CHAPTER 5

# Component Assessment

This chapter discusses the function of each component and how it helps to address PCI DSS 2.0 compliance requirements. Each component was assessed by Verizon Business, and the full reference architecture report is available in Appendix B, "Verizon Business Reference Architecture Report—Cisco PCI Solution for Retail."

This assessment took place at a specific point in time using currently available versions of products and software.

## Component Section Overview

Each component section includes the following:

- Description
- PCI assessment summary
- Primary PCI function
- Capability assessment
- Design considerations
- PCI assessment detail

### PCI Assessment Summary

For each component, the PCI Assessment Summary table (see Table 5-1) lists each of the PCI sub-requirements that were passed, required compensating controls, or failed.

*Table 5-1 PCI Assessment Summary Example*

| **Models Assessed** | |
|---|---|
| Cisco Catalyst Switch | |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2.2, 2.2.4, 2.3 |

*Table 5-1 PCI Assessment Summary Example (continued)*

| | |
|---|---|
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

# Capability Assessment

Each component requires specific capabilities to be deployable in a compliant environment. Customers and vendors alike have complained that it is difficult to understand what capabilities are required when developing or purchasing equipment for the purpose of compliance. Therefore, Cisco has developed a simplified approach to clarify the scales that are relevant. Sub-requirements have been grouped for ease of assessment, as shown in Table 5-1.

*Table 5-2 Capability Assessment Example*

| Cisco Component | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 9 (9.1.2)** |
| [Description of primary PCI function] | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

The PCI DSS 2.0 security standard is written from the perspective of helping a merchant become compliant. It is not grouped in a clear manner for the evaluation of hardware or software. The following grouping of sub-requirements is an extrapolation of the standard to simplify the assessment of hardware and software:

- *Secure services* comprises sub-requirements that affect the secure administration and hardening of the component, and include the following:
  - Disable any unnecessary services—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4)
  - Secure administrative access—*Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3)
  - Vendor supported—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1)
- *Authentication* comprises sub-requirements that affect the identity of personnel accessing systems in the cardholder data environment, including the following:
  - Role-based access—*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2)
  - Use secure, unique accounts—*Assign all users a unique ID before allowing them to access system components or cardholder data. Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14)
- *Logs* comprises sub-requirements that affect the forensic analysis capabilities of the cardholder data environment, including the following:
  - Audit trails—*Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3)
  - The ability to use Network Time Protocol—*Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3)

Table 5-3 explains the color-codes icons used in the tables.

***Table 5-3 Color-Coded Icon Definitions***

| Icon | Description |
|---|---|
| 🟢 | The component has the native capability to satisfy the requirement. |
| ◉ | The component has the capability to use other components to satisfy the requirement. |
| ▼ | The component requires compensating controls to satisfy the requirement. |
| ⊗ | The component has no capability to satisfy the requirement. |

## Design Considerations

This section provides compliance principles as well as best practices for each technology deployed within a retail business environment.

## PCI Assessment Detail

This section includes the following:

- PCI sub-requirements satisfied by solution component—Lists which PCI sub-requirements were successfully audited and validated by the respective technology. Each sub-requirement includes a configuration example or reference of how the sub-requirement was met. This result is directly correlated to the implementation built in the Cisco lab and presented in Chapter 4, "Implementing and Configuring the Solution."
- PCI sub-requirements that require compensating controls—Lists which PCI sub-requirements needed additional compensating controls to successfully pass the PCI audit. Examples include additional configurations, products, or policies to meet compliance requirements.
- PCI sub-requirements that failed—Lists which PCI sub-requirements could not be satisfied.

# Endpoints and Applications

The endpoints and applications layer of the solution framework addresses the components such as voice, e-mail, and physical security.

## Voice

### Cisco Unified Communications Manager and IP Phones

The Cisco Unified Communication Manager is a suite of voice applications, signaling control, and utilities that provide IP communications capabilities using devices such as the IP phones. It is configured as an appliance that is easy to deploy, flexible to manage, and allows robust security.

*Table 5-4 PCI Assessment Summary—Cisco Unified Communications Manager*

| **Models Assessed** | |
|---|---|
| Cisco Unified Communication Manager 8.5.1 | |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 9** | 9.1.2 |
| **PCI 10** | 10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5 |

*Table 5-4 PCI Assessment Summary—Cisco Unified Communications Manager (continued)*

| PCI Sub-Requirements Requiring Compensating Controls |
|---|
| No compensating controls were required to satisfy any sub-requirements. |
| **PCI Sub-Requirements Failed** |
| No sub-requirements were failed. |

## Primary PCI Function

The primary PCI function of Cisco Unified Communications Manager is to securely manage IP phones and communications flows, as well as securing publicly accessible network jacks (9.1.2).

Table 5-4 lists the component assessment details for Cisco Unified Communications Manager.

*Table 5-5 Component Capability Assessment—Cisco Unified Communications Manager*

| Cisco Unified Communications Manager | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 9 (9.1.2)** |
| Securely manage IP phones and communication flows. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***“Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

### Design Considerations

The design features for improving security for the Cisco Unified Communications Manager appliance include:

- Deployment as a clustered redundancy model that includes a publisher server and several subscriber servers
- Downloading and installing security patches when vulnerabilities are announced by the Cisco Product Security Incident Response Team (PSIRT)
- Implementing Transport Layer Security (TLS) messaging for secure signaling and Secure RTP (SRTP) for encrypted media throughout the enterprise
- Enabling device authentication and communication encryption using X.509 certificates that are signed by the Certificate Authority Proxy Function (CAPF) feature on the server

Best practices for Cisco Unified Communications Manager phone security are as follows:

- The Gratuitous ARP setting on the Cisco Unified IP Phones should be disabled.
- Disabling the web access setting prevents the phone from opening the HTTP port 80; this blocks access to the phone’s internal web pages.
- Disabling the PC Voice VLAN access setting in the phone configuration window prevents the devices connected to the PC port from using the voice VLAN functionality.
- Disabling the Setting Access option in the phone configuration window prevents users from viewing and changing the phone options, including the Network Configuration options, directly on the phone.
- Cisco Unified IP Phones can be configured for authentication and encryption by installing a CTL file on the phones that includes security tokens, trusted server and firewall information, and CAPF.

For more information on securing Unified Communications, see the *Cisco Unified Communications System 8.x SRND* at the following URL:
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/security.html

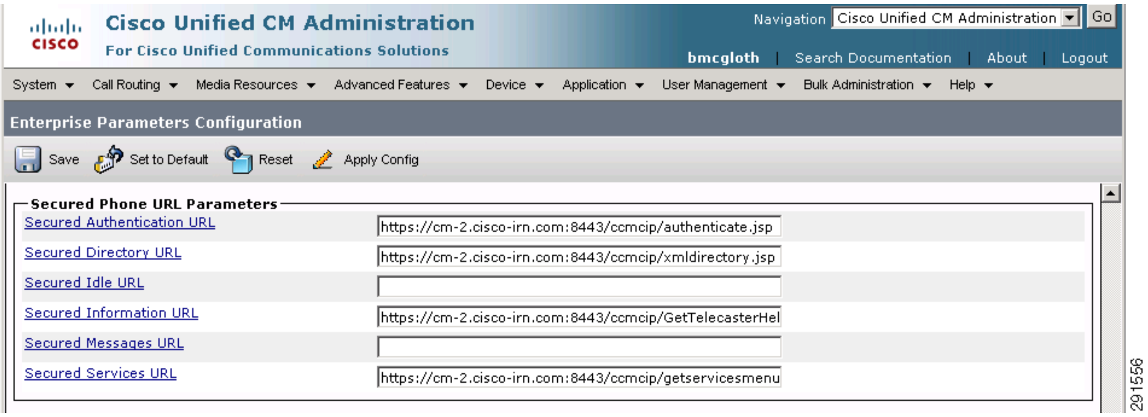
### PCI Assessment Detail—PCI Sub-Requirements Satisfied

#### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  The Cisco Unified Communication Manager appliance operating system includes only the components needed to run the application. Root access to the OS is disabled and this prevents any unwanted services from being implemented. Telnet and HTTP access to the server administration is disabled. The communication between phones and server over HTTP can be secured using SSL. (See Figure 5-1.)

*Figure 5-1 Enterprise Parameters Configuration*


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
bmcgloth | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Save Set to Default Reset Apply Config
291556

Enterprise Parameters Configuration

Secured Phone URL Parameters

| | |
|---|---|
| Secured Authentication URL | https://cm-2.cisco-irn.com:8443/ccmcip/authenticate.jsp |
| Secured Directory URL | https://cm-2.cisco-irn.com:8443/ccmcip/xmldirectory.jsp |
| Secured Idle URL | |
| Secured Information URL | https://cm-2.cisco-irn.com:8443/ccmcip/GetTelecasterHel |
| Secured Messages URL | |
| Secured Services URL | https://cm-2.cisco-irn.com:8443/ccmcip/getservicesmenu |

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The Cisco Unified Communication Manager appliance does not allow changes to the operating system, or to the database or installation of unsupported hardware or of unsupported third-party software.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  The Cisco Unified Communication Manager uses SSL for web-based administrative and user access and uses SSH for remote terminal access.

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in the Cisco Unified Communication Manager appliance. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise through a web browser or CLI.

