes tab of the Asset Details view for the asset, which displays the File changes, Folder changes and Registry changes list.

For more information refer to Change Management section.

Entities with most changes

The list of files, folders or registry entries that have undergone most changes, along with the system count is displayed in this section. By clicking on the entity name, you will be led to the asset list for which this entity has frequently changed.

Assets

Asset Discovery

Overview

Vulnerability Assessment begins with discovery - of network assets. Asset Discovery provides an inventory of assets which you desire to be scanned. It involves addition of the resources present in your enterprise (the servers, workstations, laptops, routers, switches and others) into the Security Manager Plus enterprise setup for vulnerability scanning and assessment. Asset Discovery provides details such as IP Address, DNS Name, Operating System of all the network resources that was discovered.

Discover Assets

Assets can be added or discovered in any one or both of the following ways :

- Agentless mode - You enter hostname/IP address of the asset from the web interface of Security Manager Plus (SMP) and the Security Manager Plus server discovers and manages the asset for you.
- Agent-based mode - You install the Security Manager Plus Agent on a Windows system/host and it automatically registers to the SMP server and shows up in the web interface on the Assets tab.

Discovering Assets in the Agentless mode

Security Manager Plus provides you with a number of ways to discover your enterprise resources :

- **DNS Name or IP Address**
  - Visit the 'Assets' tab
  - Click on the 'New Assets' button
  - Select the 'Host[s]' radio button.
  - In the text box, type the type the DNS/host names or IP addresses of the network assets that you would like to discover.
  - Multiple assets (can comprise both Windows and Linux OS) can also be specified here by separating each asset with a comma.
  - Click on 'Discover' button to begin discovery.
  - You would see a discovery in progress cycle till all the host are discovered.
  - If Security Manager Plus is not able to resolve any DNS Name, due to the host not being in network or has been switched off, then it would suitably warn you, stating "Could not resolve the hosts <host-name>".

[0R]

- # IP Range
    - Visit the 'Assets' tab
    - Click on the 'New Assets' button
    - Select the 'IP Range' radio button.
    - Enter the range of IP addresses of assets within a particular subnet that you would like to discover (can comprise of both Windows and Linux OS).
    - Click on 'Discover' button to begin discovery.
    - You would see a discovery in progress cycle till all the host are discovered.

The successfully discovered systems will be listed in the Assets view in the background.

Supplying Credentials

You can supply the credentials (username and password) required to login and detect/deploy missing patches and service pack, for **individual** hosts from the 'Assets' tab.

Visit the Assets tab, and click on the  icon against the host name in the Assets table. You can either specify user-defined credentials or use credentials defined in the Credential Library. Based on whether the system is Windows or Linux, enter the user name and password accordingly, to login to the system. Provide the information and click on 'Save' button. Once the credentials are configured, the icon against the system name changes to  .

Deleting host-specific credentials can be done only from the Admin tab --> Credential Library link --> Credential details table.

Type of credentials

- Windows - for Windows hosts. Specify system login username and password.
- Linux - for Linux hosts. Specify super user name and password to login.
- Others - for Windows hosts only. Current type supported: MSSQL - if the asset being discovered/scan has an MSSQL server installed and running, you can specify username & password of the 'master' database in the MSSQL server on this system. This credential will be used to login to the system.

Deleting Assets

You can delete the discovered assets using the '**Delete**' button in the Assets tab. Deleting an asset will result in deletion of its scan result, provided the scanning for the 'to be deleted' asset has been already done.

Asset Scans

The discovered assets can be scanned from the Assets tab using the '**Scan**' button after selecting the desired IP Address / DNS Name. You can also perform scans using any of the many provisions like : New Scan, Schedule Scan . Refer 'Scans' for more details.

Search for Assets

Assets (systems or hosts in Security Manager Plus) that have been discovered & scanned can be located using the '**Search Assets**' search box on the top right-corner of every screen, by specifying the IP address of the DNS name of the host and clicking on the **Go** button.

The search results will display the systems or hosts that match, along with their OS type, number of vulnerabilities & last scanned time. You can run a scan again from here or generate a vulnerability report for a particular asset.

An **Advanced Search** feature is also provided to locate 'scanned' hosts based on select criteria. You can select the desired search options from the list of choices available and supply the value to form a criterion. Any number of such criteria can be specified and can be set to match either all or any one criterion. The Search Results listing the hosts are displayed at the bottom of this screen itself.

You can also search for assets from the Scan Results view for a particular scan. The criteria specified here will be used to search for assets from the chosen scan alone.

Groups

Groups

Scanning your entire network can be cumbersome as it is very resource intensive. Groups make the task of scanning and reporting for your enterprise resources more efficient. You can scan a group repeatedly and know that the same IP's and domains are included every time. By organizing scans based on groups you can limit the scope of the scan target, making the results and prioritization of tasks more manageable. Groups provide flexibility, allowing for cases where the same assets may be defined in multiple groups having different business priorities.

Security Manager Plus provides logical grouping for scans as follows :

- Asset Groups
- Vulnerability Groups
- Patch Groups

Asset Groups

Asset groups are logical grouping of network IP's. You can group the discovered IP's based on domains and other network entities like switches and routers. You can create a group, say Windows Group for all your Windows machines in your network , Linux Group for all your Linux machines in your network, and even groups for all your Cisco routers or HP switches present in your network. Asset grouping thus provides you with the option to perform selective scanning of desired hosts.

By organizing assets into logical subsections of your network, you can limit the scope of the scan target, making the results and remediation tasks more manageable. Asset groups provide flexibility, allowing for cases where the same assets may be defined in multiple groups having different business priorities.

View Asset Groups

To view the list of existing asset groups,

- Visit the '**Assets**' tab.
- Click on the **Asset Groups sub-**tab
- This view will display the list of Asset Groups created (if any).
- From here you can perform operations such as, scanning the entire group by clicking on '**Scan Groups**' button and deleting the group by click on '**Delete Groups**' button.

Providing credentials for Asset group

You can set the credentials for an asset group (login username and password), which will be applied commonly across all assets in this group. This can be done by clicking on the  icon against each group name. Each asset might have been assigned a different set of credentials from the Assets tab, but when it is a part of an Asset group, the credentials applied for the group only will hold good for all vulnerability management operations.

Create a new asset group by grouping existing assets

To create a new asset group follow these instructions :

- Click on the **New Group** tab after you login to the web interface.
- This will drop to 3 options - choose the first one: '**Group existing Assets**'
- This displays the new group creation page.
- In the '**Group Name**' field enter a descriptive name.
- In the '**Description**' field enter a brief description about the asset group.
- Select from the list of host names / IP addresses and click '**Create**'.

- Your Group will be created and the assets will be added to the group and will appear in the Asset Groups list.

Alternatively, you can visit the '**Assets**' tab, select the **Asset Groups sub-**tab and click on the 'New Group' button to get to the same screen as above.

Create asset groups from Domain

You can create asset groups by picking up hosts from the different domains available in your enterprise network.

- Click on the **New Group** tab after you login to the web interface.
- This will drop to 3 options - choose the third option: '**Import from Domain**'
- This will lead to a screen where the list of domains is automatically displayed.
- Choose the domains from the list and click 'Create Groups'
- Each domain selected will be added as an individual asset group with group name same as domain name

  All systems under the domain will be automatically part of the respective asset group

Note : *This feature is available only when the Security Manager Plus server is running in a Windows system.*

Create asset groups by importing from CSV file

You can create asset groups by specifying host names or IP addresses of systems in a CSV file, and then importing this file from Security Manager Plus

- Click on the **New Group** tab after you login to the web interface.
- This will drop to 3 options - choose the second option: '**Import from CSV**'
- Click on the '**Import from File**' link present on the right hand side of the screen.
- This will lead to a screen from where you can browse and select the file with the systems list
- The name of the asset group, description of the group and system names or IP addresses can be provided in the file. More than one group can also be created by separating each group information with hash (#)
- Once the file has been selected, click on the **Create** button. Groups will be created as per the information in the file.

You can also supply the hostnames/IP address in the '**Device Names**' text area provided on this screen, manually and they will be added to the asset group.

Asset Group Details

By clicking on the asset group name, you can get into the details of this particular groups. The following information is displayed :

- Devices tab
- Security tab

Devices tab

This tab lists the devices that have been grouped and gives information about the group like Last Scanned time, credentials for the group, what vulnerability group was applied to this asset group for scanning, when was the asset group created etc.

The Asset List displays the hosts in the group along with the following info :

- vulnerability count for each asset based on severity (high, medium & low)
- number of open ports
- missing patches & missing service packs count
- scan status

Security tab

The Security tab for an asset group displays the security snapshot of the group. The following info is displayed :

- Vulnerabilities count based on severity
- Missing patches count based on severity
- Missing service packs count
- Installed patches count based on severity

Pie chart

A pie-chart depicting the vulnerability risk percentage for the asset group is displayed.

Vulnerabilities list

The list of vulnerabilities that have been detected on the assets in this group based on a vulnerability scan is seen. The number of affected hosts for each of these vulnerabilities is listed. Clicking on the affected host count or vulnerability name will lead you to the Vulnerability details view which describes the vulnerability & provides appropriate links to external websites like CVE, Bugtraq etc. It will also list the host names which this vulnerability affects.

Missing patches list

This list presents the missing patch information for the asset group. The number of hosts for each of these missing patches is listed. Clicking on the affected host count or patch name will lead you to the Patch details view which describes the patch & provides appropriate links to Microsoft's or Red Hat's websites. This patch can be deployed from here on the list of affected hosts.

Remediate Asset Group

From an Asset group, you can remediate the hosts by applying missing Windows patches & service packs. From the Assets tab --> Asset Groups tab --> Asset group name link --> click on the '**Remediate**' button to either Deploy Missing Patches or Service Packs.

Deploying Patches

Clicking on 'Deploy Patches' option from the 'Remediate' menu, lists all the missing patches applicable for this Asset Group. From here you can select whichever patches you wish to deploy on the group. Choose the patches of interest and click on the 'Deploy Patch' button. Doing so will display a screen wherein you will be able to see a list of hosts belonging to the Asset group, in which the selected patches are missing. From this view, click the 'Deploy' button to perform patch deployment on the hosts.

Patch Deployment History

If any patch is deployed on a host, a history will be maintained about when it was deployed and to which all systems and what was the status of deployment. You can view this by clicking the patch history icon  against each patch in the list.

Deploying Service Packs

Clicking on 'Deploy Service Packs' option from the 'Remediate' menu, lists all the SPs applicable for this Asset Group. From here you can select whichever service pack you wish to deploy on the group. Choose the SP of interest and click on the 'Deploy' button. Doing so will display a screen wherein you will be able to see a list of hosts belonging to the Asset group, in which the selected SP is missing. From this view, click the 'Deploy Service Pack' button to perform service pack deployment on the hosts.

Note that you can deploy only one service pack at a time on a host, so you can select only a single SP from this view.

Download Service Packs

You can also download service packs from this view. Select the SP and click on the 'Download' button. You can initiate an instant download or schedule the SP download for a later time. From this screen, there is also a provision to use an already downloaded SP.

Service Pack Deployment History

If any SP is deployed on a host, a history will be maintained about when it was deployed and to which all systems and what was the status of deployment. You can view this by clicking the service pack history icon  against each SP in the list.

Deploying Linux Packages

If there are Linux systems in the Asset group, you can deploy missing Linux packages on these assets by clicking on the 'Deploy Linux Packages' option from the 'Remediate' menu. You can select the packages that you wish to deploy and click on the Deploy button.

Refer to Linux Package Management Scripts section for more information.

Reports for Asset Group

Reports can be generated for every Asset group created. For this visit the Assets tab --> Asset Groups tab --> Asset group name link --> click on the '**Reports**' button. This will drop down to all the reports that are present in Security Manager (predefined as well as custom reports). Choose whichever report you want for the group and click on the appropriate name.

Actions from Asset Group

The following are the actions that can be performed from Asset groups. These can be accessed from the '**Actions**' button in an Asset group view.

Scan Notification

This is an option to configure the e-mail ID to which a notification will be sent when a scan for the asset group is completed. You can specify the e-mail ID in the text field provided. Selected reports from Security Manager Plus can also be attached along with the scan complete notification. You can choose the report type from the drop-down menu and click 'Save'.

Schedule Scan

You can initiate an on-demand vulnerability scan on an Asset group from the Asset groups view or you can schedule a scan from this menu option, so that it runs at a specified time and periodicity.

Scan Now

You can start an on-demand scan by choosing this option.

Edit Group

You can edit an existing Asset group from here. You can alter the group name, description, add more hosts to this group or remove hosts from this group.

Ticket Settings

When the Trouble Ticket E-mail Settings are configured from the Admin tab, then you can use this option to select a criterion, which when exceeds by a configured count, e-mail will be generated to the trouble ticket system. For e.g. Total Vulnerability count : Greater than : 10. You can also remove the ticket settings from the same screen if configured already.

Change Management

You can associate Change Management profiles to this asset group so that files, folders and/or registry entries are tracked for changes. Each profile will have a set of files, folders and registry entries that are configured for change management & change tracking.

Vulnerability Groups

Vulnerability Groups are logical grouping of vulnerability knowledge base. You can form vulnerability groups from the existing list of vulnerability test cases based on risk level, vulnerability type or services affected.

