

Trusted Access Manager Release Notes

Table of Contents

<u>CUSTOMER RELEASE NOTES</u>	1
<u>INTRODUCTION</u>	1
Trusted Access Manager Features.....	2
<u>SYSTEM REQUIREMENTS</u>	2
Supported Platforms.....	2
Enterasys NetSight Console.....	3
UNIX® Operating System Patches.....	3
<u>PRODUCT/FIRMWARE SUPPORT</u>	3
<u>INSTALLATION</u>	3
Evaluation Copy.....	3
<u>CONFIGURATION CONSIDERATIONS</u>	4
<u>ENTERASYS NETSIGHT COMPATIBILITY</u>	4
<u>KNOWN RESTRICTIONS AND LIMITATIONS</u>	4
Install/Uninstall.....	4
General.....	5
Help System.....	6
<u>IMPORTANT URLS</u>	6
<u>GLOBAL SUPPORT</u>	6
<u>ADDENDUM</u>	7

Enterasys Sentinel™ Trusted Access Manager
Version 1.0
December, 2005

INTRODUCTION:

Enterasys Sentinel Trusted Access Manager is an integrated security management application that provides enhanced system-level controls to proactively protect your network from unwanted or unauthorized access. The Client/Server architecture lets you deploy Trusted Access Manager in a multi-user environment where remote clients can connect to a common, centralized database. Because Trusted Access Manager depends on functionality provided by Enterasys NetSight Console, every installation of Trusted Access Manager must include the installation of Console version 2.1.

When updates have been obtained using the 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 Trusted Access Manager, you can launch the help system and access help for all topics.

Trusted Access Manager Features

Security Domains

Security Domains let you group your Trusted Access Gateway appliances and the switches assigned to those gateways, and define a configuration that specifies the authentication and assessment requirements for the end-systems connecting to that domain. The configuration also specifies the security policies that will be applied to end-systems, depending on assessment results.

User and MAC Overrides

Override rules let you override a Security Domain's configuration with a special configuration to be used for a specific end-system, based on MAC address or user name.

Leverages Automated Security Manager

You can configure Enterasys NetSight Automated Security Manager to notify Trusted Access Manager when it quarantines a MAC address. 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.

MAC Locking

MAC Locking lets you lock a MAC address to a specific switch or port on a switch so that the end-system can only access the network from that port or switch. If the end-system tries to authenticate on a different port or switch, it will be rejected or assigned a specific policy based on an action that you specify when you create the MAC Lock.

End-System Monitoring

You can monitor end-system events and view the health results from an end-system's latest assessment scan. Quickly view historical and last-known connection states for each end-system, and obtain information on security risks found on an end-system during a scan.

End-System Statistics

You can view end-system connection state statistics presented in easy-to-read graphic charts. View current end-system status, historical end-system status, or end-system events over time.

<p>It is recommended that you thoroughly review this document prior to installing or upgrading this product.</p>

SYSTEM REQUIREMENTS:

Supported Platforms

The system requirements for operating Trusted Access 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

Trusted Access Manager Release Notes

- **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

Enterasys NetSight Console

The Trusted Access Manager Client and Server license must be installed on a workstation that has an Enterasys NetSight Console version 2.1 Server already installed. Trusted Access Manager depends on functionality provided by the NetSight Server, which is a component of Console 2.1. Trusted Access Manager Client-only installations do not have this requirement.

UNIX® Operating System Patches

Before installing Trusted Access 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 www.sunsolve.sun.com.

PRODUCT/FIRMWARE SUPPORT:

Trusted Access Manager supports the following Enterasys hardware products and firmware versions:

Product	Firmware Version
Matrix E6/E7	5.08.17 5.09.14
Matrix N-Series	5.21.XX
SecureStack C2	03.02.XX
Matrix E1	03.05.11

INSTALLATION:

The Trusted Access Manager 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 Trusted Access Manager. When you finish with the series of windows, Trusted Access Manager is installed according to your specification. For complete installation information and instructions, refer to the [Installation](#) help file, and the instructions available on the web site: www.enterasys.com/netsight/. Select the download evaluation software link.

