Understanding Security Audit Tools
and PCI DSS in AOS Products

Quick Configuration Guide 61200860L1-42.1A February 2010

In response to growing concern over merchant data breaches during the last several years, the Payment Card Industry (PCI) Security Standards Council (SSC) has developed a stringent set of requirements called the Data Security Standard (DSS) to help retailers secure credit and debit card transactions. To comply with the PCI DSS, a merchant who stores, processes, or transmits the primary account number (PAN) for credit or debit cards must adhere to a strict set of requirements. However, the PCI council does not offer a certified stamp of approval for networking equipment or an approval process. It only makes recommendations as to the security, configuration, and management requirements of the equipment and software involved in the transmission and storage of payment card data.

ADTRAN Operating System (AOS) products provide a security audit tool to aid in identifying vulnerabilities in relation to the network components portion of the DSS requirements. Although the security audit tool identifies possible vulnerabilities, it does not consider where the AOS product resides in the network. Some items could be reported as risks that are not actual security issues when taking the entire network into account. It is the responsibility of the merchant or business to properly implement the AOS product for compliance. This guide is provided to enhance your understanding of the security audit tool and how to interpret the results.

Successfully passing all elements of the security audit does not ensure that the AOS unit is PCI compliant. This tool is provided as a means for identifying possible weaknesses.

To review the DSS requirements in detail, refer to the security standard online at *www.pcisecuritystandards.org*.

The Security Audit feature is available on AOS products as outlined in the ADTRAN knowledge base article number 2272, *Product Feature Matrix*. This matrix is available online at *http://kb.adtran.com*.

An AOS security audit can be initiated and the results viewed from either the command line interface (CLI) or the Web-based graphical user interface (GUI). Refer to the following sections for more information, *Using Security Audit Tools in the GUI* or *Using Security Audit Tools in the CLI on page 4*. The audit results displayed are the same in both the CLI and the GUI.

Using Security Audit Tools in the GUI

The GUI is an online configuration tool that allows you to easily configure and view system settings, as well as the status of your AOS product. The results of the last audit executed are saved in memory and persist across reboots. The user can also choose to save the results to a log file in either flash or CompactFlash® (cflash) memory (if available on the unit). The results can be viewed from the **Security Audit** menu.

Accessing the GUI

To access the GUI, follow these steps:

1. Open a new page in your Web browser.
2. Enter your unit's IP address in the browser's address field in the following form:

   http://<*ip address*>

> NOTE *The IP address may also be entered in* ***https://*** *if your unit has* ***ip http secure-server*** *enabled.*

3. At the prompt, enter your user name and password and select **OK**.

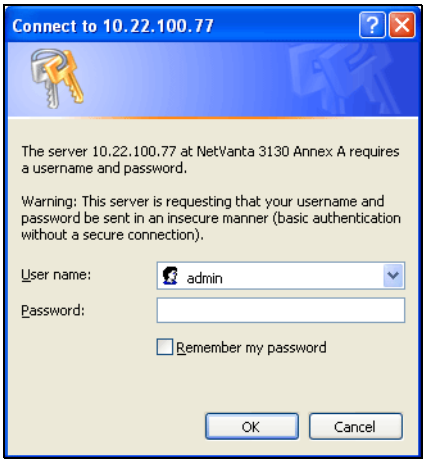

Figure 1. GUI Login Prompt

> NOTE *The default username is* ***admin*** *and the default password is* ***password****.*

Initiating the Security Audit Using the GUI

To initiate the security audit from the GUI, navigate to **Utilities** > **Audit**, and select **Run Audit** (see *Figure 2 on page 3*). The results are displayed on the screen as shown in *Figure 3 on page 4*. If you want to save the results to flash or CompactFlash memory, this option must be selected prior to selecting **Run Audit**. Even if the results are not saved to flash or CompactFlash, a copy of the last audit will persist across reboots and display the next time you log in.

