

Enterasys NetSight Automated Security Manager Release Not

Table of Contents

<u>CUSTOMER RELEASE NOTES</u>	1
<u>INTRODUCTION</u>	1
NetSight Automated Security Manager.....	2
<u>SOFTWARE CHANGES AND ENHANCEMENTS</u>	2
Software Enhancements.....	2
<u>SYSTEM REQUIREMENTS</u>	2
Supported Platforms.....	2
<u>PRODUCT DEVICE/FIRMWARE SUPPORT</u>	3
Static Policies.....	3
CDP Implementation.....	4
Optimized Node/Alias Implementation.....	5
<u>INSTALLATION INFORMATION</u>	6
Upgrading Automated Security Manager.....	7
Evaluation Copy.....	7
<u>CONFIGURATION CONSIDERATIONS</u>	7
NetSight Automated Security Manager 2.0.....	8
Dragon Intrusion Defense System.....	8
Windows™ 2000.....	8
Devices.....	8
<u>OPERATING SYSTEM PATCHES</u>	8
<u>KNOWN RESTRICTIONS AND LIMITATIONS</u>	8
Install/Uninstall.....	8
NetSight Automated Security Manager.....	10
Help System.....	10
<u>SUPPORTED MIBs</u>	11
<u>IMPORTANT URLS</u>	11
<u>GLOBAL SUPPORT</u>	12
<u>ADDENDUM</u>	12

CUSTOMER RELEASE NOTES

**Enterasys NetSight™
Automated Security Manager
Version 2.0
March 2005**

INTRODUCTION:

When updates have been obtained using the NetSight Web Update feature, the Addendum section at the end of these release notes will contain the updated release information.

The most recent version of these release notes can also be found on the NetSight Documentation web page:
<http://www.enterasys.com/support/manuals/netsight.html>.

NOTE: When this topic is opened from the CD-ROM, the links from this topic to other help topics will not work (404 – not found). Links within the topic will work and once you've installed NetSight Automated Security Manager, you can launch the help system and access help for all topics.

NetSight Automated Security Manager

NetSight Automated Security Manager combines the features of a comprehensive intrusion detection system, such as Enterasys' Dragon Intrusion Defense System (IDS), with NetSight Compass' search capabilities and NetSight Policy Manager to provide an effective defense against threats to the security of your network. Automated Security Manager lets you easily configure your responses to threats.

It is recommended that you thoroughly review these release notes prior to the installation or upgrade of this product.

SOFTWARE CHANGES AND ENHANCEMENTS

This release of Automated Security Manager introduces the NetSight client-server architecture compatible with NetSight Console 2.0.

Software Enhancements

The following enhancements have been implemented in this release of NetSight Automated Security Manager:

- Client-Server architecture
- Launched as a client separately or from Console's Applications Menu
- Rule Variables moved to ASM Configuration Window
- Rule variables can be configured for specific times and days of the week
- Linux SuSe support
- Applications Menu lets you launch other NetSight plugin applications
- NetSight Events view is now available in the Activity Monitor window
- MAC only events processing
- Manual Confirmation Timer automatically confirms an action if manual confirmation does not occur within the specified time
- Multi-User Authentication MIB support
- Undo Trap feature

SYSTEM REQUIREMENTS

ASM requires installation of NetSight Console Server 2.0.

Supported Platforms

The system requirements for operating NetSight Automated Security Manager are listed here.

- **Windows 2000, Windows 2003 Server, Windows XP Professional** w/Service Pack 2 (qualified on the English version of the operating systems)
 - Recommended P4-2.4 GHz, 1GB RAM
 - Free Disk Space - 600MB
- **Solaris 2.8, Solaris 2.9** (with latest operating system patches installed.)

Enterasys NetSight Automated Security Manager Release Notes

- Recommended Sun®Ultra 30/60 (or equivalent), 900MHz, 1GB RAM
 - Free Disk Space – 600MB

 - **Linux: Red Hat Version 9, Red Hat Enterprise ES, WS version 3, and SuSE Linux**
 - Recommended P4–2.4 GHz, 1GB RAM
 - Free Disk Space – 600MB
-

PRODUCT DEVICE/FIRMWARE SUPPORT:

Static Policies

Devices that support Static Policies must be able to discard traffic at the role level and apply a Quarantine role that is set up to discard traffic (as defined in NetSight Policy Manager 1.7). The following tables list devices and firmware revisions for which NetSight Automated Security Manager has been qualified. Firmware versions other than these may not be fully supported.