Evaluation Copy

When you install Trusted Access Manager, you can select to install a 90-day Evaluation Copy. To upgrade from an evaluation copy of Trusted Access Manager 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

- **Web-based Authentication does not support automatic reauthentication of the end-user.** This prevents Trusted Access Manager from assigning the user the appropriate policy following a scan of the user's end-system. The user will continue to receive the designated scanning policy until they manually reauthenticate via the authentication web page. When they reauthenticate, they will receive the correct policy based on scanning results. This is not an issue if scanning is not required. You can alert end-users of this issue by adding a message to the authentication web page. Use Policy Manager to edit the web page banner so that it reads something like:

"Your login may be subject to an assessment of your computer. Please be advised that you may have to log in again when the assessment is complete."

In addition, the "Force Reauth" and "Force Reauth and Scan" buttons on the End-Systems tab will not work for end-systems that have authenticated via Web-based authentication.

ENTERASYS NETSIGHT COMPATIBILITY:

Trusted Access Manager's interoperability and concurrent application capabilities are listed below:

NMS Platform	Version No.	Support
Enterasys NetSight Console	2.1	Yes
Enterasys NetSight Automated Security Manager	2.1.1	Yes

KNOWN RESTRICTIONS AND LIMITATIONS:

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

Install/Uninstall

Problem 1:	(Windows 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.
Solution:	Verify that all Windows platform <u>system requirements</u> are met prior to installing Trusted Access Manager.
Problem 2:	Solaris only. The installer reports that it is unable to complete the Host Evaluation, and you cannot proceed with the installation.
Solution:	The /tmp directory is probably full. You must exit the installer and reboot the workstation. You can then restart the installation.

Trusted Access Manager Release Notes

General

Problem 1:	If a switch supports more than two RADIUS servers, an enforce will only modify the first two entries. Any other RADIUS server entries (configured on the switch via CLI or Policy Manager) will remain as Active.
Problem 2:	Enforcing a Trusted Access Gateway that does not belong to a Security Domain will clear any configuration information from the gateway. When this happens, you may need to manually update the RADIUS settings on your switches.
Problem 3:	You cannot create a Trusted Access Gateway without specifying a Primary and Secondary RADIUS Server. This creates a problem for network environments where RADIUS servers are not installed.
Solution:	You must add a non-existent RADIUS server via the Manage RADIUS Servers window and specify that server as the Primary and Secondary RADIUS Server in the Create Trusted Access Gateway window. This will be fixed in a future release.
Problem 4:	If you define an invalid Assessment server and then change to a valid server, end-systems that failed to scan with the invalid server will not be scanned by the new server.
Solution:	To get the scan to occur on these end-systems with the new Assessment server, you must either "Force Reauth and Scan" or delete the end-system in the right-panel End-Systems tab.
Problem 5:	You are allowed to enforce a Security Domain configuration that has scanning enabled, but has no Assessment servers defined. No error message is returned when the enforce is performed. This is an invalid configuration and will cause an end-system to enter the Scan state, but since no Assessment Servers have been defined, it will not be scanned.
Problem 6:	On rare occasions, Trusted Access Manager does not launch. You can log in and see the "Splash Screen," but the application never opens.
Solution:	Close the splash screen window and relaunch the application.
Problem 7:	<p>When a Security Domain configuration has scanning enabled, and a user tries to authenticate on an end-system where the MAC address cannot be resolved to an IP address, two events are logged in the End-System Events table on the End-Systems tab.</p> <p>This event is incorrect and can be ignored: State = Scan Extended State = Scan Started</p> <p>This event is correct: State = Error Extended State = MAC to IP Resolution Failed</p>

Help System

Problem 1:	A graphic hotspot may not work correctly the first time you click it unless the graphic is fully displayed on the screen.
Problem 2:	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.
Solution:	Return to the Search tab, clear the entry and click Search. Go back to the Contents and the navigation will work correctly.
Problem 3:	Help does not launch from the Help button in the Authorization/Device Access window.
Solution:	You can access Help for the Authorization/Device Access window from the Help viewer Table of Contents (Help > Help Topics).

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

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: www.enterasys.com/support.

ADDENDUM:

This section provides updated release information, available to current Trusted Access 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.

12/2005 P/N: 9034187-00 Subject to Change Without Notice F1650-H