View vulnerability groups

To view the list of all existing vulnerability groups,

- Visit the '**Admin**' tab.
- In this view, from the **Manage** section, click on **Vulnerability Groups** link
- This, by default, leads to the **Groups** tab, which displays a complete list of all vulnerabilities that is scanned by Security Manager Plus.

Actions from this view

- Scan this group - click on this link against each vulnerability group, to associate a hostname to scan based on this group
- Add vulnerabilities to group - click this link, to add more vulnerabilities to the group (from the All vulnerabilities list)
- Delete - click to delete this vulnerability group

Create custom vulnerability group

You can create your own custom vulnerability groups, from the existing vulnerabilities listthat Security Manager Plus maintains in its vulnerability database, based on type, risk and service affected. To create custom vulnerability group follow these instructions :

- Visit the '**Admin**' tab.
- In this view, from the **Manage** section, click on **Vulnerability Groups** link to come to the **Groups** tab
- Click on the '**New Group**' button
- From here, specify the Group name and Description and select the vulnerabilities to be grouped from the all vulnerabilities list in the table below
- Click 'Create' to create and save the new Vulnerability group

Viewing Group Details

You can view the information about each and every vulnerability associated to a vulnerability group, like Risk level, Vulnerability description, CVE ID. You can choose to view the different vulnerabilities under each group by selecting the group name from the 'Show Vulnerabilities in' drop-down menu to the right corner of this screen.

Actions from this view

- Add to Group - you can select vulnerabilities from a chosen group and add them to any other group by clicking on this button and choosing the other vulnerability group name
- Delete from Group - you can discard vulnerabilities from this group by clicking this button

Viewing affected hosts & details for a particular vulnerability

Click on the **Short Description** link against each vulnerability to view the complete description of the vulnerability and its remediation solution if any, along with the list of hosts it affects.

Patch Groups

Patches belonging to a specific category, can be grouped together, so that they can be managed effectively. Each custom patch group will be represented by a name, and all patch management operations like adding downloading patches, deploying patches, adding patches to another group etc. can be done for this group.

For example, say you want to manage all the **Critical** patches for the Internet Explorer 6 software installed in your enterprise. You can create a group called '**IE_6_Critical**' and associate all patches for IE 6 from to this group. From the custom patch group view 'IE-6_Critical' you can manage these patches.

Follow these topics to work with Custom Patch Groups :

- Creating & viewing patch group
- Working with patch groups

Creating & viewing patch group

To create a patch group follow these instructions :

- Visit the '**Admin** tab --> **Manage** section --> **Patch Groups'** link. This view will display the list of Patch Groups created (if any)
- Click on the 'New Patch Group' button present in the screen
- Now from this configuration screen, enter the Group Name and the description of the patch group
- You can use the filter in the patches table to choose the OS type, patch language, product and service pack to list the patches
- Select the patches that you wish to group from the tabular list, and click the 'Create' button
- Your group will be added and will appear in the Patch Groups list
- The Edit icon adjacent to the group name can be used to edit the group details (name & description)
- You can add more patches to this group or even delete the patch group

Viewing patch group

- You can click on the Group Name text-link, to view the patches in that group
- From here you can, you can perform operations such as, displaying systems affected by the selected patch, downloading patches, adding patches to other groups, deleting patches from this group and deploying selected patch groups to system groups etc.

Working with patch group

The following are the operations that can be performed from Patch Group views :

- Displaying systems affected by a patch
- Deploying patches/ patch group to system groups
- Deploying patches to a system
- Downloading patches present in a group
- Adding patches to other patch groups
- Deleting patches from group
- Viewing patch specific information

Displaying systems affected by a patch

In order to find which systems are missing patches from the group; select the desired patches from the list and click on the "**Deploy**" button. This will display a screen wherein you will be able to deploy a patch to multiple systems (1 patch to many systems) and any number of selected patches to multiple systems (many patches to many systems), by choosing from the . Note that this list is based on the latest scan results in Security Manager Plus.

For more information on installing patches, refer Deploying Patches section.

Deploying patches /patch groups to system groups

To deploy patches in a group to system groups or to deploy entire patch groups to system groups, select the patches and click on the '**Deploy to Group**' button. This will bring you to a screen from where you can select from a list of system groups to which the chosen patches need to be applied. More than one system group can also be selected.

Deploying patches to a system

Click on any patch name in the group list and you will be led to a screen where the systems/assets that miss this patch, will be listed. From here, you can deploy the patch to these assets.

Downloading patches present in a group

To download the patches in the group (if they are not already available in the Security Manager Plus server), select the patches of interest and click on the "**Download**" button.

Adding patches to other patch groups

Patches in an existing patch group can be included in other patch groups, by clicking on the '**Add to Group**' button.

Deleting patches from group

In order to delete patches from a particular group, select the patches and click on the '**Delete from group**' button.

Vulnerability Scan

Vulnerability Scan

Overview

If Asset Discovery has not been specifically performed prior to scanning, then Security Manager Plus's vulnerability scanning will first begin with the discovery of the desired network resources. On completion of asset discovery, Security Manager Plus detects the open ports and a scan is performed on the open ports for identifying which services or applications are listening in these ports.

On identifying the service, tests are run to identify the service specific vulnerabilities and missing patches. When a scan is complete, vulnerabilities are displayed in a color-coded list , like: HIGH, MEDIUM, LOW, that indicates the severity / risk of each potential problem. Clicking on individual vulnerabilities displays information on the name of the vulnerability, a detailed description, and suggested remediation methods.

Scan Preference

There are a various ways to perform scans using Security Manager Plus. You can exercise these options from the **New Scan** tab drop-down options :

- Scan Hosts
- Scan Network
- Scan Asset Group

These options run an on-demand scan. Apart from these you can also Schedule Scans for assets and asset groups.

Scan Hosts

To start a new scan from here :

- Supply host name or IP address. Multiple hosts can be separated by commas.
- Select the Scan Type from the list. You can scan for All vulnerabilities or any of the predefined Vulnerability groups.
- Custom vulnerability groups can also be created from Admin tab --> Manage --> Vulnerability Groups and associated from here.
- Supply credentials (Windows/Linux) to perform a detailed scan of the hosts
- Credentials can be user defined or predefined (from the Admin tab --> Credentials Library)

- Usernames must have administrator privileges & must be specified in the format: <domainname>\<username> if the hosts are in a Windows domain. If they are not, then specify: <systemname>\<username>
- If you wish to be notified via e-mail after scan completion, select Notify and provide your e-mail address. E-mails can be sent based on criteria as well.
- If a ticket has to be generated to your Trouble-ticketing system, select Generate Ticket and choose the criterion. The Trouble-ticket e-mail ID can be configured from Admin tab --> Configure section --> Trouble Ticket Settings link

Scan Network

- Enter IP ranges to scan, starting from the lowest IP to the highest IP (for example: 192.160.121.0 to 192.160.121.255).
- Select the Scan Type from the list. You can scan for All vulnerabilities or any of the predefined Vulnerability groups.
- Custom vulnerability groups can also be created from Admin tab --> Manage --> Vulnerability Groups and associated from here.
- Supply credentials (Windows/Linux) to perform a detailed scan of the hosts
- Credentials can be user defined or predefined (from the Credentials Library)
- Usernames must have administrator privileges & must be specified in the format: <domainname>\<username> if the hosts are in a Windows domain. If they are not, then specify: <systemname>\<username>
- If you wish to be notified via e-mail after scan completion, select Notify and provide your e-mail address. E-mails can be sent based on criteria as well.
- If a ticket has to be generated to your Trouble-ticketing system, select Generate Ticket and choose the criterion. The Trouble-ticket e-mail ID can be configured from Admin tab --> Configure section --> Trouble Ticket Settings link

Scan Asset Group

- Select the Asset group to be scanned from the list of asset groups. The list will be empty if asset groups have not been created.
- Select the Scan Type from the list. You can scan for All vulnerabilities or any of the predefined Vulnerability groups.
- Custom vulnerability groups can also be created from Admin tab --> Manage --> Vulnerability Groups and associated from here.
- Supply credentials (Windows/Linux) to perform a detailed scan of the hosts
- Credentials can be user defined or predefined (from the Credentials Library)
- Usernames must have administrator privileges & must be specified in the format: <domainname>\<username> if the hosts are in a Windows domain. If they are not, then specify: <systemname>\<username>
- If you wish to be notified via e-mail after scan completion, select Notify and provide your e-mail address. E-mails can be sent based on criteria as well.

- If a ticket has to be generated to your Trouble-ticketing system, select Generate Ticket and choose the criterion. The Trouble-ticket e-mail ID can be configured from Admin tab --> Configure section --> Trouble Ticket Settings link

Scan in Progress & viewing logs

When a scan is initiated, a 'Scan in Progress' message appears on screen. On clicking that message or by refreshing the view, you can see the Scan Status column against the asset or asset group name which displays a 'In Progress' message. Clicking on this will pop-up a window which will display the scan progress logs.

When a scan is successfully completed, the Scan Status column gets updated to display this.

Stopping a scan

When a scan is in progress, it can be stopped from the [stop] link against the asset name. The Scan Status column for this asset gets updated with the 'Stopped' message.

Scheduled Scan

How to schedule a scan?

You can set up schedule scan for Assets or Asset Groups by visiting the respective views from Asset tab and clicking on the  icon against the Asset name or the Asset Group name. In the **Scheduler** section you are provided with the following options for scheduling a scan :

- **Once Only**
  This option is for scheduling a **single scan** on a specified date and time desired by you.
- **Hourly**
  This option is for scheduling a scan to be performed on an **hourly basis**, starting at the specified date and time desired by you.
- **Daily**
  This option is for scheduling a scan everyday at a particular time desired by you.
- **Weekly**
  This option is for scheduling a scan at a particular time on certain days of the week desired by you.
- **Monthly**
  This option is for scheduling a scan on a particular day of the month at a particular time desired by you.

Once all the necessary details required for a New Schedule have been given, click the **Save** button.

Editing a scan schedule

Once a schedule has been created, the icon changes to this  . On clicking this icon, you can view the type of schedule set (will be highlighted), change the settings or even enable or disable by selecting the checkbox.

Viewing Scan Results (Asset Details)

You get to view the results of your scan as soon as the scan is completed. The scan results provide the vulnerability details about each individual IP / Host.

Getting to Scan Results or Asset Details

By default, once a scan is completed you get to view the results of the scan immediately. Click on the **Asset Name link** in the **Assets** tab link to take you to the **Scan Result** or **Asset Details** view of the particular host / IP address in the scan.

Asset Details

The Scan Details view consists of the following information :

- Security
- Hardware
- Software
- User Groups
- Changes

Remediate Asset

From Asset Details view, you can remediate the host by applying missing Windows patches & service packs. From the Assets tab --> All Assets tab --> Asset Name link --> click on the '**Remediate**' button to either Deploy Missing Patches or Service Packs.

Deploying Patches

Clicking on 'Deploy Patches' option from the 'Remediate' menu, lists all the missing patches applicable for this Asset. From here you can select whichever patches you wish to deploy on the asset. Choose the patches of interest and click on the 'Deploy Patch' button to perform patch deployment on the host.

Patch Deployment History

If any patch is deployed on a host, a history will be maintained about when it was deployed and to which all systems and what was the status of deployment. You can view this by clicking the patch history icon against each patch in the list.

Deploying Service Packs

Clicking on 'Deploy Service Packs' option from the 'Remediate' menu, lists all the SPs applicable for this Asset. From here you can select whichever service pack you wish to deploy. Choose the SP of interest and click on the 'Deploy' button to perform service pack deployment on the host.

Note that you can deploy only one service pack at a time on a host, so you can select only a single SP from this view.

Download Service Packs

You can also download service packs from this view. Select the SP and click on the 'Download' button. You can initiate an instant download or schedule the SP download for a later time. From this screen, there is also a provision to use an already downloaded SP.

Service Pack Deployment History

If any SP is deployed on a host, a history will be maintained about when it was deployed and to which all systems and what was the status of deployment. You can view this by clicking the service pack history icon  against each SP in the list.

Deploying Linux Packages

If the asset is a Linux system, you can deploy missing Linux packages by clicking on the 'Deploy Linux Packages' option from the 'Remediate' menu. You can select the packages that you wish to deploy and click on the Deploy button.

Refer to Linux Package Management Scripts section for more information.

Reports for Assets

Reports can be generated for every Asset. For this visit the Assets tab --> All Assets tab --> Asset name link --> click on the '**Reports**' button. This will drop down to all the reports that are present in Security Manager (predefined as well as custom reports). Choose whichever report you want for the asset and click on the appropriate name.

Actions from Asset Details

The following are the actions that can be performed from Asset Details. These can be accessed from the '**Actions**' button in an Asset Details view.

Scan Notification

This is an option to configure the e-mail ID to which a notification will be sent when a scan for the asset is completed. You can specify the e-mail ID in the text field provided. Selected reports from Security Manager Plus can also be attached along with the scan complete notification. You can choose the report type from the drop-down menu and click 'Save'.

Schedule Scan

You can initiate an on-demand vulnerability scan on an Asset from the Asset details view or you can schedule a scan from this menu option, so that it runs at a specified time and periodicity.

Scan Now

You can start an on-demand scan by choosing this option.

Edit Host

You can edit an existing Asset from here. You can alter the host name (display name) and Operating system type.