Devices/Firmware that support Static Policies:

Product Family	Firmware Version
<i>Matrix C1</i>	1.01.xx 2.00.xx
<i>Matrix C2</i>	2.01.24 3.00.xx
<i>Matrix E1</i>	3.00.xx 3.01.xx 3.02.xx 3.03.xx
<i>Matrix E6/E7 (2nd/3rd Generation)</i>	5.06.xx 5.07.xx 5.08.xx
<i>Matrix N3/N7 Platinum</i>	3.00.xx 4.00.xx 4.05.xx 4.11.xx 5.01.xx
<i>Matrix N3/N7 Gold</i>	3.10.xx 4.05.xx 4.11.xx 5.01.xx
<i>RoamAbout R2</i>	5.03.xx
NOTE: Static Policy support for this device does not permit	

MAC-level control, only control at the port level.	
--	--

Devices/Firmware that do not support Static Policies:

Product Family	Firmware Version
<i>Matrix E5</i>	3.00.xx
<i>Matrix V2</i>	2.03.xx 2.04.xx
<i>Vertical Horizon</i> <i>VH-2402S</i> <i>VH-2402-L3</i> <i>VH-4802</i> <i>VH-8TX1UM/MF</i>	2.05.19 1.00.16 2.05.05 2.04.07.08
<i>RoamAbout Access Point 3000</i>	1.00.xx
<i>Matrix B2</i>	1.00.xx
<i>Matrix C2</i>	1.00.20

CDP Implementation

CDP must be disabled on the downstream devices when attached to a device using multi-user authentication (such as the Matrix N-Series Platinum). ASM (by design) excludes CDP ports from responding to a threat. If a device using multi-user authentication has a downstream device attached, such as a RoamAbout R2 that is running CDP, then ASM will not be able respond to threats from the port where it is attached.

Use NetSight Console's **CDP Status** FlexView to disable CDP on downstream devices.

For example, from Console:

1. Select the **Wireless** Device Group in Console's left (tree) panel.
2. Open the **CDP Status** FlexView in the right panel.
3. Select all rows and use the Table Editor to set the **Global Status** to *disable* for all devices.

Devices/Firmware that do not support CDP

Product Family	Firmware Version
<i>Matrix C2</i>	1.00.20
<i>Vertical Horizon</i> <i>VH-2402S</i> <i>VH-2402-L3</i>	2.05.19 1.00.16

<i>VH-4802</i>	2.05.05
<i>VH-8TX1UM</i>	2.04.07.08

Optimized Node/Alias Implementation

Automated Security Manager processes Dragon events by locating the intruder IP address stored in the event and then taking action. This search process is completed far more quickly on devices implementing the "optimized" Node/Alias MIB table. The following table lists devices and firmware revisions supporting the optimized Node/Alias MIB table.

Devices/Firmware that support "Optimized" Node/Alias:

Product Family	Firmware Version
<i>Matrix E1</i>	3.00.xx 3.01.xx 3.02.xx
<i>Matrix E6/E7 (2nd/3rd Generation)</i>	5.06.xx 5.07.xx 5.08.xx
<i>Matrix N3/N7 Platinum and Gold</i>	3.00.xx 4.00.xx 4.05.xx 4.11.xx
<i>Matrix V2</i>	2.03.xx 2.04.xx

NOTES: Support for Optimized Node/Alias --- The Automated Security Manager Incident Detail view (right-click an entry in the Activity Monitor and select View Details) indicates whether a device supports the optimized Node/Alias table or not:

- "Reading ctAliasTable" means that the device does not support the optimized Node/Alias table.
- "Reading ctAliasProtocolAddressTable" means that the device does support the optimized Node/Alias table.

Devices that do not support Node/Alias:

- Matrix C1
- Matrix C2
- Matrix E5
- Matrix E1 (1G6xx-xx)
- Vertical Horizon

These devices do not support any form of Node/Alias. For these devices, the Automated Security Manager search resolves the searched IP address to the corresponding MAC address and does a MAC-based search to locate the physical port. Routers must be included in the search scope in order to provide access to the routers' ARP cache. In addition, you must select

the ipRouteTable and ipCIDRRouteTable MIBs in the Automated Security Manager Options MIB Selection panel.

Disable Node/Alias Learning — It's important to make sure that inter-switch links are not learning Node/Alias information, as it would slow down searches and give inaccurate results. Enabling CDP on inter-switch links disables Node/Alias learning. You can also disable Node/Alias learning on a switch port by setting the maximum number of entries per interface (*ctAliasConfigurationInterfaceMaxEntries*) to 0 on that port, using the Node Alias Control FlexView in Console.