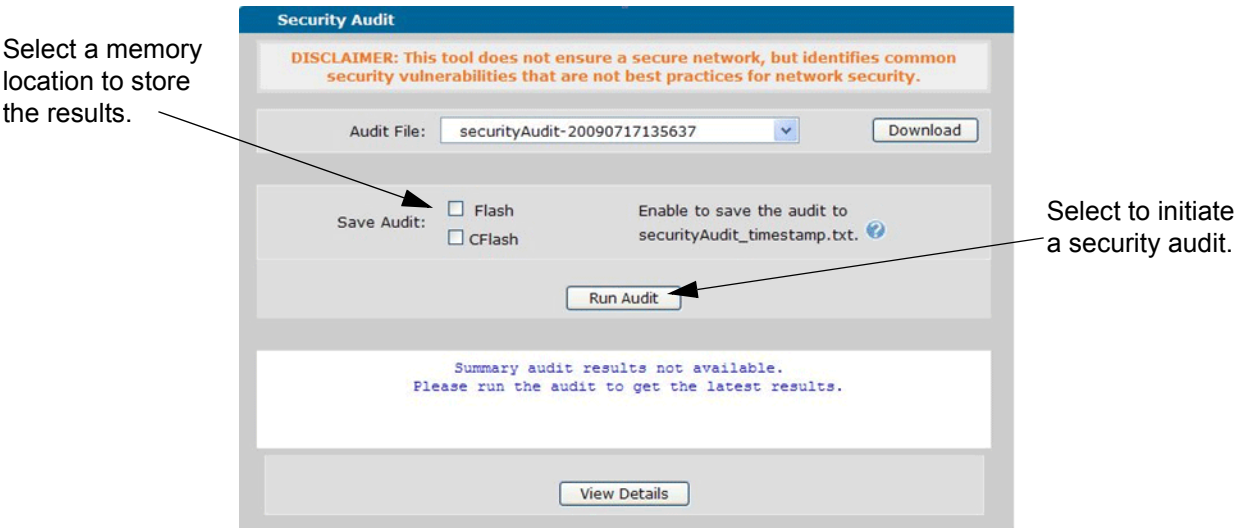

Figure 2. Security Audit Menu

> *If two people are logged in simultaneously (for example, one via Telnet and one via the console) and both try to run the audit security tool, the user who begins the audit first will take precedence. An error message will be displayed to the second user that an audit is in progress.*

Viewing Audit Details in the GUI

Once the audit is complete, the results summary displays on the **Security Audit** menu as shown in *Figure 3 on page 4*. To view the audit details from the GUI, select **View Details** from the **Security Audit** menu. The results displayed on this menu are from the last audit run and persist across reboots.

> *The audit results can be downloaded and saved on your local PC by selecting **Download** from the **Security Audit** menu.*

Figure 3. GUI Display of Audit Summary Results

To switch to the Summary view from the Detail view, scroll to the bottom of the screen and select **View Summary** (see *Figure 4*). The Detail view is too lengthy to show here but is similar to the **show audit security detail** command output example provided in *Viewing Audit Details in the CLI on page 6*.

Figure 4. Revert to View Summary Results

Using Security Audit Tools in the CLI

A security audit is initiated from the Enable mode prompt in the CLI. The results of the last audit executed are saved in memory and persist across reboots. The user can also choose to save the results to a log file in either flash memory or CompactFlash (cflash) memory (if available on the unit). The log file is named **securityAudit_**<*timestamp*>, where the <*timestamp*> is attached in the format yyyymmddhhmmss. The results can be viewed using **show** commands. Refer to *Viewing Audit Details in the CLI on page 6*.

Accessing the CLI

To access the CLI on your AOS unit, follow these steps:

1. Boot up the unit.
2. Telnet to the unit (**telnet** <*ip address*>).

   For example, **telnet 208.61.209.1**.

> NOTE *If during the unit's setup process you have changed the default IP address (**10.10.10.1**), use the configured IP address.*

3. Enter your user name and password at the prompt.

> NOTE *The AOS default user name is **admin** and the default password is **password**. If your product no longer has the default user name and password, contact your system administrator for the appropriate user name and password.*

4. Enter the Enable mode by entering **enable** at the prompt as follows:

   >enable

5. Enter your Enable mode password at the prompt.

Initiating the Security Audit Using the CLI

The following example initiates the security audit from the CLI and saves the results to a log file in flash memory:

```
>enable
#run audit security log
Audit Complete
```

If **cflash** is specified in the command, the results are stored in the CompactFlash memory. For example, the following initiates the security audit and saves the results to a log file in CompactFlash memory:

```
>enable
#run audit security log cflash
Audit Complete
```

> NOTE *Once the audit is in process, the session will be blocked until the audit is completed or until **Ctrl+C** is issued. If two people are logged in simultaneously (for example, one via Telnet and one via the console) and both try to run the audit security tool, the user who begins the audit first will take precedence. An error message will be displayed to the second user that an audit is in progress.*

Viewing Audit Details in the CLI

The results summary of the security audit can be viewed from the CLI by using the **show audit security** command. The **show audit security** command displays a summary of the results including: the type of defect, severity, and a brief description. The **show audit security detail** command lists the summary, as well as details of the defect and recommends corrective action.