Ticket Settings

When the Trouble Ticket E-mail Settings are configured from the Admin tab, then you can use this option to select a criterion, which when exceeds by a configured count, e-mail will be generated to the trouble ticket system. For e.g. Total Vulnerability count : Greater than : 10. You can also remove the ticket settings from the same screen if configured already.

Change Management

You can associate Change Management profiles to this asset so that files, folders and/or registry entries are tracked for changes. Each profile will have a set of files, folders and registry entries that are configured for change management & change tracking.

Configure Agent

This option appears only for systems being managed in the agent mode. Refer to Agent Configuration section for more information.

Security tab

Host Information

A high-level summary of a particular host in the Scan is provided, with general details like IP Address, Operating System, System Language and scan details like the Vulnerability Group, Vulnerabilities Found, Vulnerability Checks Performed, Missing Security Updates, number of open ports, initiator of the scan, start and end time of the scan and time taken for the scan.

A pie-chart depicting the vulnerability risk percentage for the host is also seen in this section.

Open Ports

Gives a complete list of open ports that were found during the scan of a particular host or IP, with details like the Service Running at the port, Service Info and the number of vulnerabilities found against each service listening in the open ports.

Vulnerabilities

This view provides you with a tabular listing of the vulnerabilities found in that particular host of the Scan Job. You get to view details like :

- Risk - a color-coded list , like: HIGH, MEDIUM, LOW, that indicates the severity / risk of the vulnerability.
- Service - services or applications that are listening in the open ports.
- Port - the open port (number) at which the service or application is running.
- Short Description - Each entry against this column is a link, clicking this link provides brief details of the vulnerability like the service affected by the vulnerability, the CVE and Bugtrack reference ID's (if any), a concise description of the cause and effect of the vulnerability, how to remediate this vulnerability, the type of vulnerability (like Denial of service, SQL Injection, Cross-site scripting ...), the risk factor to your enterprise security due this vulnerability, like: HIGH, MEDIUM, LOW,. You also can get a detailed information on the vulnerability by clicking on the short description link.
- Solution - captures the essence of remediation solution for the vulnerability info provided in the Short Description link.

  Marking False Positives

  A vulnerability will be classified as a "False Positive", when Security Manager Plus detects one but it is not considered as a real threat or if a solution has been found to work around such a vulnerability.

  From the Scan Results / Asset Details, for a particular host, in the 'Vulnerabilities' link, you will have the option to mark a vulnerability as false positive, by clicking the button against a particular vulnerability. By doing this, you can select this vulnerability to be omitted from your Scan Reports.

  You can unmark a marked false positive by clicking on the button.

AntiVirus Software

This section displays the details of any AntiVirus software that might be installed in the scanned systems. It will list the following information :

- Antivirus product name
- Version number
- Engine version

- Pattern version
- Pattern date
- Real time scan (enabled or disabled)

Service Pack Details

In this section, you can see information on what service pack is missing from the list of Windows applications that the scan has detected. Clicking on the product name from the list, will take you to the screen from where you can deploy the service pack.

Missing Patches

In this section, you get to view details like :

- Severity - Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information or as a result of patch assessment done by AdventNet.
- Bulletin : The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the Bulletin Details view, which provides more info about the Bulletin and the vulnerability.
- Patch To Install : The name of the patch that will be installed.

Note : Security Manager Plus supports detection of missing patches for Windows as well as Linux machines. Supported Windows operating systems are : Windows Vista, Windows XP, 2000 Server and Professional, NT Workstation and Server, 2003 Server and applications are : IIS, IE, SQL Server, MDAC, Media Player, .NET Framework, MSXML, DirectX, Windows Defender, MS Office etc.. Supported Linux distributions are : Red Hat Linux and Debian Linux. You need to supply the credentials of the target machine for which the scan is being performed.

Hardware Inventory

This section of the Scan Result for a particular system, lists the inventory of the different hardware components present in the system. Some of information displayed are :

- System Info - what brand the asset is, model, bios name
- Processor Info - CPU details
- Memory - RAM information like total memory, free memory, virtual memory and free virtual memory
- Drives associated to this system
- Peripherals that are connected to this system like Keyboard, Mouse, Monitor, Video/Sound Cards, USBs
- Network information - IP address, MAC address, NIC name, DNS server etc.
- Port details - port type and status

Software Inventory

This section lists all the following information :

- software that has been currently installed on the system, along with the name, vendor information and software version.
- list of installed patches on the system
- list of Windows Services that are present. The following information is displayed here :
    - Service names
    - Status - whether the service is Running or Stopped
    - Startup type - whether the service is set to start Automatically, Manually or is Disabled
    - Logon As - the user account type that this service will be started in

Note :

- Software inventory is detected only for Windows systems. Software Inventory for other Operating Systems is currently not supported
- Software Inventory for Windows systems can be detected only if Security Manager Plus server is running in a Windows system

User Groups

Windows Users List

This section of the Scan Result displays the list of user accounts existing in the scanned systems, and the following details about each account :

- Home Directory
- Script Path
- Flags
- Number of Logons
- Last Logon
- Bad Password Count
- Account Expires
- Workstations
- Password Age
- Comment

Windows Groups List

This section lists the Windows User Groups (namely Administrators, Backup Operators, Guests, Power users etc.) present in the systems, along with list of group members in each category and the group description.

Changes

This section of the Scan Result or Asset Details view displays the File Changes, Folder Changes & Registry Changes for a Windows system. A combination of files, folders or registry entries can be configured as a Change Management profile, so that Security Manager Plus can track & report changes that occur on all these entities.

Profiles

The Change Management profiles that have been associated to this Windows asset are listed. On clicking on the profile name, you will be led to the Profile configuration screen, where you can add or delete the entries under each category (file, folder or registry) for this particular profile.

File Changes

This is a tabular display of files that have been configured in the associated profile for which change detection has to be tracked during every scan. The information present in this table are:

- File name
- Last modified date & time
- Comments
- Status icon (red or green) - where red depicts that the file has been modified when comparing against the baseline during a scan & green depicts there has been no change detected.

On clicking the File name link from the above list, you get to see the values comparison chart showing the Baseline values and the Current values. From this you can understand what parameter being checked for has changed. By default, the details obtained from a file after the first scan on an asset, will be treated as the Baseline value for the different parameters.

Folder Changes

This is a tabular display of Windows folders that have been configured in the associated profile for which change detection has to be tracked during every scan. The information present in this table are:

- Folder name
- Last modified date & time
- Comments
- Status icon (red or green) - where red depicts that the folder has been modified when comparing against the baseline during a scan & green depicts there has been no change detected.

On clicking the Folder name link from the above list, you get to see the values comparison chart showing the Baseline values and the Current values. From this you can understand what parameter being checked for has changed. By default, the details obtained from a folder after the first scan on an asset, will be treated as the Baseline value for the different parameters.

Registry Changes

This is a tabular display of Registry entries that have been configured in the associated profile for which change detection has to be tracked during every scan. The information present in this table are:

- Registry key
- Current Value
- Baseline Value
- Comments
- Status icon (red or green) - where red depicts that the registry entry has been modified when comparing against the baseline during a scan & green depicts there has been no change detected.

By default, the values for a Registry key after the first scan on an asset, will be treated as the Baseline value for the different parameters.

Setting Baseline

By default, the details obtained from a File or a Folder or the values for a Registry key after the first scan on an asset, will be treated as the Baseline value for various parameters being tracked. However, this can be altered at any time and a baseline can be set to be a changed value. In order to alter the baseline, you can click on the Baseline icon in the "Set as Baseline" column for the entry which has a changed status (red icon) if you think the change is appropriate. From the subsequent scans, this will be treated as the Baseline and compared against.

Setting baselines is applicable for every entry under each category (files, folders or registry).

Report Generation

To generate reports for the systems in this scan result, click on the '**Generate Report**' on the top of the page and select the type of report. Visit Reports for more information.

Remediation

Remediation

Although detection and assessment of vulnerabilities is the core functionality of a vulnerability scanner like Security Manager Plus, remediating the detected vulnerabilities is a powerful feature that greatly assists system administrators and IT staff to take quick action and eradicate security threats - using the same software.

Remediating vulnerabilities comprises of aspects like generating trouble tickets so that administrators can be notified instantly and hence take appropriate steps to mitigate risks, effecting configuration changes in systems, routers or firewalls, starting or stopping certain services, making Registry entries, deploying missing patches and service packs, detecting viruses and quarantining them and many more.

There are different types of vulnerabilities and remediating them all involves different mechanisms based on the nature of the vulnerability. Security Manager Plus supports remediation by deploying missing patches and service packs for Windows systems. Refer to topics in the following section on how to go about patch deployment.

Deploying Patches & Service Packs

Remediate Assets & Asset Groups

These are the following topics in this document :

Viewing Missing Patches for Assets & Asset Groups

From the Asset Details view, click on the **Remediate** button --> **Deploy Patches** link to view the list of missing patches for the asset, based on the latest scan on the asset. You get to see a list of missing patches for the host with the following information :

- Severity - Determines the importance of the patch. These severity ratings are as per the bulletin or advisory information or as a result of patch assessment done by AdventNet
- Bulletin ID : The advisory article provided by the vendor which contains information about the vulnerability and patch availability. Clicking this link, will lead you to the **Bulletin Details** view, which provides more info about the Bulletin and the vulnerability
- Patch Name : The patch that is missing. The icon against the patch name will display the vulnerability (in brief) that a patch addresses
- Download Status : Determines whether the patch is downloaded from the internet (vendor site) and is made available in the Security Manager Plus server for deployment, if the download has failed for some reason or if the download is not available.
- Reboot status - if a reboot of the system is required after the application of a patch.
- Patch History Report - This view displays the list of tasks that have been already executed for this particular patch. In this view, you can see to which system a patch has been applied, at what time, its status and associated remarks on task completion

For Asset Groups, from the Asset Group Details view, click on the **Remediate** button --> **Deploy Patches** link to view the list of missing patches for the asset group, based on the latest scan on the asset group. You get to see a list of missing patches for all the hosts that are a part of this group. The information displayed here is the same as for Asset Details.

Deploying Missing Patches

From the patches list view (from Asset Details view or Asset Group view), you can select the patches of interest and click on the 'Deploy Patch' button.

Before commencing the actual deployment, Security Manager Plus checks if the patches selected are already downloaded and available locally in the Security Manager Plus server. If not, a download request is first initiated and the patches in question are downloaded from the vendor websites via the internet. Once the patches are available locally, they are then copied to the remote systems and executed. The transfer of the patches from the Security Manager Plus server to the remote systems is via secure means (https). Therefore tampering of patches and installation of inappropriate hotfixes is completely eliminated.

On clicking the **Deploy Patch** button, you will be led to a patch deployment configuration screen. Make the necessary configurations as below, and click on the '**Deploy**' button. This will bring up a Deployment Status screen with information on the progress of the deployment.

Deployment Scheduling

From the Deployment configuration screen, you can choose the deploy the selected patches instantly (select the 'Deploy Now' radio button) or schedule the deployment at a later time (select the 'Deploy Later' option and set the date and time).

Restart Options

Restart

Security Manager Plus automatically determines if rebooting the system is required after patch deployment, for the installation to complete successfully. The radio button in the restart options is set accordingly. You have the provision to change the options, but it is best advised to let the configurations remain.

If the restart option is selected, you further have options to configure the time interval to wait before the system reboots itself. You can also force the applications to close automatically.

Shutdown

If you wish to bring the system to a **halt** after patch deployment has been completed, you can choose the 'Shutdown' option.

If the shutdown option is selected, you further have options to configure the time interval to wait before the system shuts down. You can also force the applications to close automatically before shutting down.

Don't Restart

This option is for patches that do not require a restart of a system after deployment

Alert Message

After the deployment is complete, you can configure a custom message to be displayed in the affected system.

MS Office Media Configuration

When MS Office patches are a part of your selected list of patches, you will see a configuration section where you will need to specify the MS Office CD path or AIP path. Refer to Configuring MS Office Media Location for more information.

Timeout Configuration (only for SP deployment)

The estimated minimum timetaken in minutes, for the deployment of an SP to complete, is specified here by default. You can increase the timeout value if you are operating on a low-end machine or on a slow network. If the deployment of the service pack takes longer than this duration, you will get an intimation in the Status Window to this effect and then the service pack deployment task will proceed till a system preset time.

E-mailing Deployment Status

The status of the deployment can be intimated by e-mail to any e-mail address (ideally the administrator's e-mail ID) that is configured here. Enter any number of e-mail addresses in the text-field provided; separated by comma. A report will be sent to those IDs when the deployment task is completed.

Viewing Service Packs for Assets & Asset Groups

From the Asset Details view, click on the **Remediate** button --> **Deploy Service Packs** link to view the list of missing service packs for the applications detected in the asset, based on the latest scan on the asset.

From this list, you can identify which service pack is available and which is missing. You can then proceed to download and deploy the missing service pack for each product, one at a time.

The other details in the service pack view are same as the ones in missing patches view.

From the Asset Details view, click on the **Remediate** button --> **Deploy Service Packs** link to view the list of missing service packs for the applications detected in the asset, based on the latest scan on the asset.