The following table provides Automated Security Manager search time comparisons between optimized and not optimized Node/Alias implementations.

Search Time Comparisons:

Number of Devices	Node/Alias Optimized 4000 entries	Node/Alias Not Optimized 4000 entries	Node/Alias Optimized 200 entries	Node/Alias Not Optimized 200 entries
25	3 sec	1 min 40 sec	3 sec	7 sec
100	9 sec	5 min 50 sec	9 sec	25 sec
200	20 sec	11 min 10 sec	20 sec	47 sec
300	25 sec	16 min 52 sec	25 sec	1 min 13 sec
800	1 min 3 sec	58 min 46 sec	1 min 3 sec	3 min 13 sec

INSTALLATION INFORMATION:

NetSight Automated Security Manager can be installed on the following platforms:

- Windows:
 - Windows® 2000
 - Windows® XP Professional
 - Windows® 2003 Server
- UNIX®
 - Solaris® 2.8
 - Solaris® 2.9
- Linux
 - Red Hat Version 9
 - Red Hat Enterprise ES, WS version 3
 - SuSE Linux (Systems running SuSE Linux should be re-booted prior to installation. See Known Restrictions – Install/Uninstall Problem 11 in the NetSight Console 2.0.1 Release Notes.)

The NetSight Installer (InstallAnywhere® by Zero G Software, Inc.) leads you through a series of windows that ask you for all the information required in order to install NetSight Automated Security Manager. When

you finish with the series of windows, NetSight Automated Security Manager is installed according to your specification. For complete installation information and instructions, refer to the [Installation](#) help topic, and the instructions available on the web site: www.enterasys.com/netsight/.

Upgrading Automated Security Manager

If you are upgrading from Automated Security Manager, release 1.1, you can import ASM components from a NetSight (Console release 1.5) database. The information that is imported from the earlier database replaces any ASM information that you've configured in the currently open database. However, some preparations and caveats should be understood prior to importing elements from the earlier version into Automated Security Manager 2.0.

- Make a Backup of your current NetSight 2.0 database (use the [Database](#) tab of the Server Information view). Importing components from the 1.5 database into 2.0 will overwrite all existing ASM tables in the database.
- Log Entry Details are not imported. Log Entries from release 1.1 are imported, however attempting to open the Log Entry Details view will result in an error message.
- When importing from a remote client, Custom Action Scripts and Custom Undo Scripts must be manually copied to their proper location on the server. This is because only the paths to scripts are imported to the server; the scripts themselves are not imported to the server. Copy your custom scripts to the `<install area>\Enterasys Networks\NetSight Atlas Console 2.0\server\plugins\AutoSecMgr\scripts` directory on the server.
- You must populate the NetSight Database with devices prior to importing ASM components. Either convert the prior version of the NetSight database or **Discover** the devices on your network.
- Devices, Device Groups, Profiles, Users, and Authorization Groups that are already in the NetSight Console 2.0 database will not be changed.
- You must have read and write file access in the directory from where you want to **Open** an earlier database and where you will **Save** the updated database.

Errors detected during the import are reported in the Events View – Automated Security tab. Refer to [Importing a Database](#) for more specific information on importing from a NetSight (Console release 1.5) database.

Evaluation Copy

When you install NetSight Automated Security Manager, you can select to install a 30-day Evaluation Copy. The evaluation copy installs NetSight Automated Security Manager. The evaluation period for starts when it is installed and expires 30 days later.

If you decide to convert an evaluation copy of Automated Security Manager at the end of the evaluation period, you should contact your Enterasys Networks Representative to purchase the software and receive a License Key. You will not need to reinstall the software to perform the conversion from an evaluation copy to a fully licensed version of the software.

CONFIGURATION CONSIDERATIONS

NetSight Automated Security Manager 2.0

1. During installation, the license information will be unreadable if your display settings are set for a black background (e.g., High Contrast#1, High Contrast #2, or High Contrast Black). Set your display **Properties > Appearance > Color Scheme** to something other than a black background during installation.
2. Do not attempt to manually remove actions that have been applied to devices by NetSight Automated Security Manager. Use ASM's **Undo Action** feature in Activity Monitor window. Attempting to manually remove actions can leave devices in an unspecified condition, possibly compromising the security of your network.

