

**Enterasys NetSight Automated Security Manager Release Not**

# Table of Contents

<b><u>CUSTOMER RELEASE NOTES</u></b> .....	<b>1</b>
<u>INTRODUCTION</u> .....	1
NetSight Automated Security Manager.....	2
<b><u>SOFTWARE CHANGES AND ENHANCEMENTS</u></b> .....	<b>2</b>
Software Changes.....	2
Software Enhancements.....	2
<b><u>SYSTEM REQUIREMENTS</u></b> .....	<b>3</b>
Supported Platforms.....	3
<b><u>PRODUCT DEVICE/FIRMWARE SUPPORT</u></b> .....	<b>3</b>
Static Policies.....	3
CDP Implementation.....	4
Optimized Node/Alias Implementation.....	5
<b><u>INSTALLATION INFORMATION</u></b> .....	<b>7</b>
Upgrading Automated Security Manager.....	7
Evaluation Copy.....	7
<b><u>CONFIGURATION CONSIDERATIONS</u></b> .....	<b>8</b>
NetSight Automated Security Manager 2.1.2.....	8
Dragon Intrusion Defense System.....	8
Windows™ 2000.....	8
Devices.....	8
<b><u>OPERATING SYSTEM PATCHES</u></b> .....	<b>9</b>
<b><u>KNOWN RESTRICTIONS AND LIMITATIONS</u></b> .....	<b>9</b>
Install/Uninstall.....	9
NetSight Automated Security Manager.....	10
Help System.....	11
<b><u>SUPPORTED MIBs</u></b> .....	<b>11</b>
<b><u>IMPORTANT URLS</u></b> .....	<b>11</b>
<b><u>GLOBAL SUPPORT</u></b> .....	<b>12</b>
<b><u>ADDENDUM</u></b> .....	<b>12</b>

# CUSTOMER RELEASE NOTES

**Enterasys NetSight™**  
**Automated Security Manager**  
Version 2.1.2  
February, 2006

## 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. 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.

---

This Enterasys Networks product is covered by the following United States Pending Patents:  
Publication No. 20050108568  
Publication No. 20050076245

## 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 this document prior to installing or upgrading this product.**

## SOFTWARE CHANGES AND ENHANCEMENTS

### Software Changes

The following restrictions and limitations were fixed in release 2.1 of ASM:

#### Install/Uninstall

The NetSight Uninstall program now provides a warning on Solaris systems (in addition to the other platforms) when you attempt to uninstall while ASM is running.

### Software Enhancements

The following enhancements have been added to release 2.1.2 of ASM:

- **Improved performance and stability under heavy load** – If necessary under extreme network loads, you can improve ASM performance by disabling Log Entry Details. For instructions, see [ASM Configuration Considerations](#).
- **Notify Trusted Access Manager** – (added to ASM 2.1.1) You can now configure ASM to notify Trusted Access Manager when it quarantines a MAC address. Upon notification, Trusted Access Manager automatically creates a MAC override and enforces the override to all Trusted Access Gateways, effectively preventing the quarantined end-system from accessing the network from any other location.

The following enhancements were added to release 2.1 of ASM:

- **Notifications Feature.** You can now create *notifications* that will be activated with your response to network threats. For example, you can:
  - configure E-Mail notifications
  - configure notifications to create a Syslog entry
  - configure notifications that send an SNMP Trap
  - identify a script to be executed
  - configure an SNMPv3 trap notification that will be sent to a Dragon IDS
  - combine notifications in a group to provide multiple notifications
- **Show/Hide View Panels.** The View menu now lets you show/hide the Statistics Summary, Incident Filter, and Operation Mode panels.
- **Clean Up Incidents Feature.** This new feature lets you delete incidents from the Activity Monitor table based on incident status.

- **View Rule Variable Usage.** New "Used In" buttons let you view where rule variables are in use by ASM rules.
- **Support for the Cisco@CAM Table** (SNMPv1 only)

## SYSTEM REQUIREMENTS

ASM requires installation of NetSight Console Server 2.1.

### Supported Platforms

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

- **Windows® 2000, Windows Server™ 2003, 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® 8, 9, and 10 on Sun® Platforms only** (with latest operating system patches installed.)
  - Recommended Sun®Ultra 30/60 (or equivalent), 900MHz, 1GB RAM
  - Free Disk Space – 600MB
- **Linux: Red Hat Version 9, Red Hat Enterprise Linux WS, ES v3, 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>SecureStack C2</i>	2.01.24 3.00.xx
<i>Matrix E1</i>	3.00.xx 3.01.xx 3.02.xx 3.03.xx

## Enterasys NetSight Automated Security Manager Release Notes

<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
<b>RoamAbout R2</b>  <b>NOTE:</b> Static Policy support for this device does not permit MAC-level control, only control at the port level.	5.03.xx

### 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>SecureStack B2</i>	1.00.xx
<i>SecureStack 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.

## Enterasys NetSight Automated Security Manager Release Notes

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>SecureStack C2</i>	1.00.20
<i>Vertical Horizon</i>	
<i>VH-2402S</i>	2.05.19
<i>VH-2402-L3</i>	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

## Enterasys NetSight Automated Security Manager Release Notes

(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
- SecureStack C2
- Matrix E5
- Matrix E1 (1G6xx-xx)
- Vertical Horizon
- AP 3000
- RoamAbout R2

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:

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/support/manuals/netsight.html](http://www.enterasys.com/support/manuals/netsight.html).