Deploying Patches from Patches Snapshot in the Dashboard

Patches can be deployed from the Dashboard displayed in the Home tab. From the Dashboard, select the Patches tab to view the patches snapshot. You can refer to the Patches Snapshot for more information on various options available by which patches can be deployed.

Deploying Patches from Patch Groups

You can also deploy groups of patches to entire system groups. Refer to Patch Groups for more information.

Deploying All Missing Patches

You can deploy all the missing patches in your network at one shot from **Admin** tab --> **Action** section --> **Deploy Patches** screen.

Deploying MS Office Patches

The deployment of MS Office patches requires some special handling. Some of the patches do not contain complete files but only the the differences required to modify the original file with the patched code. For these Office patches to be installed, they require access to the original Office installation media such as : the original Office CD or Office Administrative Installation Point (AIP).

MS Office patches can be deployed in two different ways :

- Push patches to systems
- Synchronize systems with a patched Administrative Office Installation Point (AIP)

Pushing patches to systems

By choosing this option, you can directly deploy patches to the systems that have MS Office products installed and require patching.

Specify path to original Office installation CD

In order to install individual 'binary' or 'client' patches (that contain only the differences between the original file and the updated file), it is imperative that you provide a UNC path to the original Office installation CD used to install a specific version of Office. For example “\\winserver2\office\”.

Click the icon to alter the CD path or the credentials that are required to remotely access this UNC location. Ensure that the Security Manager Plus server is able to access the original installation media using the credentials supplied here, for Office patches to be deployed without any failures.

Note : The Office CD paths for each version of Office installed in your network, should be configured as a prerequisite from the **Admin** tab --> **Configure** --> **MS Office Media Location**.

Deploy full-file patches when possible

A 'full-file' patch is a complete installable which contains entire copies of updated files, and is usually much larger files than the 'binary' or 'client' patches.

If this option is checked, wherever applicable, full-file Office patches will be downloaded from the Microsoft site and will be applied to the systems requiring the patch. If left unchecked, only the client or binary patches will be downloaded and deployed with the help of the installation CD.

Note : Full-file patches are less likely to require access to the original installation media.

Synchronize systems with a patched AIP

What is an AIP ?

An AIP is nothing but an Office Administrative Install Point, which is a system that has an Office version installed and acts as a central source to synchronize the Office installations in other systems with the latest updates.

In order to achieve the synchronization, you will have to first create an AIP with a particular Office version, and then update the Office installations on target systems from this location. Ensure that the latest patches are installed on the AIP and then configure to update the remote Office installations from this AIP. This update process means re-installing all of Office on each system - everything on the AIP will get copied to the remote system. In other words, the AIP is nothing but a shared network resource of the necessary files, with special setup commands.

Refer to documents from the Microsoft site on how to setup an AIP and to install patches in the AIP.

Configuring the synchronization

In order to patch a particular version of an Office installation, you need provide **the full UNC path to Office AIP MSI file**. For example “\\winserverAIP\office\data.msi”.

Click the icon to alter the AIP path or the credentials that are required to remotely access this UNC location. Ensure that the Security Manager Plus server is able to access the AIP using the credentials supplied here, for Office patches to be deployed without any failures.

Note : The AIP paths for each version of Office installed in your network, should be configured as a prerequisite from the **Admin** tab --> **Configure** --> **MS Office Media Location**.

Viewing File and Registry Changes

The missing and availability status of a patch is determined by assessing these parameters :

- the file versions for all files installed by the patch
- the checksums for each file installed by the patch
- the registry key that is installed by the patch

These File change and Registry change details for a patch can be viewed by clicking on the Bulletin ID of a patch from many view and then clicking on the **File and Registry Changes** link from the pop-up window.

File Version and Checksum

Security Manager Plus compares the file names, their version numbers and checksum information from the vulnerability database, to those on the system that is being scanned. If any of the file versions and checksums on the scanned system are less than those stored in database, the associated security patch is identified as not installed or missing. If they are equal to or greater, the patch is considered as available.

The status is shown by the ✔ mark - to match the file version/checksum or **x** mark - to denote a mismatch. Note that the status info is available only when you view the Bulletin Details from the Asset Details view for a system and NOT from the Deploy Patches view.

Registry Checks

Though traditional patch detection mechanisms rely mainly on registry keys, Security Manager Plus uses a combination of checksum / file version checks and registry entries to determine the patch status. The registry key that must exist on the system being scanned, for the patch to be installed, is shown the Registry Check table.

The status is shown by the ✔ mark - to denote the presence of the registry key or **x** mark - to denote a absence of it. Note that the status info is available only when you view the Bulletin Details from the Asset Details view for a system and NOT from the Deploy Patches view.

Note that some patches might not make any registry entries to the system on which they are being installed. Therefore, the Registry Changes table maybe blank for some patches.

Reports

Predefined Reports

Once a scan is completed, analyzing the data can be quite a task. Depending upon the audience, there is often too much or too little data. The reporting framework in Security Manager Plus has been designed to provide the flexibility necessary to satisfy all parties. Various levels of technical detail are supported, allowing reports to be tailored for audiences ranging from upper management to system administrators.

Reports can be generated automatically from Security Manager Plus web-console in HTML formats and exported to PDF or CSV formats or even e-mailed to any number of recipients in these formats.

Not only are Security Manager Plus reports flexible, but they also provide the needed information efficiently in color-coded and graphical format. Vulnerability reports contain information to quickly understand what the problem is and provide supporting evidence that the system is vulnerable. URL links to vendor advisories and downloadable patches make remediation straightforward.

Reports List

Some of the Canned or Predefined Reports templates included, by default, in Security Manager Plus areas below.

Security Reports

- **Executive Report** - Provides a high-level summary of scan results in rich graphical formats. Used by the IT Managers to know the exposure level of the enterprise network to threats.
- **Remediation Report** - Provides a comprehensive report on the vulnerabilities with links to solutions for fixing the problem. Used by the System Administrators to prioritize vulnerability resolution.
- **Vulnerability Report** - Provides the complete list of vulnerabilities detected on the selected assets during the latest scan
- **Service Packs and Patches Report** - Provides a detailed report on the missing patches and service packs
- **Open Ports Report** - Displays a list of open ports detected during the latest scan on the selected hosts

Inventory Reports

- **Hardware Details Report** - Provides a report on the hardware inventory of the selected assets
- **Installed Software Report** - Provides a report on the software inventory of the selected assets

- **Windows Services Report** - Provides a detailed report on the list of Windows services detected on the selected assets
- **Windows Users and Groups Report** - Displays the list of Windows users and groups available on a scanned asset
- **File and Registry Changes Report** - Provides a detailed report on the Change Management aspects of Windows assets displaying file, folder & registry changes that are being tracked
- **Differential Report** - Compares and provides a detailed report on the difference in security postures of the network and assets on two different scans.

Compliance Reports

- **PCI DSS Compliance Report** - Provides a report which represents the compliance status of an asset or asset group with respect to the PCI DSS

Generating Reports

Reports in Security Manager Plus can be generated from here :

- Asset Details - View the Asset Details for an asset, click on the **Reports** button in this view and choose the type of the reports that you want from the list. The list is a collection of the aforementioned predefined reports as well as the custom reports.
- Asset Group - View the Asset Group Details screen for a particular asset, click on the **Reports** button in this view and choose the type of the reports that you want from the list. The list is a collection of the aforementioned predefined reports as well as the custom reports.
- Reports tab - Click on the Reports tab, choose a report title of your choice from the list and click on it, select the assets displayed for which you will need the report to be generated and click the Generate button.

Editing Report Templates

The predefined reports in Security Manager Plus are all governed by templates using which you can edit the properties (or reporting criteria) for any of the reports and save them either as the same template or as a new report template.

Note that for Executive Report & Remediation Report templates, only the reporting criteria can be edited but the report itself cannot be renamed.

E-mailing Reports

Reports can be e-mailed to the e-mail ID of your choice after you have generated the report. Click on the '**E-mail this Report**' link from the generated reports view, configure the To address and click on the 'Send' button to deliver the report. Ensure that you have your mail server settings configured from Admin tab to use this e-mailing functionality.

Configuring scan notification while scanning for assets

From the New Scan tab, click on the 'Notify on Scan Completion' checkbox and specify the the E-mail ID to which the report has to be sent and the type of report that needs to be sent. Once this particular scan completion, an e-mail will be sent with the status of the scan task with the report attached in PDF format.

Receiving Reports for Assets & Asset Groups after scan completion

Reports can be automatically sent after a scan is completed for Assets or Asset Groups. For this, you will need to visit the Asset Details view or the Asset Group Details view, click on the **Actions** button, choose the **Scan Notification** option and define the E-mail ID to which the report has to be sent and the type of report that needs to be sent.

Once this configuration is saved, every time a scan is completed for this asset or asset group, an e-mail notification will be sent with the status of the scan task with the report attached in PDF format.

Custom Reports

Customization is simple as Security Manager Plus provides report customization templates, whereby report sections can be added, removed or re-ordered. The amount of technical detail can be adjusted, allowing reports to be tailored for any target audience.

Security Manager Plus provides report customization templates that can be used to generate new custom reports or even modify existing reports. In order to create custom reports in any of the following two ways :

- Edit and save an existing report template (predefined) as a new report template, by altering the reporting criteria set in each template
- Creating a new custom report template by selecting your own reporting criteria

Editing existing report template

From the list of predefined report templates (except Executive & Remediation Report), you can edit the properties (or reporting criteria) for any of the reports and save them as a new report template. For this, click on the Reports tab --> click on the Edit Template link against the report type of your choice, alter the reporting criteria next and save the template by providing a different Report Title.

Creating new custom report template

For this, access the Reports tab --> click on the 'New Report' button here to view the report customization template. From here, select the report criteria of your choice and and save the new custom report template. All reports generated in this report's name will match the criteria specified.

The following are the details available to choose from in the template :

- Group Related Views : Select the type of graph & summary needs to be included in the reports
- Asset Related Views : Select information pertaining to assets like Host Info, Hardware & Software Details, Open Ports, Windows Services, Users & Groups, Missing Service Packs & Vulnerability Trend for the last x days
- Report Creation Details: Include name, designation or e-mail address of the generator of this report as well as the recipient of this report
- Vulnerabilities Details: Select the severity of the vulnerabilities to be reported like - Info, Low, Medium, High. Also mark if False Positive Vulnerabilities need to be reported.
- Missing Patch Details: Select the severity of the missing patches to be reported like - Unrated, Low, Moderate, Important, Critical.

PCI DSS Compliance Reports

What is the PCI DSS ?

The PCI DSS stands for Payment Card Industry Data Security Standard. It is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. It represents a set of rules that need to be adhered to by businesses that process credit cardholder information, to ensure data is protected. The PCI Data Security Standard is comprised of 12 general requirements designed to:

- Build and maintain a secure network
- Protect cardholder data
- Ensure the maintenance of vulnerability management programs
- Implement strong access control measures
- Regularly monitor and test networks
- Ensure the maintenance of information security policies

This standard is governed by PCI Security Standards Council https://www.pcisecuritystandards.org/

PCI DSS Compliance in Security Manager Plus

Security Manager Plus can help you weigh the effectiveness of your organization's PCI DSS compliance efforts. It can scan your network for vulnerabilities, determine if your network security is compromised and report whether the systems are compliant or not-compliant to the Payment Card Industry - Data Security Standards (PCI DSS). Security Manager Plus enables corporate networks adhere to PCI DSS, by assessing many key requirements of the PCI DSS and furnishing compliance reports.

PCI DSS compliance report presents the violations in your network from the requirements of Payment Card Industry (PCI) Data Security Standard (DSS). This report is generated using information provided by the "Payment Card Industry Data Security Standard" available at https://www.pcisecuritystandards.org/tech/index.htm.

PCI DSS Requirements covered in Security Manager Plus

- Section 2.1 : Always change vendor-supplied defaults before installing a system on the network(for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts)
- Section 2.2.1 : Implement only one primary function per server (for example, web servers, database servers, and DNS should be implemented on separate servers)

- Section 2.2.2 : Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices specified function)
- Section 2.2.3 : Configure system security parameters to prevent misuse
- Section 2.3 : Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access
- Section 4.1 : Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS are the Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS)
- Section 5.1.1 : Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.
- Section 5.2 : Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs
- Section 6.1 : Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.
- Section 6.2 : Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.
- Section 6.5 : Develop all web applications based on secure coding guidelines. such as the Open Web Application Security Project Guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following :
    - 6.5.1 Unvalidated input,
    - 6.5.2 Broken access control (for example, malicious use of user IDs),
    - 6.5.3 Broken authentication and session management (use of account credentials and session cookies),
    - 6.5.4 Cross-site scripting (XSS) attacks,
    - 6.5.5 Buffer overflows,
    - 6.5.6 Injection flaws (for example, structured query language (SQL) injection),
    - 6.5.7 Improper error handling,
    - 6.5.8 Insecure storage,
    - 6.5.9 Denial of service,
    - 6.5.10 Insecure configuration management
- Section 11.2 : Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
- Section 11.5 : Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly.
- Section 12.2 : Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).

Accessing PCI DSS Compliance Report

PCI DSS Compliance reports in Security Manager Plus can be generated from here :

- Asset Group - View the Asset Group Details screen for a particular asset group, click on the **Reports** button in this view and choose the report type: "**PCI DSS Compliance Report**" from the list.