  Software support for all Cisco products can be located at: http://www.cisco.com/cisco/software/navigator.html

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

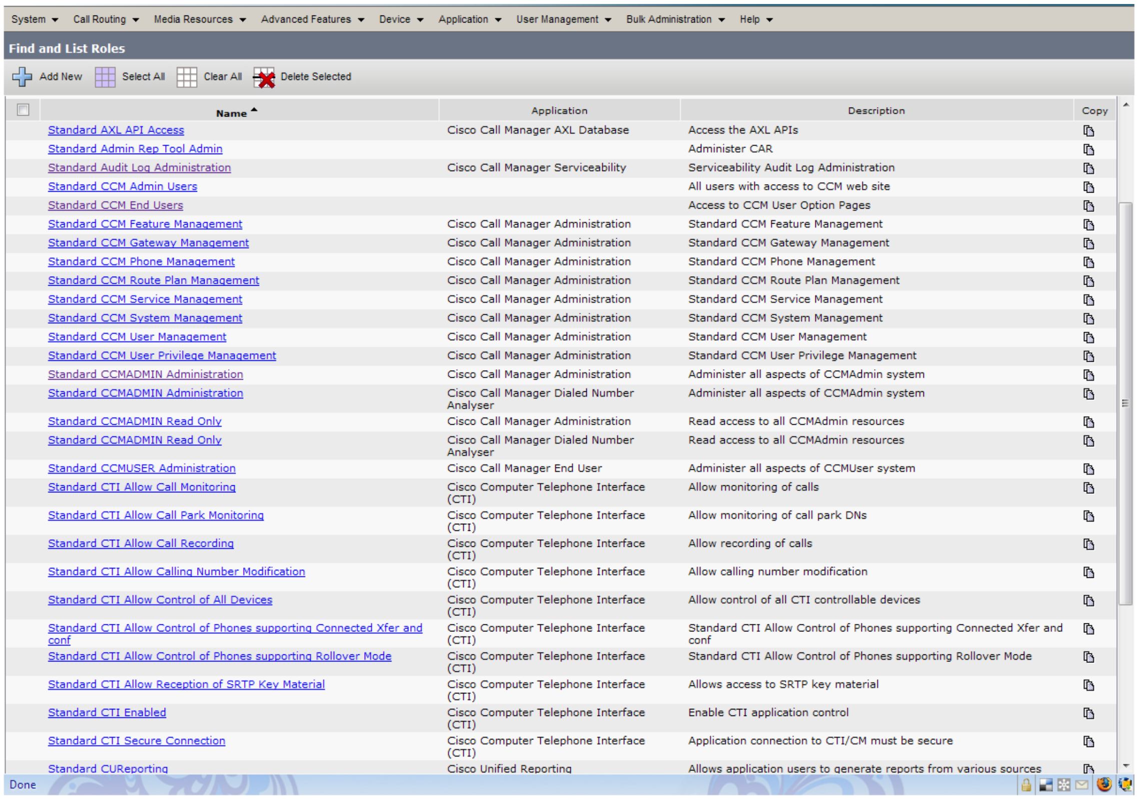
The relevant sub-requirements of Requirement 7 were met using the Cisco Unified Communication Manager's internal database. Cisco Unified Communication Manager also supports linking to a centralized user database such as Active Directory using LDAP. Within Cisco Unified Communication Manager, individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*

- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

  The Cisco Unified Communication Manager uses various role definitions for permitting access to various application components on the server. (See Figure 5-2.)

***Figure 5-2 Find and List Roles***

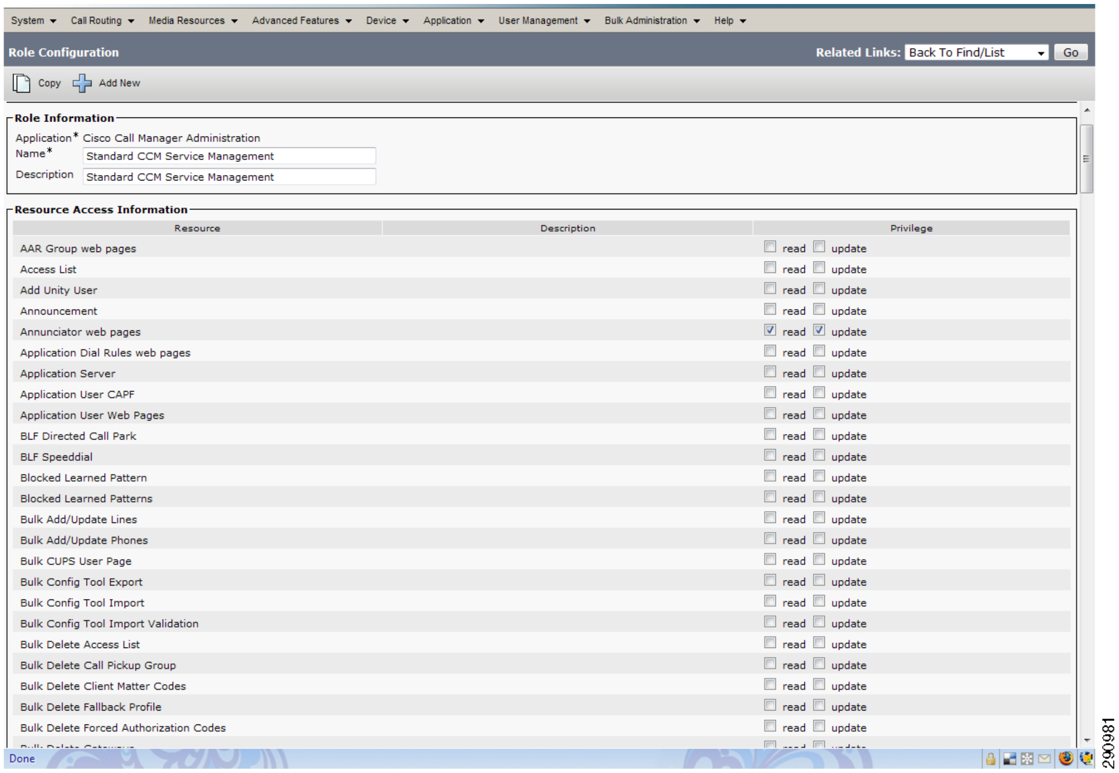


| □ | Name | Application | Description | Copy |
|---|---|---|---|---|
| | Standard AXL API Access | Cisco Call Manager AXL Database | Access the AXL APIs | ⎘ |
| | Standard Admin Rep Tool Admin | | Administer CAR | ⎘ |
| | Standard Audit Log Administration | Cisco Call Manager Serviceability | Serviceability Audit Log Administration | ⎘ |
| | Standard CCM Admin Users | | All users with access to CCM web site | ⎘ |
| | Standard CCM End Users | | Access to CCM User Option Pages | ⎘ |
| | Standard CCM Feature Management | Cisco Call Manager Administration | Standard CCM Feature Management | ⎘ |
| | Standard CCM Gateway Management | Cisco Call Manager Administration | Standard CCM Gateway Management | ⎘ |
| | Standard CCM Phone Management | Cisco Call Manager Administration | Standard CCM Phone Management | ⎘ |
| | Standard CCM Route Plan Management | Cisco Call Manager Administration | Standard CCM Route Plan Management | ⎘ |
| | Standard CCM Service Management | Cisco Call Manager Administration | Standard CCM Service Management | ⎘ |
| | Standard CCM System Management | Cisco Call Manager Administration | Standard CCM System Management | ⎘ |
| | Standard CCM User Management | Cisco Call Manager Administration | Standard CCM User Management | ⎘ |
| | Standard CCM User Privilege Management | Cisco Call Manager Administration | Standard CCM User Privilege Management | ⎘ |
| | Standard CCMADMIN Administration | Cisco Call Manager Administration | Administer all aspects of CCMAdmin system | ⎘ |
| | Standard CCMADMIN Administration | Cisco Call Manager Dialed Number Analyser | Administer all aspects of CCMAdmin system | ⎘ |
| | Standard CCMADMIN Read Only | Cisco Call Manager Administration | Read access to all CCMAdmin resources | ⎘ |
| | Standard CCMADMIN Read Only | Cisco Call Manager Dialed Number Analyser | Read access to all CCMAdmin resources | ⎘ |
| | Standard CCMUSER Administration | Cisco Call Manager End User | Administer all aspects of CCMUser system | ⎘ |
| | Standard CTI Allow Call Monitoring | Cisco Computer Telephone Interface (CTI) | Allow monitoring of calls | ⎘ |
| | Standard CTI Allow Call Park Monitoring | Cisco Computer Telephone Interface (CTI) | Allow monitoring of call park DNs | ⎘ |
| | Standard CTI Allow Call Recording | Cisco Computer Telephone Interface (CTI) | Allow recording of calls | ⎘ |
| | Standard CTI Allow Calling Number Modification | Cisco Computer Telephone Interface (CTI) | Allow calling number modification | ⎘ |
| | Standard CTI Allow Control of All Devices | Cisco Computer Telephone Interface (CTI) | Allow control of all CTI controllable devices | ⎘ |
| | Standard CTI Allow Control of Phones supporting Connected Xfer and conf | Cisco Computer Telephone Interface (CTI) | Standard CTI Allow Control of Phones supporting Connected Xfer and conf | ⎘ |
| | Standard CTI Allow Control of Phones supporting Rollover Mode | Cisco Computer Telephone Interface (CTI) | Standard CTI Allow Control of Phones supporting Rollover Mode | ⎘ |
| | Standard CTI Allow Reception of SRTP Key Material | Cisco Computer Telephone Interface (CTI) | Allows access to SRTP key material | ⎘ |
| | Standard CTI Enabled | Cisco Computer Telephone Interface (CTI) | Enable CTI application control | ⎘ |
| | Standard CTI Secure Connection | Cisco Computer Telephone Interface (CTI) | Application connection to CTI/CM must be secure | ⎘ |
| | Standard CUReporting | Cisco Unified Reporting | Allows application users to generate reports from various sources | ⎘ |

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

The role configuration menu in the Cisco Unified Communication Manager server allows specifying the assignment of privileges based on the role description. No systems access is permitted without an account. (See Figure 5-3.)