The following is sample **show audit security** output:

>**enable**
#show audit security
Using 2214 bytes

SUMMARY

Severity	Type	Description
LOW	Enable Password	MD5 encryption is not enabled
HIGH	Network Protocol	FTP server enabled
HIGH	Network Protocol	TFTP server enabled
HIGH	Network Protocol	HTTP server enabled
HIGH	Network Protocol	Telnet enabled
HIGH	Policy-Class	Private, undefined ACL
HIGH	Policy-Class	Private, stateless
HIGH	Policy-Class	Public, stateless
HIGH	Policy-Class	Public, NAT not enabled
HIGH	Policy-Class	Interfaces using default policy-class
HIGH	Password	Weak Passwords
HIGH	Password	Duplicate Passwords
HIGH	Session Timeout	Console timeout >= 15 minutes
HIGH	Session Timeout	Telnet 0 timeout >= 15 minutes
HIGH	Session Timeout	Telnet 1 timeout >= 15 minutes
HIGH	Session Timeout	Telnet 2 timeout >= 15 minutes
HIGH	Session Timeout	Telnet 3 timeout >= 15 minutes
HIGH	Session Timeout	Telnet 4 timeout >= 15 minutes
HIGH	Session Timeout	SSH 0 timeout >= 15 minutes
HIGH	Session Timeout	SSH 1 timeout >= 15 minutes
HIGH	Session Timeout	SSH 2 timeout >= 15 minutes
HIGH	Session Timeout	SSH 3 timeout >= 15 minutes
HIGH	SNMP	Using SNMPv1/v2, not secure

The following is sample **show audit security detail** output:

```
>enable
#show audit security detail
Using 4193 bytes

**DETAIL**
-------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------
ENABLE PASSWORD:
-------------------------------------------------------------------------------------------------------------------
* The enable password is not set for MD5 encryption. MD5 encryption is more
secure than standard password encryption.
-------------------------------------------------------------------------------------------------------------------
NETWORK PROTOCOLS:
-------------------------------------------------------------------------------------------------------------------
* The following protocols are enabled and may be a security risk.
Disable if not needed. Use SSH instead of Telnet and HTTP SSLv3 instead of
HTTP SSLv2.

  * FTP
  * TFTP
  * HTTP
  * Telnet
-------------------------------------------------------------------------------------------------------------------
POLICY-CLASS:
-------------------------------------------------------------------------------------------------------------------
* Potential vulnerabilities were found with the following policies. Note: NAT
may not be required on all policies; however, broadcast of IP addresses from the
internal network to the Internet should be restricted. This tool did not take
into account how the policies are used. Depending upon the configuration of your
network, these policies may or may not make your network vulnerable.
*******************************************************************************************
Name            Line                    Description
*******************************************************************************************
Private         2                       Allows undefined ACL
Private         3                       Allows stateless-inspection
Public          4                       Allows stateless-inspection
Public          N/A                     NAT not enabled for
                                        Private interface, eth 0/1

* The following interfaces are enabled but do not have a policy-class
assigned. Not having a policy-class assigned will leave the interface open to
attack.

  * vlan 1210
```

PASSWORDS / KEYS:

---

* Passwords should be at least 7 characters and have both alphabetic and numeric characters. Some passwords are considered weak if they match default passwords or contain common sequences. For example Qwerty123 is considered a weak password even though it contains both numeric and alphabetic characters. The following weak passwords were found:

  * 1f1965f156e907907d3a8ed5172557a86736(encrypted)
  * 2b2d9aa78c8dfb9fca1cf745d72e2e28cc99(encrypted)
  * 373fbaa34722617409e24b9d9a707cb09fe3(encrypted)
  * 1610d7b313a09983a2de5bb4f1a77997f346(encrypted)
  * 24223699587eef35644778c8a901cca82a70(encrypted)
  * 46400f529e54aeb56fa224fadb14c111f007(encrypted)

* Each user should have a unique password. The following passwords are duplicated:

  * 2b2d9aa78c8dfb9fca1cf745d72e2e28cc99(encrypted)
  * 46400f529e54aeb56fa224fadb14c111f007(encrypted)

SESSION TIMEOUT:

---

* The following sessions have timeout values of 15 minutes or greater. Long session timeouts may allow your system to be compromised. To increase security, set the timeout value to less than 15 minutes.
* Console
* Telnet 0
* Telnet 1
* Telnet 2
* Telnet 3
* Telnet 4
* SSH 0
* SSH 1
* SSH 2
* SSH 3

SNMP:

---

* The SNMP agent is enabled and is configured to allow SNMPv1 and SNMPv2 which are not secure. If SNMP is needed, remove the community names and add SNMPv3 group and SNMPv3 user.