  You can generate PCI DSS Compliance reports for all the sections defined in the PCI report template or choose the sections that you finish to generate the reports for from the drop down provided.

- Reports tab - Click on the Reports tab, from the Compliance Reports section, choose **PCI DSS Compliance Report --> Generate Report** and click on it, select the assets groups displayed for which you will need the report to be generated and click the Generate button.

Editing PCI DSS Compliance Report Template

The PCI DSS Compliance report in Security Manager Plus is governed by a template. Using this template you can edit the properties (or reporting criteria) for the report by choosing from the supported PCI DSS requirement sections and save them either as the same template or as a new report template. This can be done from **Reports** tab **--> PCI DSS Compliance Report --> Edit Template.**

Windows Change Management Reports

\In Windows systems, there are constant changes happening to files, folders and registry entries. Though most of these changes are due to normal processes like patch updates or system modifications, some of the changes could be the result of viruses or malicious hacker attacks that can introduce critical vulnerabilities to these Windows systems, that cause system downtime.

It therefore becomes imperative that some of the critical files, folders and registry entries are periodically monitored and the changes are kept track off during the normal vulnerability scan cycle. Change tracking and management aids largely in providing insights on the status of the entities (like files, folders or registry entries) and helps comparing against a preset baseline. This ensures IT Security staff that everything is in order and gives them control over vulnerabilities creeping into Windows systems due to unwarranted file/folder/registry changes.

In Security Manager Plus, Change Management of Windows machines is governed by Profiles. Profiles are nothing but custom templates that are defined by users to capture a list of important files, folders and registry entries that need to be periodically tracked for changes during every scan. Change tracking can be done on Assets or Asset Groups. Multiple profiles can be associated to the same asset or asset group.

For more information on working with profiles, refer to the Change Management section.

Windows Change Management Reports

Reports can be generated for assets or asset groups to display detailed change tracking and status of configured files, folders & registry entries of Windows systems. This can be done from **Reports** tab --> **File & Registry Changes Report** link.

Windows Change Management to meet PCI DSS Compliance

Section 11.5 of the PCI DSS has a clause which requires the deployment of file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly.

Security Manager Plus facilitates this and enables this clause of the PCI DSS to be met, by listing all assets that are monitored for critical system or content files. The PCI DSS Compliance report can be generated for assets or asset groups from **Reports** tab --> **PCI DSS Compliance Report**.

Re-branding Reports

The Reports generated in Security Manager Plus come with the default Security Manager Plus Logo on the top of the report and with a disclaimer text at the bottom (footer). Security Manager Plus users/consultants can alter these parameters (logo and disclaimer text) and re-brand the reports tosuit their enterprise needs or customer needs accordingly.

To re-brand reports, carry out the following :

- Visit the '**Reports**' tab
- Click on the '**Rebrand Reports**' icon in the Configure section
- Browse and supply the image file that will replace the current Security Manager Plus logo
- Enter the custom Footer text in the text area provided and save the configuration

Now, when you view any report from Security Manager Plus, it would be re-branded and will reflect the changes above.

Administration

Administration

Here you are provided with options to configure Security Manager Plus to conform to any specific requirement you might have, based on your enterprise network posture & to manage certain operations that are common. The various administration options are grouped under three major sections :

- Configure Settings
- Manage
- Actions

Configure Settings

Configure Settings

These are configurations that you must effect for smooth functioning of Security Manager Plus. These can be accessed from the **Admin** tab. Some of the configurations listed here are essential prerequisites to the vulnerability management operations from Security Manager Plus.

- Proxy Server Settings
- Mail Server Settings
- Trouble Ticket Settings
- Discovery and Scan Settings
- Vulnerability Database Updates
- Change Password
- MS Office Media Location
- Patch Store Location
- Patch Language Settings
- Log Level Settings
- Rebrand Reports

Setting Proxy

Internet access is essential to update the vulnerability database information from AdventNet site. In your enterprise network setup, you might need to go through a proxy server to access the internet. In this case, you can configure the username and password that is provided for internet access, from this screen : **Admin** tab **» Configure » Proxy Server**. This configuration is essential for the system in which the Security Manager Plus server is installed.

The different parameters to be configured are :

1. **HTTP Proxy Host** : Host name of the proxy server (eg: proxy-server)
2. **HTTP Proxy Port** : Port number at which the server is running (eg: 80)
3. **Username** to access the internet. This can be in the format : firstname.lastname@domain.com
4. **Password**

Specify values for these parameters and click '**Save**'. You can even test to see if a connection to the specified proxy server is established, by clicking on the '**Test**' button. You can also save the proxy settings and update the vulnerability knowledge base immediately from here, by selecting the 'Update Database' checkbox.

If you have not configured the above parameters correctly then the Security Manager Plus server will be unable to contact Central Repository Server, you will see the message "**Unable to contact Central Server**" posted in **Home** tab.

Removing proxy parameters

To remove the proxy configurations permanently from the system, click on the '**Remove**' button. This will mean that the Security Manager Plus server will not have access to the proxy server anymore, to connect to the internet.

Note: The 'Remove' button appears only after a configuration has been made.

.

Mail Settings

Mails can be sent to desired recipients to report completion of certain vulnerability assessment tasks like scheduled scanning of network resources for vulnerabilities, sending generated reports, sending feedback to Security Manager Plus technical support through Instant Feedback.

In order to enable this functionality, your enterprise's mail server parameters need to be configured in Security Manager Plus. You can access this configuration from : **Admin » Configure » Mail Server**

The parameters required for Mail Server Configuration are :

- **Server Name,** the SMTP (Simple Mail Transfer Protocol) server hostname/IP Address for the field
- **Port** (default port number : 25)
- Select the option **Requires Authentication** only if your mail server requires you to authenticate yourself, in which case you need to supply the **Username** and **Password**.
- **Sender E-Mail ID -** the email address provided will be the default from address which will be used while sending scan completed notification mails and sending vulnerability reports.

Setting the Trouble Ticket E-mail ID

Security Manager Plus can be configured to Generate Ticket on Scan Completion by sending mail to the supplied mail-id provided you have a Helpdesk system, like ManageEngine™ ServiceDesk Plus, in your enterprise which recognizes notification mails generated by Security Manager Plus and converts them to trouble tickets.

To configure the e-mail ID, visit the **Admin** tab **» Configure » Trouble Ticket Settings**. Specify the e-mail ID here and click the 'Save' button.

Discovery and Scan Settings

Discovery and Scan preferences affect the way Security Manager Plus performs network security assessment on target hosts. Listed below are various discovery and scan preferences that you as an administrator would require to configure/change based on network specific requirement .

Preference	Description
TCP Ping	Security Manager Plus uses the mentioned ports for discovering the network resources. **Default** : **21,23,80** **Scanning Dead Hosts** Select the '**Scan Dead Hosts**' check-box, in order to even scan hosts that do not respond to TCP ping on the ports specified above.
TCP Ports to Scan	Security Manager Plus performs port scanning to find open ports. Specify which TCP ports should be scanned during this process. Can perform port scan on all the 65,535 ports on a network device. **Default Setting : Standard Ports**
Set Timeouts	Influences the time taken for discovery and scan. **Default Setting for :** • **TCP Connection Timeout : 3000 milliseconds** • **TCP Read Timeout : 3000 milliseconds** • **UDP Timeout : 1000 milliseconds**
SNMP Settings	Used when performing SNMP based OS detection. **Default Settings:** • **Port to be Used : 161** • **Community :** (no entry) • **Number of Retries : 0**
HTTP	Directories scanned to check cgi scripts for HTTP vulnerabilities **Default Setting:** • **Directories to Scan for cgi scripts : cgi-bin**
User Account Detection	Used for setting username and password brute-force level When enabled, the Security Manager Plus will attempt to guess the

Preference	Description
	password corresponding to each detected username on each target host scanned. Select the level of brute forcing you prefer. Options provided are "Minimal" and "Exhaustive". **Default Setting : Minimal**
Configure Nmap Commands	Used for configuring the commands of the Nmap detection software. Detection using Nmap will take place based on the parameters specified here. Exercise caution before changing these settings. **Defaults Settings :** • **OS Detection : $nmap -PE -PA$portList --host_timeout=300000 -O $host** • **Standard Port Scan : $nmap -PE -PA$portList --host_timeout=300000 -sV $host** • **Full Port Scan : $nmap -PE -PA$portList -p1-65535 --host_timeout=300000 -sV $host** • **UDP Port Scan : $nmap -PE -n -PA$portList --host_timeout=300000 -sU -pU:7,9,13,19,37,42,53,67,68,69,111,123,137,138,161,177,445,500,512, 514,517,601,631,642,645,700,960,1900,2024,2049,4045,4500,32768,32771 $host** **For Windows localhost** • **Standard Port Scan : $nmap -PE -PA$portList -sT -sV $host** • **Full Port Scan : $nmap -PE -PA$portList -sT -p1-65535 -sV $host**

Vulnerability Database Updates

In **Admin** tab **>> Configure** section **>> Vulnerability Database Updates** view , you can mention the interval, **in hours**, at which you would like to check for latest vulnerability updates, after selecting the option '**Look for vulnerability database updates**'.

For related information visit Vulnerability Database Configuration.

Linux Package Management Scripts

Security Manager Plus can be used to detect missing Linux Packages and deploy them. SMP uses the target system's package management tool (up2date for RHEL, aptitude for Debian, yum for CentOS) to detect / deploy the packages that needs update.

1. **Scanning and deployment for RHEL/Debian/CentOS systems**
    1. Edit kickstart.sh and provide RHN Account details/Proxy Details. It is enough if these details are provided. Missing package detection and deployment are taken care in scan and install scripts.
2. **For other Distributions**
    1. Edit kickstart.sh and handle the commands that are needed to configure the package management tool
    2. Test kickstart.sh on a system and see if you are able to successfully configure the package management tool
    3. Edit scan.sh and handle the command that will fetch the list of missing packages
    4. Test scan.sh on a system and see if you are able to see the list of packages that needs update.
    5. Edit install.sh and handle the command that will install the missing package. Test the script
3. **Scan the Assets**
    1. The Scan Results view will list missing packages. You can deploy the missing packages from there.

Prerequisites

In order to use SMP's Linux patch deployment feature, you must ensure that you have a valid support and update subscription license with the different Linux distributions, **wherever applicable**. It is important that you provide the username/password details for a valid subscription account for the systems to be patched correctly.

Since SMP relies on the target system's package management tools mentioned above, it is important that all these tools are installed and made available for use on each of the target systems.

Change Password

The privilege to change the Login password for the Security Manager Plus web interface, is available for both Administrator and Normal user. You need to supply your 'Old Password' correctly followed by the 'New Password' and confirm the new password by repeating the same for 'Confirm Password'.

MS Office Media Location

To deploy Office patches, the locations of the Office original installation media (either the CD path or AIP path) must be specified for each version of Office installed. The configuration of this media location can be configured from here (**Admin** tab **» Configure » MS Office Media Location**).

Refer to Deploying MS Office Patches for more details on the different methods to install Office patches and service packs.

The table in this view lists all the Office product names (such as Office 2000, XP, 2003, 2007) and their respective edition types (namely Premium, Professional, Standard etc.). The Media Path and AIP Path columns allow you to add new locations or edit currently configured locations.

Configuring CD Path

Select the appropriate Office version and type and click on the '**Edit**' link against it, in the Media Path column. This will lead you to a screen where you can configure the location of the CD path/drive.

- CD Path - Specify the CD path of the system in which MS Office is installed. For example : \\winoffice\F\. Make sure that this path is **shared** from this system.
- Username - The username required to access this shared CD path. If the system is in a domain, specify username in the format : <domainname>\username
- Password - The password for the username above

After specifying the details, you can Save the configuration. The 'Remove Configuration' option allows you to completely remove the existing configuration.

Enabling/Disabling CD Path Share

Note : This is only for systems running Security Manager Plus Agents. If all your systems are managed remotely (without having a SMP agent installed), then you need not effect this configuration.

For the Security Manager Plus Agents to access this shared CD path, you need to have enabled *NullSessionShares* in this system by making a specific registry entry. This section in the screen will depict if the required share is enabled or not. Click on the 'Enable Share' button if disabled. This can be done only when the CD path has been configured and saved.

Test Connection

You can check if the Security Manager Plus server is able to access the specified CD path using the credentials supplied.

Configuring AIP Path

Select the appropriate Office version and type and click on the '**Edit**' link against it, in the AIP Path column. This will lead you to a screen where you can configure the location of the AIP path/drive.

- AIP Path - Specify the path of the AIP in which MS Office is installed. For example : \\winofficeAIP\D\. Make sure that this path is **shared** from this system.
- Username - The username required to access this shared AIP path. If the system is in a domain, specify username in the format : <domainname>\username
- Password - The password for the username above

After specifying the details, you can Save the configuration. The 'Remove Configuration' option allows you to completely remove the existing configuration.

Enabling/Disabling AIP Path Share

Note : This is only for systems running Security Manager Plus Agents. If all your systems are managed remotely (without having a SMP agent installed), then you need not effect this configuration.

For the Security Manager Plus Agents to access this AIP path, you need to have enabled *NullSessionShares* in this system by making a specific registry entry. This section in the screen will depict if the required share is enabled or not. Click on the 'Enable Share' button if disabled. This can be done only when the AIP path has been configured and saved.