### Figure 5-3 Role Configuration



**Role Information**

Application* Cisco Call Manager Administration

Name* Standard CCM Service Management

Description Standard CCM Service Management

**Resource Access Information**

| Resource | Description | Privilege |
|---|---|---|
| AAR Group web pages | | □ read □ update |
| Access List | | □ read □ update |
| Add Unity User | | □ read □ update |
| Announcement | | □ read □ update |
| Annunciator web pages | | ☑ read ☑ update |
| Application Dial Rules web pages | | □ read □ update |
| Application Server | | □ read □ update |
| Application User CAPF | | □ read □ update |
| Application User Web Pages | | □ read □ update |
| BLF Directed Call Park | | □ read □ update |
| BLF Speeddial | | □ read □ update |
| Blocked Learned Pattern | | □ read □ update |
| Blocked Learned Patterns | | □ read □ update |
| Bulk Add/Update Lines | | □ read □ update |
| Bulk Add/Update Phones | | □ read □ update |
| Bulk CUPS User Page | | □ read □ update |
| Bulk Config Tool Export | | □ read □ update |
| Bulk Config Tool Import | | □ read □ update |
| Bulk Config Tool Import Validation | | □ read □ update |
| Bulk Delete Access List | | □ read □ update |
| Bulk Delete Call Pickup Group | | □ read □ update |
| Bulk Delete Client Matter Codes | | □ read □ update |
| Bulk Delete Fallback Profile | | □ read □ update |
| Bulk Delete Forced Authorization Codes | | □ read □ update |

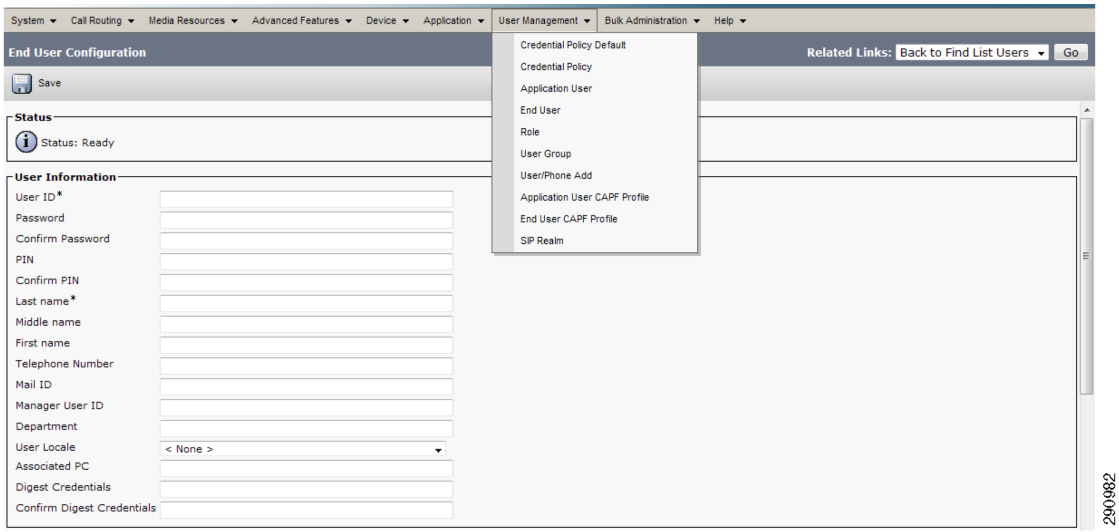
### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution through configuration of local accounts in the database, as shown below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  Sub-requirements 8.1, 8.2, and 8.4 are met by configuring user IDs and passwords in the User Management section of the Cisco Unified Communication manager web interface, as shown in Figure 5-4.

*Figure 5-4 End User Configuration*



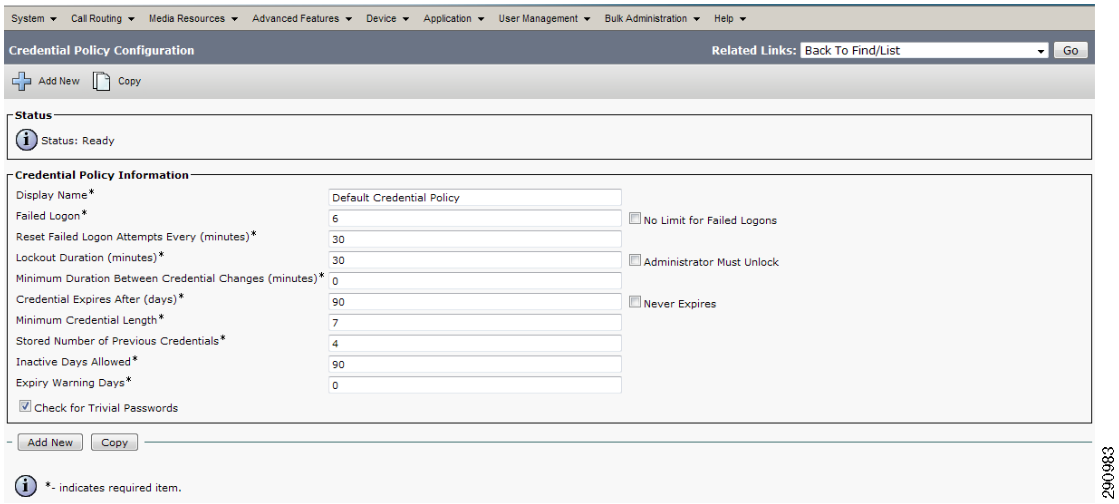
Status: Ready

User Locale: < None >

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Sub-requirements 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, and 8.5.14 are met by configuring a credential policy for user management and applying that policy to a designated group. Figure 5-5 shows a modified default credential policy.

*Figure 5-5 User Credential Policy Configuration*



Credential Policy Configuration

Status

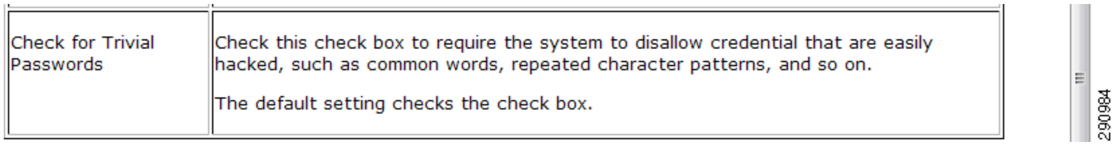
Status: Ready

Credential Policy Information

| | | |
|---|---|---|
| Display Name* | Default Credential Policy | |
| Failed Logon* | 6 | □ No Limit for Failed Logons |
| Reset Failed Logon Attempts Every (minutes)* | 30 | |
| Lockout Duration (minutes)* | 30 | □ Administrator Must Unlock |
| Minimum Duration Between Credential Changes (minutes)* | 0 | |
| Credential Expires After (days)* | 90 | □ Never Expires |
| Minimum Credential Length* | 7 | |
| Stored Number of Previous Credentials* | 4 | |
| Inactive Days Allowed* | 90 | |
| Expiry Warning Days* | 0 | |

☑ Check for Trivial Passwords

*- indicates required item.



| | |
|---|---|
| Check for Trivial Passwords | Check this check box to require the system to disallow credential that are easily hacked, such as common words, repeated character patterns, and so on.<br>The default setting checks the check box. |

The system provides trivial credential checks to disallow credentials that are easily hacked. You enable trivial credential checks by checking the Check for Trivial Passwords check box in the Credential Policy Configuration window.

Passwords can contain any alphanumeric ASCII character and all ASCII special characters. A non-trivial password meets the following criteria:

- Must contain three of the four allowable characteristics: uppercase character, lowercase character, number, and symbol.
- Must not use a character or number more than three times consecutively.
- Must not repeat or include the alias, username, or extension.
- Cannot consist of consecutive characters or numbers (for example, passwords such as 654321 or ABCDEFG)

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

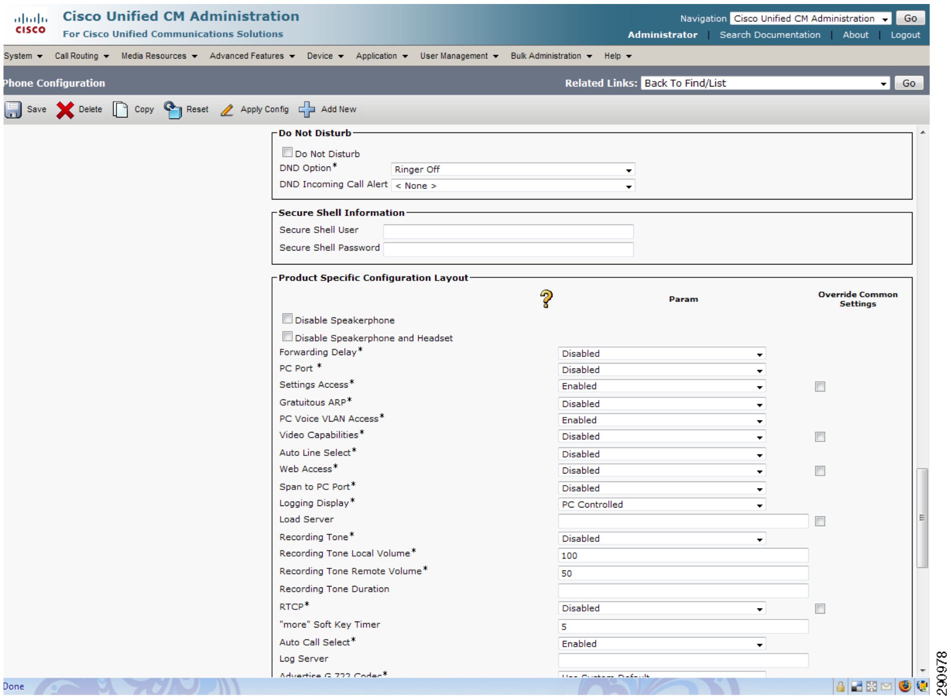
  Sub-requirement 8.5.15 is part of the default system behavior. The system locks the user's session if the session has been idle for fifteen minutes, requiring the user to login again.