Dragon Intrusion Defense System

1. Alarms should be configured as **RealTime** to ensure that ASM receives all events from Dragon. Alarms that are set to Dynamic may filter some events that are needed by ASM.

Windows™ 2000

1. You should disable the **Guest** account when running NetSight Automated Security Manager on a Windows™ 2000 host system. Windows 2000 allows a user without an account on the machine to login using the **Guest** account. This is a potential security problem.

Devices

1. The Matrix N-Series Gold supports up to two users per port, with the possibility that one MAC could be that of an IP phone. Be careful when configuring the Quarantine role and the ASM rules to avoid configuring an action that would inadvertently affect the IP phone.
2. ASM resolves IP addresses to MAC addresses using information from routing MIBs (ipNetToMediaTable, ipCidrRouteTable, and ipRouteTable). Devices which support multiple virtual routers (Matrix N-Series Gold and Platinum) need to be modeled using the correct SNMPv3 context for the router, in order to access the routing MIBs.

OPERATING SYSTEM PATCHES

Before installing NetSight Automated Security Manager on the UNIX platform, be sure to install the latest patches for your operating system. You can download the most recent operating system patches from <http://sunsolve.sun.com/>.

KNOWN RESTRICTIONS AND LIMITATIONS

The known restrictions and limitations for this release of NetSight Automated Security Manager are listed below. Solutions for these restrictions and limitations are noted, if available.

Install/Uninstall

Problem 1:	(Windows 2000/XP/Server 2003 only) An evaluation of your system is not automatically performed during the installation. If system requirements are not met, the install will take
-------------------	---

Enterasys NetSight Automated Security Manager Release Notes

	place, but results will be unpredictable.
Solution:	Verify that all Windows 2000/XP system requirements are met prior to installing NetSight Automated Security Manager.
Problem 2:	(Solaris only) In the Select Destination window of the Installer, if you click Browse and then double click to select a directory, the OK button doesn't work.
Solution:	You must select the directory using a single click instead of a double click.
Problem 3:	(Solaris only) The Installer does not come up due to path problems.
Solution:	Ensure that /usr/usb does not precede /bin in your path. To do this, in a Unix window, type which chown . If the result is /usr/ucb/chown, replace /usr/ucb with /bin in your path. If the result is /bin/chown, the path is not the problem.
Problem 4:	(Solaris only) When the Installer is started, the following message is reported: Warning: Cannot convert string "-monotype-arial-regular-r-normal--*-140-*-*p-*-iso8859-1" to type FontStruct.
Solution:	No action is required. The Installer will use a default font.
Problem 5:	(Solaris only) The NetSight Uninstall program cannot warn you that the Automated Security Manager is running when you attempt to uninstall. When this happens, some components are not removed and subsequent installation and operation is unspecified.
Solution:	Exit from the NetSight Automated Security Manager and stop all services prior to starting Uninstall on Solaris workstations.
Problem 6:	During installation, the license information will be unreadable if your display settings are set for a black background (e.g., High Contrast#1, High Contrast #2, or High Contrast Black).
Solution:	Set your display Properties > Appearance > Color Scheme to something other than a black background during installation.
Problem 7:	When there is insufficient space in the selected install area, the installer reports the situation and lets you select an alternate location. If the alternate location does not provide the required space, the installer again reports the shortfall, but instead of showing the alternate path, it incorrectly shows the path to the original install area. The space provided by the alternate path is analyzed correctly; only the path that is reported is wrong.
Solution:	Select an install area that provides the required disk space. Refer to System Requirements for more information.
Problem 8:	Uninstall does not uninstall all files. This results in a message, when installing NetSight Console, indicating that ASM is still installed.
Solution:	After uninstalling ASM, remove the .com.zerog.registry.xml file. On Windows, this file is located in the C:\Program Files\Zero G Registry directory. On Solaris or Linux, this file is located in the /var directory.