Test Connection

You can check if the Security Manager Plus server is able to access the specified AIP path using the credentials supplied.

Patch Store Location

The patches and service packs downloaded from the internet are stored in a specific directory in the Security Manager Plus server. The default location is : *<Server_Install_Dir>/AdventNet/SecurityManager/store*.

If you wish to change the location of the directory in which the downloaded patches and service packs are stored in the server machine, you can specify the path in the field provided (**Admin** tab **» Configure » Patch Store Location**)

Patch Language Settings

Security Manager Plus has the support for scanning and patching non-English language Windows OS. The languages supported are listed below :

- Italian
- Dutch
- Russian
- Japanese
- Danish
- Portuguese (Portugal & Brazil)
- Finnish
- Czech
- Hungarian
- Swedish
- Chinese (Simplified, Traditional & Hong Kong)
- Norwegian
- Thai
- German
- Korean
- Arabic
- Greek
- Spanish
- Hebrew
- Polish
- Turkish
- French

The patches for all these languages are included in our patch database. By default, the patches displayed in the Patches Knowledge Base tab are the English-language Windows patches. If you wish to change this setting to a language of your choice, you can do so by select from the drop-down menu here or set this permanently from the '**Admin** tab **--> Patch Language Settings**' screen.

After the configuration has been saved, the Patches Knowledge Base tab will depict the Windows patches for the language selected here, each time you visit this view.

Log Level Settings

Log Level can be used to debug any issues or exception that you come across while working with Security Manager Plus. This is useful while sending support file to Security Manager Plus Technical Support Team, to analyze and resolve the issue faster. By default, the log level is set at **INFO** .

Re-branding Reports

The Reports generated in Security Manager Plus come with the default Security Manager Plus Logo on the top of the report and with a disclaimer text at the bottom (footer). Security Manager Plus users/consultants can alter these parameters (logo and disclaimer text) and re-brand the reports tosuit their enterprise needs or customer needs accordingly.

To re-brand reports, carry out the following :

- Visit the '**Reports**' tab
- Click on the '**Rebrand Reports**' icon in the Configure section
- Browse and supply the image file that will replace the current Security Manager Plus logo
- Enter the custom Footer text in the text area provided and save the configuration
- Now, when you view any report from Security Manager Plus, it would be re-branded and will reflect the changes above

Manage

Manage

These are some screens where you can administer & manage the different vulnerability management & patch management functions of Security Manager Plus.

- Credential Library
- Vulnerability Groups
- Patch Groups
- User Administration
- Change Management
- Agent Administration
- Download Windows Agent

Manage Credentials

Why do we need credentials ?

Any username/password combination that can be applied to a number of machines with administrator privileges can be pre-configured and stored in the Security Manager Plus database, these credentials are encrypted before storing them in the Security Manager Plus database. This credential will be used during scan to remotely login and identify the asset details, and perform various registry checks (in Windows) to identify related vulnerabilities and missing patches for the assets for which the scan is being performed.

Adding credentials

Go to tab **Admin » Manage » Credential Library**

- Click on the '**Add Credentials**' button from here
- Select the **Windows** radio button for configuring credentials for Windows systems or **Linux** radio button for Linux systems
- For**Credential Name** provide a unique name & **Description** of your choice.
- **User Name**, this user must have administrator privileges (Windows)
- Provide the correct **Password** used to authenticate to the remote system
- **Retype Password** to confirm.
- For Linux Credentials, provide both the Super User (root user) as well as Normal User details
- Click '**Save**' button to add these details.
- The newly added credentials will immediately appear in the '**Credential Details**' section of the page.
- You can delete the credentials, by clicking on the '**Delete**' icon.
  Public key-based authentication

  SSH keys (specific to hosts) can be supplied to authenticate **Linux hosts** before scanning. This is **optional** to supplying credentials with password.

  In order to use this functionality, under the Linux credentials --> Normal User Login Details, check the 'Public Key Authentication' check-box and provide the User Name and copy-and paste the SSH private key information in the Private Key text-area.

  Note :
  - This feature is optional
  - It is supported for SSH2 (version 2) protocol only

Vulnerability Groups

Vulnerability Groups are logical grouping of vulnerability knowledge base. You can form vulnerability groups from the existing list of vulnerability test cases based on risk level, vulnerability type or services affected.

View vulnerability groups

To view the list of all existing vulnerability groups,

- Visit the '**Admin**' tab.
- In this view, from the **Manage** section, click on **Vulnerability Groups** link
- This, by default, leads to the **Groups** tab, which displays a complete list of all vulnerabilities that is scanned by Security Manager Plus.

Actions from this view

- Scan this group - click on this link against each vulnerability group, to associate a hostname to scan based on this group
- Add vulnerabilities to group - click this link, to add more vulnerabilities to the group (from the All vulnerabilities list)
- Delete - click to delete this vulnerability group

Create custom vulnerability group

You can create your own custom vulnerability groups, from the existing vulnerabilities listthat Security Manager Plus maintains in its vulnerability database, based on type, risk and service affected. To create custom vulnerability group follow these instructions :

- Visit the '**Admin**' tab.
- In this view, from the **Manage** section, click on **Vulnerability Groups** link to come to the **Groups** tab
- Click on the '**New Group**' button
- From here, specify the Group name and Description and select the vulnerabilities to be grouped from the all vulnerabilities list in the table below
- Click 'Create' to create and save the new Vulnerability group

Viewing Group Details

You can view the information about each and every vulnerability associated to a vulnerability group, like Risk level, Vulnerability description, CVE ID. You can choose to view the different vulnerabilities

under each group by selecting the group name from the 'Show Vulnerabilities in' drop-down menu to the right corner of this screen.

Actions from this view

- Add to Group - you can select vulnerabilities from a chosen group and add them to any other group by clicking on this button and choosing the other vulnerability group name
- Delete from Group - you can discard vulnerabilities from this group by clicking this button

Viewing affected hosts & details for a particular vulnerability

Click on the **Short Description** link against each vulnerability to view the complete description of the vulnerability and its remediation solution if any, along with the list of hosts it affects.

Patch Groups

Patches belonging to a specific category, can be grouped together, so that they can be managed effectively. Each custom patch group will be represented by a name, and all patch management operations like adding downloading patches, deploying patches, adding patches to another group etc. can be done for this group.

For example, say you want to manage all the **Critical** patches for the Internet Explorer 6 software installed in your enterprise. You can create a group called '**IE_6_Critical**' and associate all patches for IE 6 from to this group. From the custom patch group view 'IE-6_Critical' you can manage these patches.

Follow these topics to work with Custom Patch Groups :

- Creating & viewing patch group
- Working with patch groups

Creating & viewing patch group

To create a patch group follow these instructions :

- Visit the '**Admin** tab --> **Manage** section --> **Patch Groups'** link. This view will display the list of Patch Groups created (if any)
- Click on the 'New Patch Group' button present in the screen
- Now from this configuration screen, enter the Group Name and the description of the patch group
- You can use the filter in the patches table to choose the OS type, patch language, product and service pack to list the patches
- Select the patches that you wish to group from the tabular list, and click the 'Create' button
- Your group will be added and will appear in the Patch Groups list
- The Edit icon adjacent to the group name can be used to edit the group details (name & description)
- You can add more patches to this group or even delete the patch group

Viewing patch group

- You can click on the Group Name text-link, to view the patches in that group
- From here you can, you can perform operations such as, displaying systems affected by the selected patch, downloading patches, adding patches to other groups, deleting patches from this group and deploying selected patch groups to system groups etc.

Working with patch group

The following are the operations that can be performed from Patch Group views :

- Displaying systems affected by a patch
- Deploying patches/ patch group to system groups
- Deploying patches to a system
- Downloading patches present in a group
- Adding patches to other patch groups
- Deleting patches from group
- Viewing patch specific information

Displaying systems affected by a patch

In order to find which systems are missing patches from the group; select the desired patches from the list and click on the "**Deploy**" button. This will display a screen wherein you will be able to deploy a patch to multiple systems (1 patch to many systems) and any number of selected patches to multiple systems (many patches to many systems), by choosing from the . Note that this list is based on the latest scan results in Security Manager Plus.

For more information on installing patches, refer Deploying Patches section.

Deploying patches /patch groups to system groups

To deploy patches in a group to system groups or to deploy entire patch groups to system groups, select the patches and click on the '**Deploy to Group**' button. This will bring you to a screen from where you can select from a list of system groups to which the chosen patches need to be applied. More than one system group can also be selected.

Deploying patches to a system

Click on any patch name in the group list and you will be led to a screen where the systems/assets that miss this patch, will be listed. From here, you can deploy the patch to these assets.

Downloading patches present in a group

To download the patches in the group (if they are not already available in the Security Manager Plus server), select the patches of interest and click on the "**Download**" button.

Adding patches to other patch groups

Patches in an existing patch group can be included in other patch groups, by clicking on the '**Add to Group**' button.

Deleting patches from group

In order to delete patches from a particular group, select the patches and click on the '**Delete from group**' button.

User Administration

Working with user information, creating new users and deleting users is a privilege that is allowed for an admin user. Normal users will not get to see the User Administration screens.

Under User Administration, you can :

- View User List
- Create new user
- Import user from AD

Viewing User List

The screen displays a list of users that are configured to access the Security Manager Plus web administration UI.

The username 'admin' cannot be deleted from the system. The password for 'admin' can be reset by using the **Change Password** option.
Deleting users - In order to delete users, select the login names from the users list, and click on the 'Delete' link.

Create New User

Any user with administrator privileges set for the Security Manager Plus system, can create new users. To do so, click on the '**Add New User**' button and, specify the following parameters :

- Login Name - user name, can be any unique name e.g. dbeckham
- Password - password for logging in. This can be the same as the login name, but it recommended to specify a different password (select the appropriate radio button)
- Confirm Password - re-enter the same password for confirmation
- Access Level / User Group - select from 2 options (Administrator or Normal User)
- E-mail address - The email address provided will be used :
    1. as the default from address in the instant feedback form, for that particular user login.
    2. in case you forgot your password. A new password will be generated and sent to this mail-id.

Click on the '**Save**' button to add the user. This configuration will appear in the User List in the previous screen.

Import User from AD

The users present in the Active Directory (AD) of your Domain Controller can be allowed to login to the Security Manager Plus web interface. For this, you will first need to import the user from the AD into Security Manager Plus and then activate the AD authentication for login.

To import user, click '**Import User From AD**' button, specify the following parameters :

- Domain Name: name of the Windows domain where the AD server is present. Choose from existing domain list or add a new domain
- Domain Controller : name of the domain controller/AD server machine which has the Active Directory, from which you want to import users
- User Name : the user name (with administrator privileges) to login to AD
- Password : the password for the above user
- Users to Import : list of **valid** users from AD that needs to be imported into Security Manager Plus

Click on the '**Save**' button to add the user. This configuration will appear in the User List in the previous screen.

Activating/Deactivating AD authentication

The Active Directory Authentication will be Activated after you finish importing at least one user from AD using the above steps. You can disable this by clicking on the **Deactivate** button.

Note :

- This feature is available only when the Security Manager Plus Server is running on a Windows system.
- When AD Server authentication is enabled, you will be able to login to Security Manager Plus only using the valid AD user names/password that have been imported. Logging in using the other user names created manually or even by the default user names (admin & guest) will not be possible.

Change Management Profiles

Creating Change Management Profiles

In order to create a new change management profile, visit the **Admin** tab --> **Change Management** link. From here, you can click on the 'New Profile' button, and specify the following information :

- specify the name of the profile
- specify the description of the profile
- configure the e-mail ID to which a notification mail has to be sent if there are any changes detected during a scan
- specify option to generate a trouble-ticket if changes are detected (applicable only if Trouble ticket e-mail ID is configured from Admin tab)

Associating Entities to a Profile

Once a profile is created, you can associate files, folders and/or registry entries to this profile. These can be associated by visiting the Profile configuration screen and adding the entries by clicking on the respective 'Add' button. Each entity can be added to the profile either by typing the file/folder/registry path manually and or by importing paths from a text file.

Every entry can be clicked upon to check for which all assets/hosts that particular entry is being tracked for. You can also delete a particular entry from here if it is not needed anymore in the profile.

Actions on Change Management Profiles

Once a profile is created, it gets listed in the Change Management Profiles screen. From here you can perform the following tasks:

1. Create a new change management profile.
2. Add File, Folder and Registry entries to the Profile.
3. Associate the profile with Assets or Asset groups
4. Scan the Assets or Asset groups periodically to detect changes
5. Enable or Disable the created profiles. Files, Folders and Registry entries in "Disabled" profiles will not be scanned for changes

Associating a Profile to an Asset or Asset Group

This can be done in two ways:

- from the Change Management Profiles screen (Admin tab --> Change Management link) - clicking on the appropriate Action icon and selecting the assets/groups

- from the Asset Details or Asset Groups view --> Actions button --> Change Management link

During an asset scan or asset group scan, the change detection mechanism will be applied and all the parameters will be compared against the baseline and status will be reported.

Parameters tracked when detecting changes

Here are the parameters that are applied for change detection on these entities. These changes can be viewed from the Asset Details view --> Changes tab, by clicking on the entry path being tracked in the associated profile. All values are compared against a baseline and the change is reported.

The Inventory dashboard also displays a high-level view of the assets & entities which have undergone frequent changes.