### Requirement 9: Restrict Physical Access to Cardholder Data

- **PCI 9.1.2**—*Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.*

  This requirement is met by disabling the PC port setting in the phone configuration window for ports that are not in use, as shown in Figure 5-6.

*Figure 5-6 Phone Configuration*


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
Administrator | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Phone Configuration
Related Links: Back To Find/List Go
Save Delete Copy Reset Apply Config Add New
Done
290978

**Do Not Disturb**

□ Do Not Disturb

| | |
|---|---|
| DND Option* | Ringer Off |
| DND Incoming Call Alert | < None > |

**Secure Shell Information**

| | |
|---|---|
| Secure Shell User | |
| Secure Shell Password | |

**Product Specific Configuration Layout**

□ Disable Speakerphone

□ Disable Speakerphone and Headset

| | Param | Override Common Settings |
|---|---|---|
| Forwarding Delay* | Disabled | |
| PC Port * | Disabled | |
| Settings Access* | Enabled | □ |
| Gratuitous ARP* | Disabled | |
| PC Voice VLAN Access* | Enabled | |
| Video Capabilities* | Disabled | □ |
| Auto Line Select* | Disabled | |
| Web Access* | Disabled | □ |
| Span to PC Port* | Disabled | |
| Logging Display* | PC Controlled | |
| Load Server | | □ |
| Recording Tone* | Disabled | |
| Recording Tone Local Volume* | 100 | |
| Recording Tone Remote Volume* | 50 | |
| Recording Tone Duration | | |
| RTCP* | Disabled | □ |
| "more" Soft Key Timer | 5 | |
| Auto Call Select* | Enabled | |
| Log Server | | |
| Advertise G.722 Codec* | Use System Default | |

### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

The Cisco Unified Communications Manager is able to track and monitor all administrative user access and events.

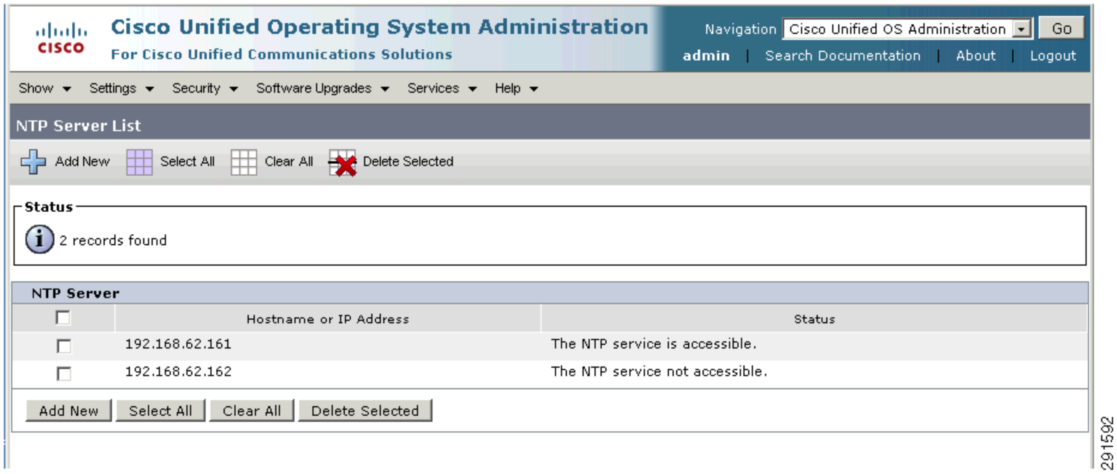
- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco Unified Communication manager uses Network Time Protocol (NTP) to update and synchronize local clock facilities to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. This requirement is met by configuring the NTP server, as shown in Figure 5-7.

***Figure 5-7 NTP Server List***



NTP Server List

Status

2 records found

NTP Server

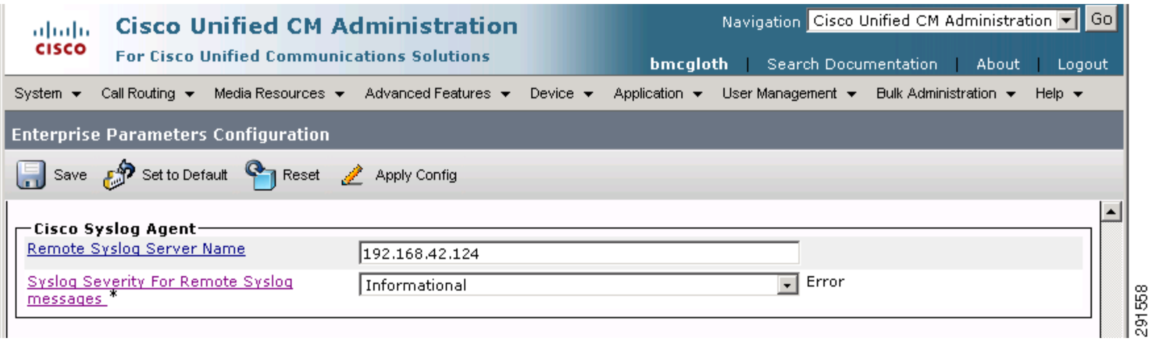
| □ | Hostname or IP Address | Status |
|---|---|---|
| □ | 192.168.62.161 | The NTP service is accessible. |
| □ | 192.168.62.162 | The NTP service not accessible. |

To meet all of the requirements listed below, the PCI solution for retail uses a central logging repository located in the data center. RSA enVision collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  The Cisco Unified Communication Manager can be configured to send the logs to an external syslog server where it cannot be altered by the appliance users. Figure 5-8 and Figure 5-9 show the configurations necessary for log forwarding.

Figure 5-8 Enterprise Parameters Configuration


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
bmcgloth | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Save Set to Default Reset Apply Config
291558

Enterprise Parameters Configuration

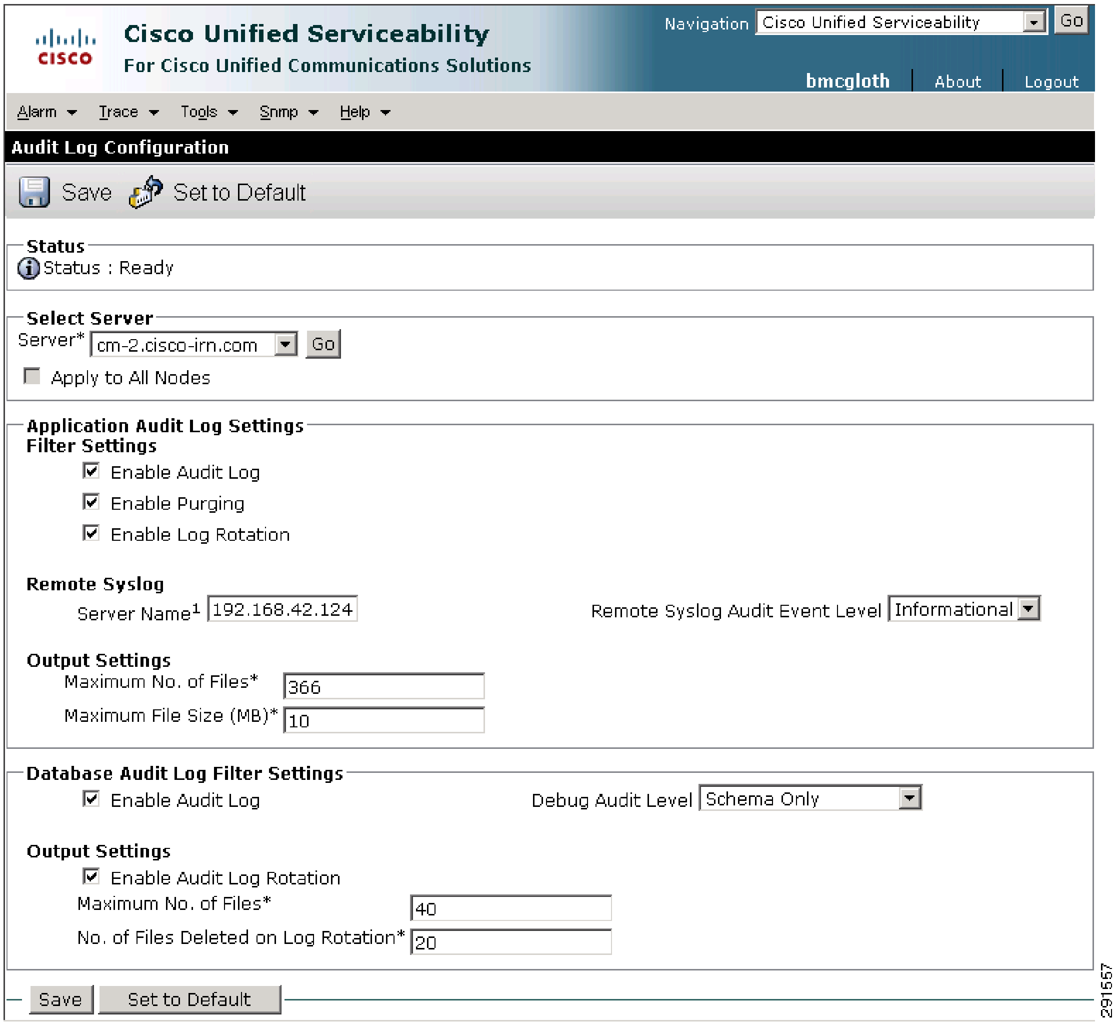
Cisco Syslog Agent

Remote Syslog Server Name: 192.168.42.124

Syslog Severity For Remote Syslog messages *: Informational Error

Figure 5-9 shows the necessary configuration under Cisco Unified Serviceability.