NetSight Automated Security Manager

General

Problem 1:	(Linux and UNIX only) You cannot specify a range of pages when printing from tables on UNIX or Linux systems. If you select Print from the Table Tools popup menus, the resulting print settings window does not open to a sufficient size (and cannot be resized) to allow access to the page range fields.
Solution:	For these systems, the only option is to print the entire table.
Problem 2:	If an action has been taken on a port and a timer has been set to Undo the action, if another trap comes in that implicates the same port, the second action will be taken. At this point, the first action cannot be Undone because the settings have changed so when the first timer expires, the Undo will fail.
Solution:	If multiple actions are taken on the same ports, they must be undone in reverse order so that the port can be successfully returned to its original state. Note that in this case, the rules should be evaluated to insure this is the desired behavior for the Automated Security Management system.
Problem 3:	The SNMPTrap Service synchronizes its timestamp with your system's clock when the service is launched, but does not recognize changing to or from Daylight Savings Time while running. This causes a one hour discrepancy in the timestamps for Traps and Informs that appear in Console and Automated Security Manager after making the change.
Solution:	Stop and Restart the SNMPTrap Service when changing to or from Daylight Savings Time.
Problem 4:	In the Activity Monitor, if several threats are received with the same Sender ID, Sender Name, and Threat IP, and they are Filtered because a Search for that Threat IP is already in progress, the Status of the incident sometimes stays at Search in Progress, even though the Search has completed.
Solution:	Set the ASM Operation Mode to Disable, which will force all Searches in Progress (Searches Pending) to be cancelled. Set the ASM Operation Mode to "Search Only" or "Search And Respond" and subsequent threats received will generate new Incidents in the Activity Monitor. The entries for the cancelled searches can be deleted, as desired.

Help System

Problem 1:	Links to topics selected in the Contents will not work correctly following a search operation. If you use the JavaHelp search to find a term, then return to the Contents and navigate to a topic, the viewer may take you to the wrong place in the topic. If the topic you select contains the term just sought using the search, the viewer will take you to the term instead of the topic you chose from the Contents.
Solution:	Return to the Search tab, clear the entry and click Search. Go back to the Contents and the navigation will work correctly.
Problem 2:	Scrolling rapidly (using the arrow keys) through the Contents panel in the help and, less frequently, scrolling within a topic (right panel) will cause a Java Exception. This is related to a JavaHelp bug.

Enterasys NetSight Automated Security Manager Release Notes

Solution:	Use the scroll bar in the help topics or use mouse clicks to navigate in the Contents panel.
Problem 3:	Printing help files from the Automated Security Manager Help viewer may cause the application to hang.
Solution:	Windows users should use Task Manager to end the Automated Security Manager Help task. Solaris users should kill the Automated Security Manager Help process. Print help files from a browser by accessing the NetSight Documentation Web page at http://www.enterasys.com/support/manuals/netsight.html , or by printing the .html files in the NetSight Automated Security Manager\docs directory.
Problem 4:	(Linux only) Linux remembers if a window was previously maximized, and if the help window is maximized prior to being dismissed, the next time it is opened, the information does not completely fill the maximized window.
Solution:	Resize the window to restore a normal presentation.

Any other problems than those listed above should be reported to our Technical Support Staff.

SUPPORTED MIBs

Click here for a list of the [IETF and Private Enterprise MIBs](#) supported by NetSight Automated Security Manager as of its initial release. For information regarding the latest software available, recent release note revisions and changes to the supported MIBs, visit the NetSight Automated Security Manager section at the following Web site:

<http://www.enterasys.com/support/manuals/netsight.html>.

Additional (indexed) MIB documentation is also available at the following Web site:

<http://www.enterasys.com/support/mibs>

IMPORTANT URLS:

The following Enterasys URLs provide access to NetSight software products and product information.

- To download the latest NetSight software products*, use the NetSight Software Download at <http://sweval.enterasys.com/>
- To download previously released NetSight products*, use the Download Library at <http://www.enterasys.com/download/>
- To receive information on Enterasys NetSight management products, including the availability of new versions and new product releases, sign up for ProActive Notification at <http://sweval.enterasys.com/notify/>
- To register any NetSight products that are covered under a service contract, use the NetSight Service Contract Product Registration form at <http://sweval.enterasys.com/netsight/>

*Software license keys are version dependent and will only operate with the version of software related to the license key.

GLOBAL SUPPORT

By Phone: (603) 332-9400

By Email: <mailto:support@enterasys.com>

By Web: <http://www.enterasys.com/support>

By Fax: (603) 337-3075

By Mail: Enterasys Networks, P.O. Box 5005, Rochester, NH 03867-5005

For information regarding the latest software available, recent release note revisions, or if you require additional assistance, please visit the Enterasys Support web site.

<http://www.enterasys.com/support>

ADDENDUM:

This section provides updated release information, available to current NetSight Automated Security Manager customers through the web update operation. Use the [Check for Updates](#) feature to determine if updates are currently available. The updates are listed by date, with the most recent updates listed first.

3/2005 P/N: 9038159 Subject to Change Without Notice F0615-E