File changes

- File size
- MD5 Checksum (change in content)
- Modified time
- Created time
- Last accessed time
- Vendor
- Encryption status
- Hidden status
- Compression status
- System status

Folder changes

- Folder size
- No. of files
- No. of folders
- Modified time
- Created time
- Last accessed time
- Encryption status
- Hidden status
- Compression status
- System status

Registry Changes

- Current value of registry entry
- Baseline value of registry entry

Setting Baseline

By default, the details obtained from a File or a Folder or the values for a Registry key after the first scan on an asset, will be treated as the Baseline value for various parameters being tracked. However, this can be altered at any time and a baseline can be set to be a changed value. In order to alter the baseline, you can click on the Baseline icon in the "Set as Baseline" column for the entry which has a changed status (red icon) if you think the change is appropriate. From the subsequent scans, this will be treated as the Baseline and compared against.

Setting baselines is applicable for every entry under each category (files, folders or registry).

Agent Administration

Consider a scenario in your enterprise network, wherein you have a number of Security Manager Plus agents installed and you want to change some agent properties globally in all agents or want to upgrade the agents to the latest version available. Carrying out these operations manually in each agent across your network is going to be tedious. To eliminate this manual procedure, Security Manager Plus has the provision to administer the agents, from the web interface of Security Manager Plus.

Visit the **Admin** tab and click the **Agent Administration** link. From here you can see the agent systems. Following are the options available in this screen.

- Configure Agents
- Upgrade Agents

Configure Agents

Security Manager Plus Windows Agent settings can also be configured from the web interface of Security Manager Plus. There are a set of parameters each for both HTTPS mode and SSL/TCP mode of the agents that can be altered from the '**Configure Agent**' option, available in the **Actions** button in the Asset Details.

Note

- Agent Configuration Information will be displayed only for systems in Agent Mode.
- Configurations effected from this screen cannot be scheduled. They will be applied immediately.
- Global configurations (for all agent systems present in the setup) can also be effected in a single-shot from the **Admin** tab --> Agent Administration screen.

These are the agent properties that can be configured from the System Configuration screen :

- Agent Details - all information pertaining to the agent installation
- Server Details - Security Manager Plus server related information required for the agent

An e-mail can be sent to the desired e-mail ID to receive notification on the Agent Configuration task completion.

Agent Details

1. Agent Mode

There are 2 modes in which Security Manager Plus Agents can function - HTTPS mode & SSL/TCP mode - depending on your enterprise requirements. The mode in which the agent is installed and functioning is identified by the 'Agent Mode' parameter under the Agent Details section. You can change the mode if required and configure the associated parameter as below :

In the HTTPS Mode, you can configure the Poll Interval - the time interval in which the agent polls the SMP server for tasks to be executed. The value is in minutes and the default value is 5.

In the SSL/TCP Mode, you can configure the TCP port on the agent machine through which the SMP agent communicates with the Security Manager Plus Server. The default value is 9005.

2. Log Level

This is the severity level of the logs in the SMP agent application. The default value is : Off. The other permissible values you can choose from are: Error, Warning, Info, Debug - in the increasing order of severity.

Server Details

Warning: Please exercise caution before you alter these parameters.

1. Server Name

It is the System name or IP address of the server machine to which the agent communicates.

2. Server Web Port

The web port on which the SMP server communicates to the agent. Note that the SMP server now runs in the HTTPS mode. Default 6767.

3. Server TCP Port

The TCP port on which the SMP server communicates to the agent. Default is 9004.

Upgrade Agents

Upgrading the Security Manager Plus agent software 'manually' every time a new version of the agent is available in the Security Manager Plus server, is a tedious task. To eliminate this manual procedure, Security Manager Plus has the provision to automatically upgrade the agent software versions, from the web interface of Security Manager Plus.

Windows agent updates are available as a part of the vulnerability database updates. Applying updates is similar to applying a patch on the system. The update will be downloaded from the Central Repository Server and stored in Security Manager Plus. It will then be sent to the agent with instructions to upgrade itself.

When a newer version of the agent is available with the server, it will be identified (on scanning) and displayed as a missing patch in the Scan Result screen implying that the agent in a particular system needs to be updated. From here, a simple select-and-click will take care of upgrading the agent version to the latest.

Upgrading All Agents at once

This provision is available in the web interface from the **Admin** tab --> **Agent Administration** screen. The 'latest' agent version is displayed on the top of the screen in the 'Agent Update Version Info' table. All agents need to be in sync with this version to function effectively.

The system table displays the following information :

- name of the systems in which the agent is installed
- the "version update status" of the agent - whether it is *up-to-date* (green tick) with the most recent version or *needs update* (red cross)
- the operational state of the agent - whether the agent is running or offline
- the version of the agent that is currently installed on the system

You can select the agents which have 'Update Status' showing 'Needs update', and click on the 'Upgrade Agents' button. Ensure that the system is up and the agent is running before you carry out the update. All the agents can also be simultaneously updated by selecting the entire table and clicking this button.

Once the upgrade request has been sent, revisit this screen after a while to view the status of the request. You will need to rescan a Windows systems to check if the agent update patch has been applied successfully.

Note :

- The global Windows Agent Configurations will always have default values. Any changes made will however be effected in all agents selected. Subsequent visits to the configuration will still show default values only; as it is a generic configuration screen.
- Agent Configurations and Updates can be scheduled from Agent Administration screen

Download Windows Agent

Windows Assets can be managed in the agent-based mode as well. You will need to download the Security Manager Plus agent, install it on the target systems and then manage them from the web console. To download the agent, visit **Admin** tab and click on the **Download Windows Agent** link.

You can either copy the agent installable on each of the target machines or access the Security Manager Plus web interface, visit the Admin tab and download the agent on each machine.

Installing Security Manager Plus Agents in bulk

Agents can be installed in a silent mode without user intervention on many target machines at a time. There is a procedure to create a silent installation and use a logon script to install multiple agents. Contact support@securitymanagerplus.com for instructions.

Actions

Actions

This section presents the screens or views from where you can perform bulk operations. There are also options to view lists of tasks, patches and service packs.

- Deploy Patches
- Deploy Service Packs
- Diagnosis
- Task Status
- Stored Service Packs
- Stored Patches
- Vulnerability Knowledge Base
- Patches Knowledge Base

Deploy Patches

From **Admin** tab --> **Actions** section --> **Deploy Patches** screen, you can view all the missing Windows patches in your network. This list here is dependent on the number of systems present in your Security Manager Plus setup and the last scan result.

From this view, you can see the following information :

- Severity - severity of the missing patch namely Critical, Important, Moderate, Low & Unrated
- Patch Name - the name of the patch that is missing. Clicking on the patch name, will show the complete details of the patch along with the list of assets in which this patch is missing
- Host Count - number of hosts for which this patch is missing
- Bulletin - the bulletin ID in which this patch is associated. Clicking on the bulletin name
- Reboot status - whether reboot of the system is required after installation of this patch or not
- History - a historical report of the patch, as to which all assets attempt has been made to install the patch, at what time & what is the status of the installation

Deploying Patches

You can select the patches of your choice from here and install them at one go on all the systems that miss the selected patches. For this, select the patches and click on the '**Deploy Patch**' button. The view will show you a list of systems under each patch. You can choose the systems from here and then deploy.

Deploy Service Packs

From **Admin** tab --> **Actions** section --> **Deploy Service Packs** screen, you can view all the missing service packs in your network. This list here shows all the Windows products for which service packs are available. From here you can choose the specific product and service pack number which is supported and click on the '**Deploy**' button.

This will bring up a list of Windows systems in which the selected SP is missing. You can select the systems or deploy the SP on all the listed systems. This list is dependent on the number of Windows systems present in your Security Manager Plus setup and the last scan result.

From this view, you can see the following information :

- SP Name - the name of the SP that is missing. Clicking on the SP version from the name, will show the complete details of the SP
- Download status - whether the SP is downloaded already into Security Manager Plus or not
- Release date - the date at which this SP was released by Microsoft
- History - a historical report of the SP, as to which all assets attempt has been made to install the SP, at what time & what is the status of the installation

Downloading SPs

Since SPs are files of huge size, there is an option to download SPs separately. For this select the SP and click on the 'Download' button. You can either do an instant download or schedule the download for a later time.

In case you have downloaded an SP earlier (directly from the website) and stored it in your system, and would like to use the same to be deployed in the systems which miss the SP, you can very well do so. Ensure that you have downloaded the right version of the SP and follow the instructions that are displayed in this screen.

- Copy the SP that has been directly downloaded from the website URL, to the patch store directory, present in the Security Manager Plus server machine
- Rename the file in the format specified on this screen
- Click on the link displayed, to verify that the SP file has been saved correctly and to update the service pack store

Diagnosis

You can troubleshoot the system environment for any system to verify if the conditions are conducive for scanning it, using the **Diagnose** function. From the **Admin** tab --> **Diagnosis** link, you can enter the system names, select the credentials for the systems, specify the Telnet and SSH ports (for Linux machines) and click on the **Diagnose** button in the bottom of the screen.

Security Manager Plus's Diagnosis of the System environment includes performing the following tests on the target machines :

System Checks for the system where Security Manager Plus is running

- For Linux systems, if *samba-tng* package is installed or not (this package is important for a Security Manager Plus server running on Linux to communicate with Windows systems)
- For Linux systems, if root privileges are available for Nmap to run
- If there is internet connectivity - to access the Security Manager Plus vulnerability database from our site and to download patches from vendor websites
- If there is a firewall present

Other tests on target systems

- Ping - a 'ping' command is executed from the Security Manager Plus server machine to the target machines, so see if they are alive in the network
- OS Type - detects the OS information of the host being diagnosed
- Registry Service check (*Windows machines only*) - To check if the registry service is running in the target machine and if the service can be accessed remotely from the server machine. Also to check if the credentials supplied (username and password) have enough privileges (read administrator rights) to access the registry
- Shares check (*Windows machines only*) - To test if the ADMIN$ share is enabled in the target machine
- Service creation check (*Windows machines only*) - To test if a service can be created in the remote machines to carry out patch detection operations
- Login Test (*Linux machines only*)- To check if the credentials supplied (username and password) for the Linux machines can be used to successfully login to the target machines and if the telnet & ssh services are running in the specified ports

The results of these test give an idea on the environment of the target system. If any of the tests fail, scanning may fail. You should take corrective measures to address the issues, and retry system scanning. Note that you can enter multiple systems and diagnose them at one go.

Task Status

Task Status presents a list of all the recent vulnerability management tasks that have either been performed or scheduled for execution. To view the task details and the task status of all operations, visit **Admin** tab » **Task Status**

Each operation is associated with a unique task ID which forms an easy reference at any point. From this view, you can get to know the creation time of each task, its completion time, the type and status of the task and information message.

For more info on each task, click on the Task Name link in the Task Type column. This will lead to the '**Task Details**' with specifics about the particular task. You can filter based on the Task Type from the drop-down menu provided above the table.

Deleting Tasks

The tasks listed in the Task Status view can be deleted on selecting particular tasks from the list and clicking the 'Delete' button. This will remove all references of the task from the system - be it a 'Completed' Task or a 'Scheduled' Task.

Stored Service Packs

To view the list of service packs downloaded from the internet and stored in the Security Manager Plus server, visit the **Admin** tab and click on the '**Stored SP List**' link. This list displays the SP names, File size, Release Date and other related information.

To delete the SPs from the Security Manager Plus server, select the desired SPs and click the '**Delete Service Packs**' link. Doing so will change the Download Status column against the corresponding patch in the views where service packs are displayed.

Stored Patches

To view the list of patches downloaded from the internet and stored in the Security Manager Plus server, visit the **Admin** tab and click on the '**Stored Patch List**' link. This list displays the patch names, Bulletin ID and other patch related information.

To delete the patches from the Security Manager Plus server, select the desired patches and click the '**Delete Patches**' button. Doing so will change the Download Status column against the corresponding patch in the other views where patches are displayed.

Vulnerability Knowledge Base

The **Vulnerability Knowledge Base** section in the **Admin** tab, contains a complete list of the vulnerabilities and related information. This list gets updated regularly with latest information available in the **Central Repository Server** depending on your vulnerability updates cycle.

This view contains a list of vulnerabilities that will be scanned for, during a Vulnerability Scan. You can search the vulnerability knowledge base , based on **Risk, Service, Description** or **CVEID**. Clicking on the Description link will give you more details about the vulnerability and the hosts that are affected by the vulnerability.

Patches Knowledge Base

The **Knowledge Base** section in the **Admin** tab, contains a complete list of the vulnerabilities and patches information. This list gets updated regularly with latest information available in the **Central Repository Server** depending on your vulnerabilityupdates cycle.

This view contains a list of patches that will be scanned for, during a Vulnerability Scan. You can search the patches knowledge base, based on **Severity, Title, Bulletin** or **Patch To Install**. Clicking on the Description link will give you more details about the patch and the hosts that miss this patch. You can even deploy this patch on these hosts using the Deploy patch button from here.

The patches knowledge base can be sorted based on the Patch Language from the filter provided above the table.