Figure 5-9 Audit Log Configuration


Cisco Unified Serviceability
For Cisco Unified Communications Solutions
Navigation Cisco Unified Serviceability Go
bmcgloth | About | Logout
Alarm Trace Tools Snmp Help
Save Set to Default
Go
Save Set to Default
291567

Audit Log Configuration

Status

Status : Ready

Select Server

Server* cm-2.cisco-irn.com

□ Apply to All Nodes

Application Audit Log Settings

Filter Settings

☑ Enable Audit Log

☑ Enable Purging

☑ Enable Log Rotation

Remote Syslog

Server Name1 192.168.42.124 Remote Syslog Audit Event Level Informational

Output Settings

Maximum No. of Files* 366

Maximum File Size (MB)* 10

Database Audit Log Filter Settings

☑ Enable Audit Log Debug Audit Level Schema Only

Output Settings

☑ Enable Audit Log Rotation

Maximum No. of Files* 40

No. of Files Deleted on Log Rotation* 20

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

# Physical Security

Cisco Physical Security solutions provide broad capabilities in video surveillance, IP cameras, electronic access control, and groundbreaking technology that converges voice, data, and physical security in one modular platform. Cisco Physical Security solutions enable customers to use the IP network as an open platform to build more collaborative and integrated physical security systems while preserving their existing investments in analog-based technology. As customers converge physical security infrastructures and operations and begin using the IP network as the platform, they can gain significant value through rapid access to relevant information and interoperability between systems. This creates a higher level of situational awareness and allows intelligent decisions to be made more quickly.

## Cisco Video Surveillance

Video surveillance technology provides security monitoring capabilities within a store environment. Video surveillance for loss prevention can now be extended into the area of protecting the cardholder data environment.

As the core component of Cisco's video surveillance software portfolio, the Cisco Video Surveillance Media Server offers the power and flexibility to meet a diverse range of video surveillance requirements. The media server:

- Uses IP technology to provide outstanding scalability in terms of sites, cameras, viewers, and storage
- Delivers low-latency, high-quality, event-tagged video
- Supports a broad range of cameras, codecs (such as JPEG, and MPEG-4, and H.264), viewing platforms, and network topologies
- Archives at various frame rates, durations, and locations

Quickly and effectively configure and manage video throughout your enterprise with the Cisco Video Surveillance Operations Manager (VSOM). Working in conjunction with the Cisco Video Surveillance Media Server and Cisco Video Surveillance Virtual Matrix, the Operations Manager meets the diverse needs of administrators, systems integrators, and operators by providing:

- A web-based toolkit for configuration, management, display, and control of video from a wide variety of both Cisco and third-party surveillance endpoints
- Management of a large number of Cisco Video Surveillance Media Servers, Virtual Matrixes, cameras, and users
- Flexible video recording options including motion-based, scheduled, and event-based
- Comprehensive control of users and user roles including scheduling of operator shifts, event filters, and user-specific video views
- Detailed activity reports and system audit

*Table 5-6 PCI Assessment Summary—Cisco Video Surveillance*

| **Models Assessed** | |
|---|---|
| Cisco Video Surveillance Manager version 6.3.1 | |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 9** | 9.1, 9.1.1 |
| **PCI 10** | 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 104.3, 10.5, 10.5.1, 10.5.2, 10.5.3, 10.5.5 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

## Primary PCI Function

The primary function of video surveillance is to monitor physical access to sensitive areas within the cardholder data environment (9.1.1).

Table 5-6 lists the component assessment details for the Cisco Video Surveillance solution.

*Table 5-7 Component Capability Assessment—Cisco Video Surveillance*

| Cisco Video Surveillance | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 9 (9.1.1)** |
| Monitor physical access to sensitive areas within the cardholder environment. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

- Ensure that cameras are positioned to monitor servers or systems within the cardholder data environment.
- Cameras should be appropriately positioned to identify personnel accessing these systems.
- Ensure adequate storage of video for three months.

For more information, see the Cisco IP Video Surveillance Guide at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/IPVS/IPVS_DG/IPVSchap4.html

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2—***Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  The Cisco Video Surveillance Manager includes only the required services, ports, applications, and access required for standard operation of the system. Use the Cisco Video Surveillance Operations Manager Secure Login feature, found within the Administrative Settings, to enable and force secure HTTPS application login.

- **PCI 2.2.4—***Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The Cisco Video Surveillance Manager and Multiservices Platform contain only the required components needed to run the applications. If additional network, software, or platform security customization is required, consult *Securing Video Surveillance Manager: Best Practices and Recommendations* at the following URL: http://www.cisco.com/en/US/docs/security/physical_security/video_surveillance/network/design/bestprac_4_1_6_1.pdf

- **PCI 2.3—***Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  The Cisco Video Surveillance Manager uses SSL for web-based administration and operator access, and uses SSH for remote terminal access. Use the Cisco Video Surveillance Operations Manager Secure Login feature, found within the Administrative Settings, to enable and force secure HTTPS application login. SSH access should be used to securely login to the VSM host.

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Video Surveillance Operations Manager. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at: http://www.cisco.com/cisco/software/navigator.html

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of requirement 7 were met using VSOM's Role-based Access Control (RBAC) system to logically group each user within a role based on their need to know. This restricts unauthorized access and usage of system components. The VSOM RBAC allows granular access control for each system component, including devices such as servers, cameras, and encoders, along with application-level functionality of accessing these resources.

This configuration was used to address the following individual requirements.

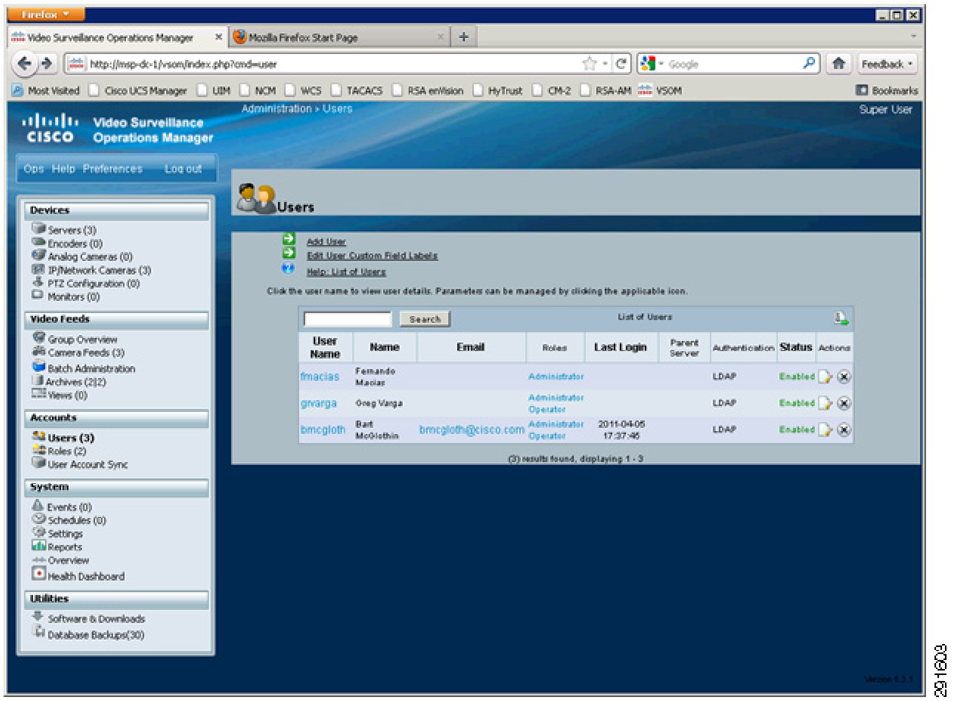
- **PCI 7.1—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:*
  - **PCI 7.1.1—***Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
  - **PCI 7.1.2—***Assignment of privileges is based on individual personnel's job classification and function*
  - **PCI 7.1.3—***Requirement for a documented approval by authorized parties specifying required privileges.*
  - **PCI 7.1.4—***Implementation of an automated access control system*

- **PCI 7.2—***Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:*
  - **PCI 7.2.1—***Coverage of all system components*
  - **PCI 7.2.2—***Assignment of privileges to individuals based on job classification and function*
  - **PCI 7.2.3—***Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  The role configuration menu in Video Surveillance Operations Manager server allows specifying the assignment of privileges based on the role description. No systems access is permitted without an account.

  Individual users and roles are created locally and authentication directed to LDAP, as shown in Figure 5-10.

***Figure 5-10 VSOM Users Authenticate to LDAP Service***



Click the user name to view user details. Parameters can be managed by clicking the applicable icon.

| User Name | Name | Email | Roles | Last Login | Parent Server | Authentication | Status | Actions |
|---|---|---|---|---|---|---|---|---|
| fmacias | Fernando Macias | | Administrator | | | LDAP | Enabled | |
| gvarga | Greg Varga | | Administrator<br>Operator | | | LDAP | Enabled | |
| bmcgloth | Bart McGlothin | bmcgloth@cisco.com | Administrator<br>Operator | 2011-04-05 17:37:46 | | LDAP | Enabled | |

(3) results found, displaying 1 - 3

### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing LDAP connectivity for AAA services and Microsoft Active Directory for user account services. Configure AAA services via LDAP, as shown below.