## 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 ASM 2.1.

- Make a backup of your current NetSight 2.1 database (use the [Database](#) tab of the Server Information view). Importing components from the 1.5 database into 2.1 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 Console\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 2.1 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 [How to Import a Database](#) for more specific information on importing from a NetSight (Console release 1.5) database.

To upgrade from a previous version of ASM to version 2.1.2, follow these instructions.

1. Exit ASM.
2. Uninstall ASM according to the instructions for that version.
3. Verify that Console 2.1 has been installed.
4. Install ASM 2.1.2 according to the [Installation](#) instructions.
5. Launch ASM 2.1.2.

## Evaluation Copy

When you install NetSight Automated Security Manager, you can select to install a 90-day Evaluation Copy. To upgrade from an evaluation copy of ASM to a purchased copy, contact your Enterasys Networks Representative to purchase the software and receive a License Key. You do not need to reinstall the software to perform the conversion.

## CONFIGURATION CONSIDERATIONS

### NetSight Automated Security Manager 2.1.2

1. **Do not manually remove actions.** 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 the Activity Monitor window. Attempting to manually remove actions can leave devices in an unspecified condition, possibly compromising the security of your network.
2. **Disable Log Entry Details.** Under extreme network loads, you can improve ASM performance by disabling Log Entry Details. The Log Entry Details window displays information about a specific trap/action entry in the Automated Security Manager Activity Monitor, and can be useful for debugging purposes. The window is launched by double-clicking an entry in the Activity Monitor table.

To disable Log Entry Details, edit your ASM properties file as follows:

- a. Navigate to the Properties file: <your install directory>\Enterasys Networks\Netsight Console\server\plugins\AutoSecMgr\AutoSecMgr.properties
- b. Open the AutoSecMgr.properties file in a text editor and add the following lines:  
#asm.logging.summary.useTopic=false  
#asm.logging.summary.enabled=false  
asm.logging.detail.useTopic=false  
asm.logging.detail.enabled=false
- c. If you still have performance problems, you can disable all logging by uncommenting the two lines that control summary logging. Summary logging refers to the events logged in the Automated Security Event Log tab.

### 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

<b>Problem 1:</b>	(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 place, but results will be unpredictable.
<b>Solution:</b>	Verify that all Windows 2000/XP <u>system requirements</u> are met prior to installing NetSight Automated Security Manager.
<b>Problem 2:</b>	(Solaris only) In the Select Destination window of the Installer, if you click <b>Browse</b> and then double click to select a directory, the <b>OK</b> button doesn't work.
<b>Solution:</b>	You must select the directory using a single click instead of a double click.
<b>Problem 3:</b>	(Solaris only) The Installer does not come up due to path problems.
<b>Solution:</b>	Ensure that <code>/usr/usb</code> does not precede <code>/bin</code> in your path. To do this, in a Unix window, type <b>which chown</b> . If the result is <code>/usr/ucb/chown</code> , replace <code>/usr/ucb</code> with <code>/bin</code> in your path. If the result is <code>/bin/chown</code> , the path is not the problem.
<b>Problem 4:</b>	(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.
<b>Solution:</b>	No action is required. The Installer will use a default font.
<b>Problem 5:</b>	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.
<b>Solution:</b>	Select an install area that provides the required disk space. Refer to <u>System Requirements</u> for more information.
<b>Problem 6:</b>	Uninstall does not uninstall all files. This results in a message, when installing NetSight Console, indicating that ASM is still installed.

## Enterasys NetSight Automated Security Manager Release Notes

<b>Solution:</b>	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

<b>Problem 1:</b>	(Linux and UNIX only) You cannot specify a range of pages when printing from tables on UNIX or Linux systems. If you select <b>Print</b> from the <b>Table Tools</b> popup menu, the resulting print settings window does not open to a sufficient size (and cannot be resized) to allow access to the page range fields.
<b>Solution:</b>	For these systems, the only option is to print the entire table.
<b>Problem 2:</b>	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.
<b>Solution:</b>	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.
<b>Problem 3:</b>	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.
<b>Solution:</b>	Stop and Restart the SNMPTrap Service when changing to or from Daylight Savings Time.
<b>Problem 4:</b>	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.
<b>Solution:</b>	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.
<b>Problem 5:</b>	Occasionally, importing frozen ports from Policy Manager fails if SNMP Redirect is enabled. This can be an issue depending on the number of frozen ports on a single device, and varies depending on the device type.
<b>Solution:</b>	There are three ways to work around this issue: 1) disable SNMP Redirect while importing, 2) before importing, verify in Policy Manager that there are no more than eight frozen ports on a single device, or 3) manually exclude ports that failed to import.

## Help System

<b>Problem 1:</b>	A graphic hotspot may not work correctly the first time you click it unless the graphic is fully displayed on the screen.
<b>Problem 2:</b>	If you use the JavaHelp search to find a term, then return to the Contents and navigate to another topic that contains the term you were just searching for, the viewer takes you to the term inside that topic.
<b>Solution:</b>	Return to the Search tab, clear the entry and click Search. Go back to the Contents and the navigation will work correctly.
<b>Problem 3:</b>	Help does not launch from the Help button in the Authorization/Device Access window.
<b>Solution:</b>	You can access Help for the Authorization/Device Access window from the Help viewer Table of Contents (Help > Help Topics).

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: (800) 872-8440

By Email: [support@enterasys.com](mailto:support@enterasys.com)

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

By Mail: Enterasys Networks, 50 Minuteman Rd., Andover, MA 01810

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.

**2/2006    P/N: 9038159-02    Subject to Change Without Notice    F1650-H**