Contacting Technical Support

In case you have any technical difficulties in using the Security Manager Plus software, any queries on the product functionality, features that you would like to see in the product or any other concerns, you can e-mail the Security Manager Plus Technical Support team at : support@securitymanagerplus.com

Using the Feedback Form

Every page in the Security Manager Plus Web UI has a link named "Feedback". Clicking this will invoke a mail submission form using which you can post any feedback on the product. An e-mail will be sent to Security Manager Plus's support mail ID.

Using the Support tab

You can also visit the **Support** tab, from the UI and use the facilities available there to contact Security Manager Plus Technical Support team. The various options available are :

- Support File Creation - When you click the **Create** button, the latest support information file (zip file containing requisite log files etc.) will be created. You can send this file by e-mail to support@securitymanagerplus.com to enable us debug the problem
- Need Support - Submit a support request form in our website (internet access required)
- Troubleshooting Tips - Refer to the troubleshooting tips section in our website to find a possible solution to the problem you have encountered (internet access required)
- User Forums - Visit the Security Manager Plus technical forum in our website to discuss with other Security Manager Plus users (internet access required)
- Need Features - Submit a feature request form in our website (internet access required)
- Toll Free Number - Call +1-888-720-9500 for telephone support

Security Manager Plus Information

In the Support page, you can also view some diagnostic information to assist you in reporting problems with necessary details.

* JVM Memory Information of the Security Manager Plus server
* Security Manager Plus server system information
* Security Manager Plus server installation information
* General Product Information like version number and build number

Troubleshooting Tips

Please refer to http://manageengine.adventnet.com/products/security-manager/troubleshoot.html for the latest Troubleshooting Tips.

Installation/ Un-Installation and Server Start-Up / Shutdown

1. **When I uninstall the product in windows, some folders are not getting deleted.**

Reason	Solution
This usually happens when you try to uninstall the product immediately after you have shutdown the Security Manager Plus server.	Ensure that you uninstall the product only after the Security Manager Plus MySQL Server instance (*mysqld-nt.exe* process in Windows Task Manager) has been terminated completely after the server shutdown.

2. **Server-startup fails.**

Reason	Solution
The Windows installation directory contains space.	Please ensure that the Windows directory in which Security Manager Plus is installed doesn't contain any space , for example, do not install Security Manager Plus in **C:\Program Files**.
During the previous run of the Security Manager Plus server if you had terminated the server abruptly or there was an unclean shutdown then some of the server processes would not have been terminated and the MySQL server instance would continue to run in the system. You will notice a message "*Trying to start MySQL server failed*" in the console.	Forcefully terminate the MySQL Server instance (*mysqld-nt.exe* in Windows, *mysqld* in Linux).
Does the system running Security Manager Plus server have a Personal Firewall enabled? Security Manager Plus server will open available ports during Server Startup and if the firewall does not allow opening of ports, then Server startup will fail.	Disable the Personal Firewall.
Any other	In Windows, use the 'Show Startup Logs' option from the Security Manager Plus System Tray Icon, to view the startup logs and see if you can find the cause for the failure. Also zip the **logs** directory from <Security Manager Plus_Home> and send it to support@securitymanagerplus.com so that we can analyze and get back to you.

3. **(In Linux) When i start the server it shows "java.io.FileNotFoundException .. (Permission Denied) ?**

Reason	Solution
The Security Manager Plus Server may have been initially started in super user mode, then restarted in the normal user mode.	Run the server only in the normal user mode. Give ownership to all the files in the server as shown below : *chown -R <username> <groupname>* .

4. **When I start the Security Manager Plus Server, I am getting the following error "Error: write on output file failed err=28" ?**

Reason	Solution
This error occurs if there is not enough Hard Disk space	Security Manager Plus server installation and start-up requires a minimum of 200 MB Hard Disk space.

Web Client

1. **I am unable to access Security Manager Plus Server through the Web Client. Why ?**

Reason	Solution
Security Manager Plus Server not started	Start the Security Manager Plus server from the Task Tray Icon or Start Menu --> Programs --> ManageEngine Security Manager Plus 5 --> Start Security Manager Plus Service (Windows) or by executing **Security Manager Plus.sh start** from 'bin' directory (Linux)
Wrong URL	Make sure that the correct URL is used to connect to the server, namely,**http://<Security Manager PlusServerHost>:port_number/** (e.g. http://localhost:6262/) The default web server port is 6262, provided this default port had not been changed during server startup . **Note :** Security Manager Plus server and Web Client also communicate through **https** via port 6767 (default).
You did not accept the Security Certificate while connecting to the server in Secure Mode	You must accept the security certificate that is presented to you while connecting to the Security Manager Plus server. This is perfectly safe and necessary for the Web Client to access the Security Manager Plus Server.
The trial period of the Security Manager Plus Server would have expired.	Restart the Security Manager Plus server to move to Free Edition or contact sales@adventnet.com for obtaining the Annual Subscription Professional License.

2. **Why does my Web Client user interface looks crippled?**

Reason	Solution
Incompatible Browser	Refer to the Security Manager Plus system requirement , and see whether your browser is supported.
JavaScript not enabled	JavaScript has to be enabled in your browser for you to work with Security Manager Plus Web Client.

3. **I am unable to perform any activity in Security Manager Plus Web Client. Why ?**

Reason	Solution
You might have logged in using an account that has limited privileges to Security Manager Plus Server operations. For example, guest is an account that has limited privileges.	To work with or configure the product, log in as 'Admin' user. For more information on user account privileges, refer to the User Administration section .

4. **I am repeatedly seeing the login screen. Why ?**

Reason	Solution
Your browser does not accepts cookies.	Cookies should be accepted by your browser in order to communicate with the Security Manager Plus Server seamlessly.

Asset Discovery

1. **Security Manager Plus is unable to discover my network assets. Why ?**

Reason	Solution
Assets not reachable	Ensure that the IP address or host names are correct and are reachable through either TCP or ICMP ping. You can configure the ports to be used for TCP ping in the Admin page (Admin » Discovery and Scan).

2. **OS detection is not happening correctly in Linux systems. Why ?**

Reason	Solution
Super User privileges is needed for NMap based OS detection.	Ensure that NMap executable is available in PATH and is given Super User privileges.

Scan

1. **Scan does not work, scan result shows 0 vulnerabilities**

Reason	Solution
Vulnerability Database is not up to date	Update your Security Manager Plus Server vulnerability database with the latest vulnerability signatures from the Central Repository Server hosted in AdventNet site, by clicking the "**Update Vulnerability Database Now**" (Admin » Vulnerability Database Updates) .
Scan times out	Set proper timeout values for Security Manager Plus to discover and scan your assets, based on your network configuration and load. You can Set Timeouts in the **Discovery and Scan** view of the Admin page (Admin » Discovery and Scan Settings).

2. **Vulnerability results for scans performed for windows machines shows "No records found" for Missing Patches. Why ?**

Reason	Solution
Windows administrator credentials not supplied before performing the scan	Credentials are needed for detecting windows registry mis-configurations and for detecting missing patches. Provide the credential details in the **Credential Library** view of the Admin page (Admin » Credential Library).
Samba-TNG software is not installed	If you intend to run the Security Manager Plus Server in Linux OS, ensure that Samba-TNG software (version 0.4 and above) is installed. This software facilitates communication between the Linux server and target Windows machines. Useful while identifying missing patches in target Windows machine. You can download the software from : http://download.samba-tng.org/tng .

3. **Sometimes the scan is taking a lot of time to complete and at times it does not complete at all?**

Reason	Solution
Scan Timeout	This happens if the Scan Timeout has been set with high values. For default values refer Discovery and Scan - Timeouts (Admin » Discovery and Scan Settings).
All Ports option is selected for TCP Ports to Scan	
Scanning large number of IP's / hosts in a single scan	Limit the number of IP's / hosts that is scanned per scan.
Performing Exhaustive brute-force level (Admin » Discovery and Scan) checks while scanning	
Server exceptions	Check the log files available under : **<Security Manager Plus_Home>\logs** directory. If you find any exceptions please send the log files to support@securitymanagerplus.com from Support tab --> 'Support File Creation' link.

4. **Scanning a Linux system fails to show missing patches with message "ssh version incompatibility", though SSH is installed and running in the system**

Reason	Solution
The Linux system you are trying to scan supports only **sshv2** protocol	To scan Linux systems that support **sshv2** protocol, carry out the following steps and then scan the system from the UI : • Download *sshtools-j2ssh-0.0.4-alpha-bin.tar* file from the URL : http://prdownloads.sourceforge.net/sshtools and extract • Place the **jar** files present in the '**lib**' directory obtained in the extraction, in <Security Manager Plus_Server_Install_Dir>/lib directory • Restart the Security Manager Plus server

Others

1. **Got the following error while updating the vulnerability database : "Error occurred while updating the Database - Error Message : Could not contact the Central Server".**

Reason	Solution
Security Manager Plus Server machine has no access to the Internet	The Security Manager Plus Server machine must have access to the Internet for it to download the latest vulnerability signatures from the Central Repository Server hosted in the AdventNet site.
Proxy Settings not configured	If you access the Internet through a Proxy Server, then you need to configure the proxy server details in Proxy Settings view of the Security Manager Plus Admin page (Admin » Proxy Server). Ensure that all the required proxy server parameters are provided correctly.

Frequently Asked Questions

What is Security Manager Plus ?

Security Manager Plus is a vulnerability scanner and reporting software for detecting and assessing network vulnerabilities across heterogeneous networks comprising servers, workstations, laptops, routers, switches and other network entities.

What are the components of Security Manager Plus ?

Security Manager Plus consists of the following primary components

- External Vulnerability Aggregator
- Central Repository Server
- Security Manager Plus Server
- Security Manager Plus Agents (optional)

What type of systems and services does Security Manager Plus scan ?

• Web Servers • Database Servers • Application Servers • RPC Services • CGI Scripts • FTP • DNS • POP3 • SNMP	• SMTP • IMAP • SSH • SSL • Proxy Servers • UDP • TCP/IP • Registry	• User Accounts • Dos Vulnerabilities • SQL Injection vulnerabilities • Trojans and Viruses • Switches • Routers • Windows • Linux • VPNs and many more...

How does the Security Manager Plus Server installed in the enterprise, be in sync with the latest vulnerability and patch information ?

The Security Manager Plus Server will periodically download the the latest vulnerability and patch information published in the Central Repository Server hosted in the AdventNet site, and use the information as a baseline for its vulnerability assessment operations.

Is Security Manager Plus a Patch Management software ?

Yes indeed. Security Manager Plus is primarily a vulnerability assessment and reporting software with patch management capabilities. It does help you in identifying & deploying the missing patches for

Windows operating systems. Supported Windows operating systems are : Windows Vista, Windows 2003 Server, XP Professional, 2000 Server and Professional, NT Workstation and Server and applications are : IIS, IE, SQL Server, MDAC, Media Player, .NET Framework, MSXML, DirectX and MS Office.

How many different types of vulnerabilities do you detect ?

Security Manager Plus 5 currently performs scans for more than 3500 vulnerabilities and missing patches, and this number keeps growing as and when we update our Central Repository Server with the latest vulnerability signatures.

What impact will Security Manager Plus have on my network?

Security Manager Plus is designed to minimize both the scan time as well as the network bandwidth it uses. Thus, its impact on network traffic load is minimal.

Should the machine in which Security Manager Plus is installed have a Internet connection ?

Yes. The Security Manager Plus server machine must have access to the Internet for it to download the latest vulnerability signatures from the Central Repository Server hosted in the AdventNet site.

Is Security Manager Plus host-based or network-based ?

Security Manager Plus is a network-based vulnerability assessment and reporting software that scans for vulnerabilities on all networked resources, including servers, network devices (e.g. routers, switches, etc.), and workstations. Security Manager Plus can assess any device that has an IP address.

How to create and use a Custom Security Certificate in Security Manager Plus?

Security Manager Plus, by default, comes with its own AdventNet Security Certificate. If you wants to create and use your own Certificate, the following are the steps to do.

The following are the Steps for creating a Certificate using the '**keytool**', a program that is available in JDK.

1. **Step 1**

   Type the following command:

   keytool -genkey -alias tomcat -keyalg RSA -dname 'CN=<domain name>, OU=<Organizational Unit>, O=<Organization>, L=<City Name>, S=<State Name>, C=<Country>' -validity <number of days> -keypass <keypassword> -storepass

<storepassword> -keystore server.keystore

E.g.,
keytool -genkey -alias tomcat -keyalg RSA -dname 'CN=demo.SecurityManagerPlus.com, OU=AdventNet Inc., O=AdventNet Inc., L=Pleasanton, S=CA, C=USA' -validity 365 -keypass demo -storepass demo -keystore server.keystore

2. **Step 2**

   Copy the 'server.keystore' file to **<Security Manager Plus_Home>/conf**

3. **Step 3**

   Edit the file **<Security Manager Plus_Home>/conf/server.xml** and change the keystorePass value to the one created above. For the above example, keystorePass="demo"

4. **Step 4**

   Restart the Security Manager Plus Server.

What is the Licensing Policy for Security Manager Plus ?

We provide a Professional Edition download that becomes a limited free edition after 30 days of evaluation, unless a registeredlicense key is purchased. This registered license key is valid for a year from the date of purchase (Annual Subscription) beyond which it becomes a limited free edition.

The limited Free Edition has all the functionality's provided by the professional edition except that the number of scans is limited to any 5 IPs (only) of the users choice , and is not supported by AdventNet.