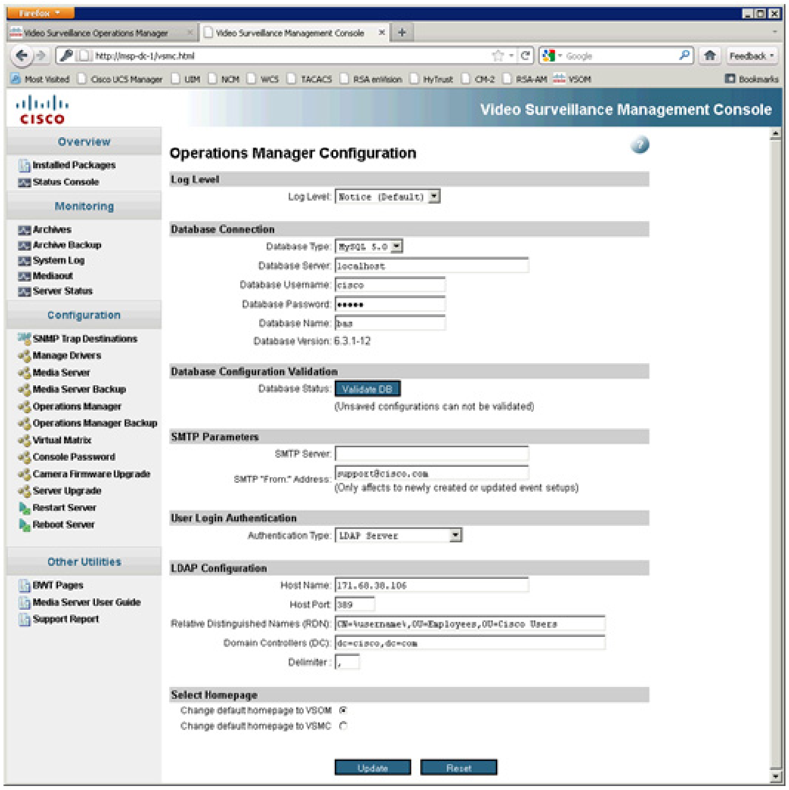
- **PCI 8.1—***Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2—***In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*

- *Something you are, such as a biometric*

- **PCI 8.4—***Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5—***Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9—***Change user passwords at least every 90 days.*
- **PCI 8.5.10—***Require a minimum password length of at least seven characters.*
- **PCI 8.5.11—***Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12—***Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13—***Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14—***Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Using the Video Surveillance Management Console, configure LDAP as specified in the installation guide. Figure 5-11 shows the LDAP configuration implemented for validation.

***Figure 5-11 VSOM LDAP Configuration***



Operations Manager Configuration

Log Level

Log Level: Notice (Default)

Database Connection

Database Type: MySQL 5.0

Database Server: localhost

Database Username: cisco

Database Password: •••••

Database Name: bas

Database Version: 6.3.1-12

Database Configuration Validation

Database Status: Validate DB

(Unsaved configurations can not be validated)

SMTP Parameters

SMTP Server:

SMTP "From:" Address: support@cisco.com

(Only affects to newly created or updated event setups)

User Login Authentication

Authentication Type: LDAP Server

LDAP Configuration

Host Name: 171.68.38.106

Host Port: 389

Relative Distinguished Names (RDN): CN=%username%,OU=Employees,OU=Cisco Users

Domain Controllers (DC): dc=cisco,dc=com

Delimiter : ,

Select Homepage

Change default homepage to VSOM ●

Change default homepage to VSMC ○

Update Reset

- **PCI 8.5.15—***If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

Cisco VSOM has a minimum session timeout of 30 minutes in the configuration for the version validated. Administration time limits would need to be enabled systemically through an active directory policy to the admin workstation desktops, locking them when there is no activity after 15 minutes.

#### Requirement 9: Restrict Physical Access to Cardholder Data

- **PCI 9.1—***Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.*
- **PCI 9.1.1—***Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*

  Physical access to sensitive areas and cardholder data is restricted by solutions in video surveillance management and IP cameras by securing data center facilities and cashier areas within retail stores. This includes video recording options for flexible configuration of video recording archives and low-latency, high-quality, event-tagged video. Also available is the following:

  - A web-based interface for configuration, management, display, and control of video from a wide variety of surveillance and monitoring endpoints
  - Management of a large number of video surveillance media servers, video walls, cameras, and users
  - Comprehensive control of users and user roles including scheduling of operator shifts, event filters, and user-specific video views
  - Detailed activity reports and system audit

#### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco VSOM is able to track and monitor all administrative user access and events.

Cisco VSOM uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*

  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*
- **PCI 10.4—***Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).*
  - **PCI 10.4.2—***Time data is protected.*
  - **PCI 10.4.3—***Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Network Time Protocol (NTP) is supported and must be enabled within both the IP cameras and Video Surveillance Manager.

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects information from all devices to ensure the integrity and correlation of events.

Requirement 10.5 was met using the integrated Log Backup functionality to send the logging data to the RSA enVision server.

- **PCI 10.5—***Secure audit trails so they cannot be altered.*
  - **PCI 10.5.1—***Limit viewing of audit trails to those with a job-related need.*
  - **PCI 10.5.2—***Protect audit trail files from unauthorized modifications.*
  - **PCI 10.5.3—***Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
  - **PCI 10.5.5—***Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  The following configuration script was implemented to send the local log files to the RSA enVision server to be secured and the integrity established:

```
Directory:  /etc/cron.daily
Filename:  ftp-backup-files.cron

#!/bin/sh
FTP_USER=anonymous
FTP_PASS='vsom@cisco.com'
localDIR="/usr/BWhttpd/bas/db/backups"
serverDIR="/vsom_backup/"

cd $localDIR
ftp -n -i 192.168.42.124   <<EOF
user $FTP_USER $FTP_PASS
binary
cd $serverDIR
mput VSOM_MSP-DC-1_backup_20$(date +%y%m%d)*.tar.gz
quit
EOF
exit 0
```

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

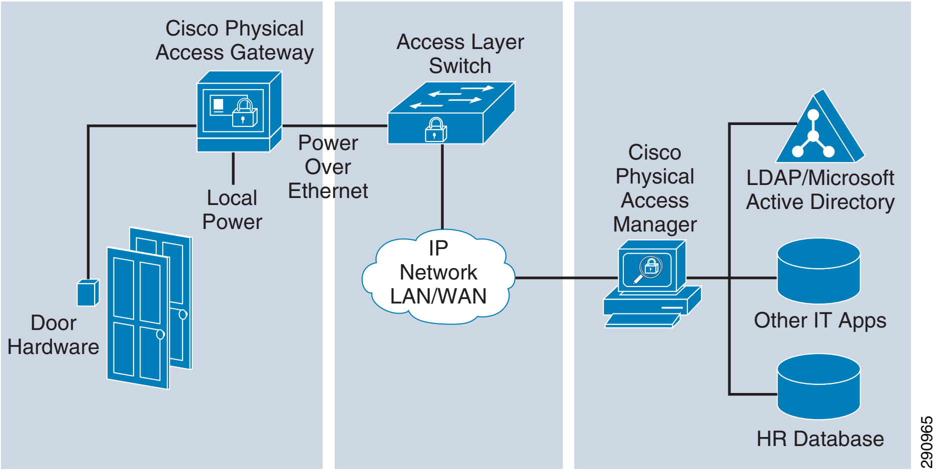
## Cisco Physical Access Control

Cisco Physical Access Control allows retailers to secure their physical doors and locations. Cisco Physical Access Control addresses specific PCI requirements by providing:

- Secure access to the server by supporting secure protocols such as HTTPS and also securing the accounts using strong passwords
- Role-based access to the system by making use of profiles that can restrict access to the modules, depending on the roles
- Automated backup of events to a centralized server
- Ability to archive audit reports on a centralized server

Cisco Physical Access Control is a comprehensive IP-based solution that uses the IP network as a platform for integrated security operations (see Figure 5-12). It works with existing card readers, locks, and biometric devices and is integrated with Cisco Video Surveillance Manager (VSM) and with Cisco IP Interoperability and Collaboration System (IPICS).

*Figure 5-12 Scalable, Modular Architecture*



Cisco Physical Access Control has two components:

- The hardware component, Cisco Physical Access Gateway, provides a modular and scalable platform to connect readers, inputs, and outputs to the system. The gateway scales from a single door to thousands of doors at a fixed cost per door.
- The software component, Cisco Physical Access Manager, manages the hardware, monitors activity, enrolls users, and integrates with IT applications and data stores.

*Table 5-8 PCI Assessment Summary—Cisco Physical Access Manager*

| | |
|---|---|
| **Models Assessed** | |
| Cisco Physical Access Manager version 1.2.0 | |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5, 10.5.1, 10.5.2, 10.5.3, 10.5.5 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

### Primary PCI Function

The primary function of the CPAM appliance is to configure, manage, monitor, and report on the physical doors and door hardware, protecting sensitive areas within the cardholder data environment (9.1).

Table 5-8 lists the component assessment details for Cisco Physical Access Control.

*Table 5-9 Component Capability Assessment—Cisco Physical Access Control*

| Cisco Physical Access Control | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 9 (9.1)** |
| Limit and monitor physical access to sensitive areas within the cardholder data environment. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***“Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

Best practices are as follows:

- Use high availability for Cisco Physical Access Manager (PAM) servers.
- Map each store location and identify the following:
  - Actual doors and modules
  - Door devices and module ports
- Use backup power supply for servers, modules, and devices.
- Cisco PAM was implemented following the Cisco Physical Access Manager Appliance User Guide, Release 1.2.0: http://www.cisco.com/en/US/docs/security/physical_security/access_control/cpam/1_2_0/english/user_guide/cpam_1_2_0.html

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2—***Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

The Cisco PAM appliance can be configured to disable unsecure protocols. To disable unsecure protocols, you must edit one of the configuration files on the Cisco PAM appliance. The step-by-step instructions are as follows:

- SSH into the Cisco PAM server
- sudo su
- Enter the *cpamadmin* password
- /etc/init.d/cpamadmin stop
- Comment out a configuration from the file /opt/cisco/cpam/apache-tomcat/conf/server.xml.

Remove or comment the snippet below.

```
<Connector executor="tomcatThreadPool"
           port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
```

```
/etc/init.d/cpamadmin start
```

When you try to launch the web UI using HTTP, you see “Page cannot be displayed”.

- **PCI 2.2.4—***Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The Cisco PAM appliance operating system includes only the components needed to run the application.