Reviewing Detected Security Risks

Various configuration items could be identified as posing a security risk. Remember, it is up to the user to determine if the items found are truly issues that need to be addressed. The following table lists the items that are audited, their severity level, and a description to assist you in correcting the problem. Additional documentation for many of the configuration items described below is available online at http://kb.adtran.com.

Table 1. Possible Security Risks

Violation Type	Severity	Description
Startup-Config	High	Indicates that the startup configuration file does not match the running configuration file. This is determined by comparing the message digest 5 (MD5) checksum of both files for a match.
Passwords/Keys	High	Identifies nonsecure passwords. If a password has MD5 encryption enabled, the tool tests for common password sequences, such as **qwerty**, **1234**, **abc**, **xyz**, etc. If MD5 is disabled, an alert is issued if the password: • Is less than 7 characters. • Does not contain alphabetic and numeric characters. • Matches common sequences, such as **qwerty**, **1234**, **abc**, **xyz**, etc. • Matches the default passwords. • Matches another password in the system. • Service password encryption is not enabled.
Firewall	High	Indicates the firewall is disabled.
Policy-Class	High	Identifies any of the following access control policy (ACP) vulnerabilities: • Stateful inspection is disabled. • An undefined access control list (ACL) exists in the ACP. • An interface with a private IP address (10.x.x.x, 172.16.x.x, 192.168.x.x) has an ACP assigned that does not have network address translation (NAT) configured. • An interface is enabled without an ACP assigned.
SNMP	High	Indicates the Simple Network Management Protocol (SNMP) agent is enabled and configured to allow SNMPv1 or SNMPv2. Both of these versions are considered nonsecure. SNMPv3 group and SNMPv3 user are preferred.
WiFi	High	Identifies any of the following wireless vulnerabilities: • Security mode is set to anything but WPA2 (including **none**). • Service set identifier (SSID) broadcast is enabled. • A weak key.

Table 1. Possible Security Risks *(Continued)*

Violation Type	Severity	Description
Network Protocols	High	Identifies any of the following network protocols are enabled and considered a security risk: • Hypertext Transfer Protocol (HTTP) • Hypertext Transfer Protocol Secure (HTTPS) secure sockets layer version 2.0 (SSLv2) • File Transfer Protocol (FTP) • Trivial File Transfer Protocol (TFTP) • Telnet Secure shell (SSH) is suggested as a replacement for Telnet and HTTPS secure sockets layer version 3.0 (SSLv3) instead of HTTPS SSLv2.
Session Timeout	High	Identifies the console, HTTP, SSH, or Telnet session timeout is set to a value greater than 15 minutes. Long session timeouts can compromise the system. The recommended setting is 15 minutes or less.
Time-Server	High	Indicates the time server (Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP)) is not configured. It can also indicate the time server is configured, but not synchronized. It is important to have a valid timestamp on all logs generated by the system.
Logging	Medium	Indicates user activity is not being logged. User activity should be logged either by enabling syslog or terminal access controller access-control plus (TACACs+) accounting. (The syslog can be enabled by using the **logging forwarding on** command.)
Domain Lookup	Medium	Indicates **ip domain-lookup** is enabled, but a domain name system (DNS) server has not been configured. This allows DNS requests to be broadcast.
Interfaces	Medium	Identifies the following interface vulnerabilities: • The **ip directed-broadcast** is enabled, which could make an interface vulnerable to denial of service (DoS) attacks. • A static ACL is assigned to an interface. A more secure option is to enable the firewall and assign an ACP.
Enable Password	Low	Indicates the Enable password is not set for MD5 encryption. MD5 encryption is more secure than standard password encryption.
Banner	Low	Indicates the default executive banner is still set. It is recommended that a custom banner be displayed when a user attempts to login. The banner warns of the legal consequences of unauthorized access to the unit.
Tcl Scripts	Low	Indicates Tcl scripting is enabled. Scripts could alter the unit's configuration.