- **PCI 2.3—***Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  On the Cisco PAM appliance, SSL is enabled by default. All the communication between the Cisco PAM client and the gateway is encrypted using the 128-bit AES encryption. Console access to Cisco PAM is through SSH.

#### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco PAM. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

To meet all of the requirements listed below, the PCI solution for retail uses a centralized user database in the Active Directory, which is linked via LDAP, RADIUS, and TACACS+ services. This server is located in the data center. Individual user IDs are assigned, and roles are based on group membership. Cisco Physical Access Manager connects to this resource via LDAP to address the following individual requirements:

- **PCI 7.1—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:*
  - **PCI 7.1.1—***Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
  - **PCI 7.1.2—***Assignment of privileges is based on individual personnel's job classification and function*
  - **PCI 7.1.3—***Requirement for a documented approval by authorized parties specifying required privileges.*
  - **PCI 7.1.4—***Implementation of an automated access control system*

  Role-based access can be configured on Cisco PAM by making use of profiles. Profiles are pre-defined sets of access privileges that define the Cisco PAM modules and commands available to a user. For example, users that should have all privileges can be assigned to the Administrators profile.

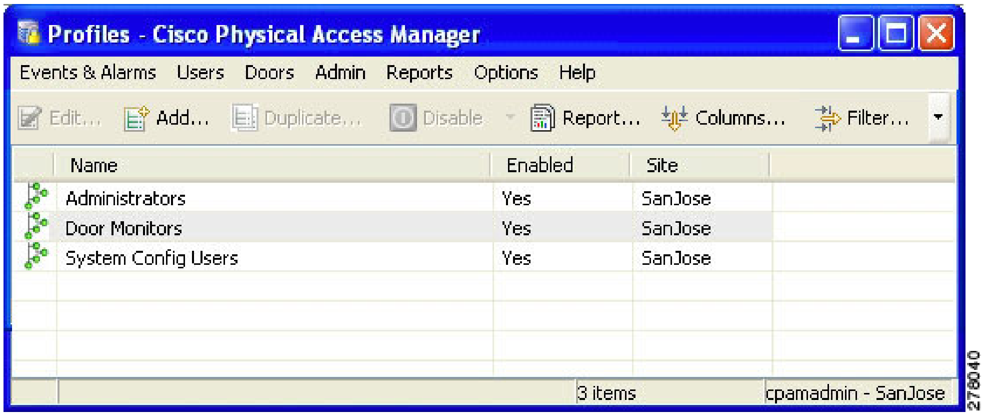
**Note** The Administrator profile is read-only and cannot be changed.

To create profiles, do the following:

**Step 1** Select **Profiles** from the Users menu.

**Step 2** To add a profile, choose **Add**. (See Figure 5-13.)

*Figure 5-13 Profiles Module Main Window*



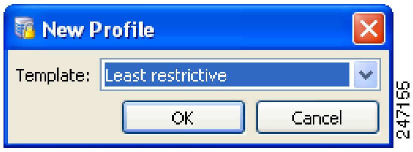
| Name | Enabled | Site |
|---|---|---|
| Administrators | Yes | SanJose |
| Door Monitors | Yes | SanJose |
| System Config Users | Yes | SanJose |

**Note** To modify an existing profile, select the entry and choose **Edit**. To remove a profile, select the entry and choose **Delete**. The Administrator profile is read-only and cannot be changed.

**Step 3** Select a Profile template that most closely matches the desired level of user access, as shown in Figure 5-14:

- Default—A basic set of privileges is set.
- Most Restrictive—No privileges are set.
- Least Restrictive—All privileges are set.

***Figure 5-14 Profile Templates***

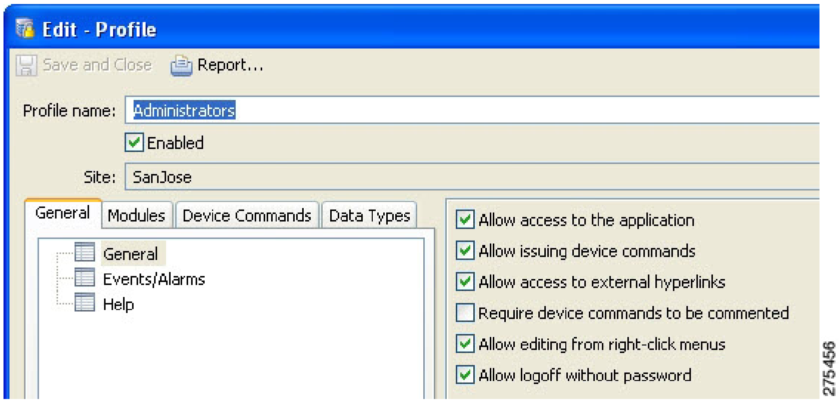


New Profile

Template: Least restrictive

**Step 4** Enter the basic profile settings, as shown in Figure 5-15.

***Figure 5-15 Profile—General Tab***



Edit - Profile

Profile name: Administrators

☑ Enabled

Site: SanJose

☑ Allow access to the application
☑ Allow issuing device commands
☑ Allow access to external hyperlinks
☐ Require device commands to be commented
☑ Allow editing from right-click menus
☑ Allow logoff without password

- Profile name—Enter a descriptive name for the profile.
- Enabled—Select the check box to enable the profile, or deselect the box to disable the profile.
- Partition—Select the partition from the drop-down menu.

**Step 5** Click the **General** tab to define the basic profile properties. Click the checkbox next to each field to enable or disable the privilege, as described in Table 5-10.

***Table 5-10 General Settings—Profile Module***

| Field | Description |
|---|---|
| **General** | |
| *Allow access to the application* | Allows access to the application. |
| *Allow issuing device commands* | Allows user to issue device commands directly to hardware. |
| *Allow access to external hyperlinks* | Allows access to external hyperlinks. |
| *Require device commands to be commented* | Requires the user to enter a comment with each device command issued in the system. |
| *Allow editing from right-click menus* | Allows access to the right-click the Edit menu. |

*Table 5-10 General Settings—Profile Module (continued)*

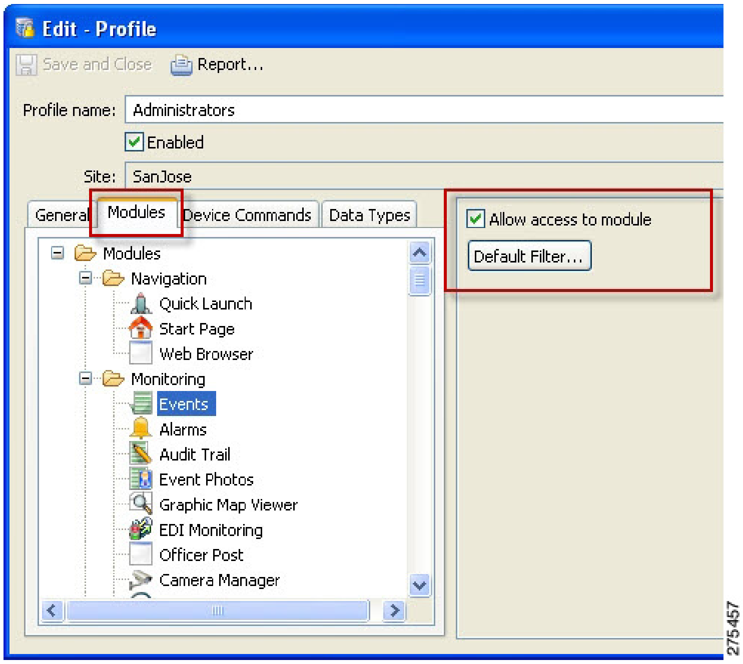
| | |
|---|---|
| *Allow logoff without password* | Allows user to logoff without a password. |
| **Events/Alarms: Alarm Annotations (Ack., Clear, Comment)** | |
| *Allow annotations* | Allows user to acknowledge, clear, and comment alarms. Click the **Filter** button to define the events that trigger the action. |
| *Allow multiple annotations* | Allows the user to acknowledge, clear, and comment multiple alarms at one time. |
| *Allow clearing of unacknowledged alarms* | Allows the user to clear unacknowledged alarms from active devices. |
| *Allow clearing of active device alarms* | Allows the user to clear alarms from active devices. |
| **Events/Alarms—On new alarms** | |
| *Open Alarms Module* | The **Alarms** module automatically opens with new system alarms. Click the **Filter** button to define the events that trigger the action. |
| *Open Manage Alarm window* | The **Alarms** module automatically opens with new system alarms. Click the **Filter** button to define the events that trigger the action. |
| *Open graphic map* | The **Graphic Map** module automatically opens with new system alarms. Click the **Filter** button to define the events that trigger the action. |
| *Show recorded video* | Displays recorded video with new system alarms. Click the **Filter** button to define the events that trigger the action. |
| *Show live video* | Displays live video with new system alarms. Click the **Filter** button to define the events that trigger the action. |
| **Help—Defines access to the various help systems** | |
| *Allow access to help documentation* | Allows access to help documentation. |
| *Enable context menu in help browser* | Allows the user to view the help context menu. |
| *Allow access to help PDF* | Allows the user to access the help PDF.<br>Adobe PDF viewer is required. |

**Step 6** Click the **Modules** tab to define the modules accessible to the profile, as shown in Figure 5-16.

**a.** Select a Cisco PAM module.

**b.** Select **Allow access to module** to enable access to the module.

*Figure 5-16 Profile—Modules Tab*



Edit - Profile

Save and Close | Report...

Profile name: Administrators

☑ Enabled

Site: SanJose

General | Modules | Device Commands | Data Types

- Modules
  - Navigation
    - Quick Launch
    - Start Page
    - Web Browser
  - Monitoring
    - Events
    - Alarms
    - Audit Trail
    - Event Photos
    - Graphic Map Viewer
    - EDI Monitoring
    - Officer Post
    - Camera Manager

☑ Allow access to module

Default Filter...

**c.** (Optional) Use the **Default Filter** with modules such as Event, Badge, and Personnel to define the filter applied when a user opens the module.

For example, to create a profile with access to the Events module that displays events for a specific door by default, complete the following sample steps:

1. Create a profile with access to the Events module, as described in the previous steps.

2. Click **Default Filter**, as shown in Figure 5-16.

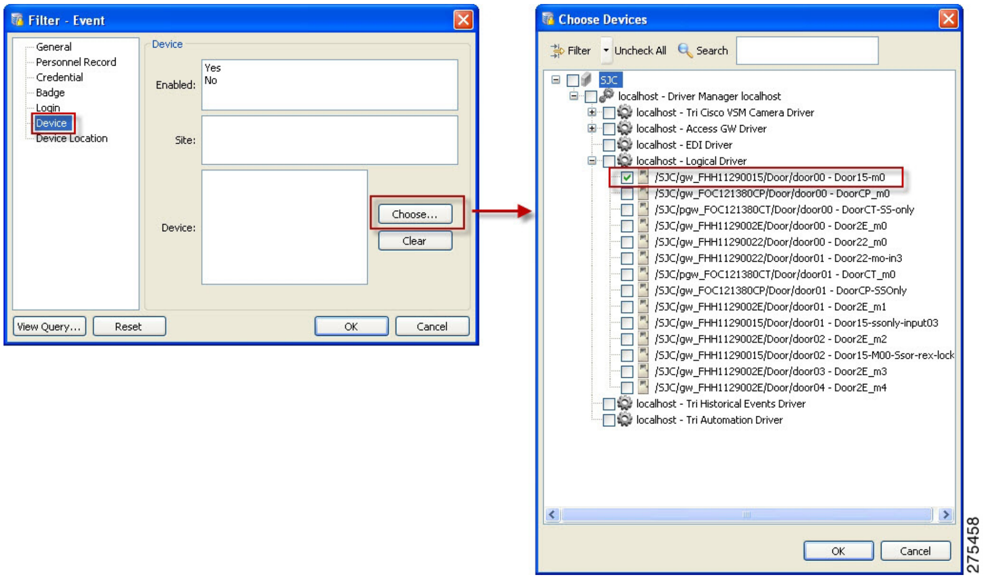
3. Select the **Device** tab, as shown in Figure 5-17.

4. Click **Choose**.

   In the Choose Devices window, expand the Logical Driver device tree and select a door (Figure 5-17).

5. Click **OK** to save the changes and close the windows.

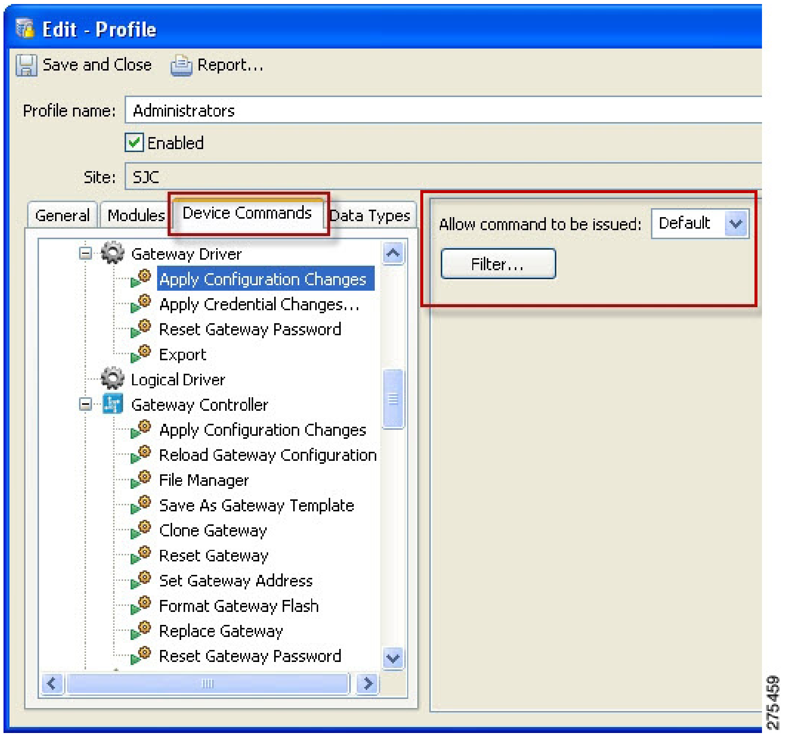
*Figure 5-17 Default Filter: Device Settings*



☐ SJC
☐ localhost - Driver Manager localhost
☐ localhost - Tri Cisco VSM Camera Driver
☐ localhost - Access GW Driver
☐ localhost - EDI Driver
☐ localhost - Logical Driver
☑ /SJC/gw_FHH11290015/Door/door00 - Door15-m0
☐ /SJC/gw_FOC121380CP/Door/door00 - DoorCP_m0
☐ /SJC/pgw_FOC121380CT/Door/door00 - DoorCT-SS-only
☐ /SJC/gw_FHH1129002E/Door/door00 - Door2E_m0
☐ /SJC/gw_FHH11290022/Door/door00 - Door22_m0
☐ /SJC/gw_FHH11290022/Door/door01 - Door22-mo-in3
☐ /SJC/pgw_FOC121380CT/Door/door01 - DoorCT_m0
☐ /SJC/gw_FOC121380CP/Door/door01 - DoorCP-SSOnly
☐ /SJC/gw_FHH1129002E/Door/door01 - Door2E_m1
☐ /SJC/gw_FHH11290015/Door/door01 - Door15-ssonly-input03
☐ /SJC/gw_FHH1129002E/Door/door02 - Door2E_m2
☐ /SJC/gw_FHH11290015/Door/door02 - Door15-M00-Ssor-rex-lock
☐ /SJC/gw_FHH1129002E/Door/door03 - Door2E_m3
☐ /SJC/gw_FHH1129002E/Door/door04 - Door2E_m4
☐ localhost - Tri Historical Events Driver
☐ localhost - Tri Automation Driver

**Step 7** Click the **Device Commands** tab to define the hardware configuration commands available to the user (see Figure 5-18).

*Figure 5-18 Profile—Device Commands Tab*



Profile name: Administrators

☑ Enabled

Site: SJC

Allow command to be issued: Default

- Gateway Driver
  - Apply Configuration Changes
  - Apply Credential Changes...
  - Reset Gateway Password
  - Export
- Logical Driver
- Gateway Controller
  - Apply Configuration Changes
  - Reload Gateway Configuration
  - File Manager
  - Save As Gateway Template
  - Clone Gateway
  - Reset Gateway
  - Set Gateway Address
  - Format Gateway Flash
  - Replace Gateway
  - Reset Gateway Password

**a.** Expand or collapse the list of commands for a device.

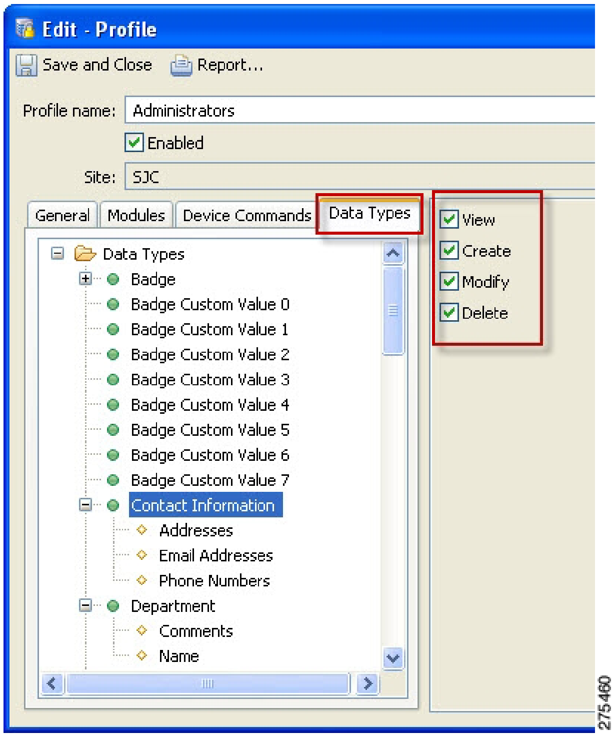
**b.** Highlight a command.

**c.** Select the following options:

- Allow command to be issued:
  - Default—If user has access to issue device commands, the command access is enabled by default.
  - No—Denies access to the command.
  - Yes—Allows access to the command.
- Filter—Apply a filter to limit the devices for the command.

**Step 8** Click the **Data Types** tab to define the data available to the profile, as shown in Figure 5-19.

***Figure 5-19 Profile—Data Types Tab***



Edit - Profile

Save and Close | Report...

Profile name: Administrators

☑ Enabled

Site: SJC

General | Modules | Device Commands | Data Types

- Data Types
  - Badge
  - Badge Custom Value 0
  - Badge Custom Value 1
  - Badge Custom Value 2
  - Badge Custom Value 3
  - Badge Custom Value 4
  - Badge Custom Value 5
  - Badge Custom Value 6
  - Badge Custom Value 7
  - Contact Information
    - Addresses
    - Email Addresses
    - Phone Numbers
  - Department
    - Comments
    - Name

☑ View
☑ Create
☑ Modify
☑ Delete

**a.** Select a module and the type of data in the list.

**b.** To restrict the data, click the check boxes for the properties listed in Table 5-11.

***Table 5-11 Profile—Data Types***

| Field | Description |
|---|---|
| *View* | Allows the user to view the selected data type. |
| *Create* | Allows the user to add and create the selected data types. |
| *Modify* | Allows the user to modify existing data. |
| *Delete* | Allows the user to delete data. |
| *Default Filter...* | Allows the user to apply a default filter to limit objects from view. |

**Step 9** Click **Save and Close** to save the profile settings.

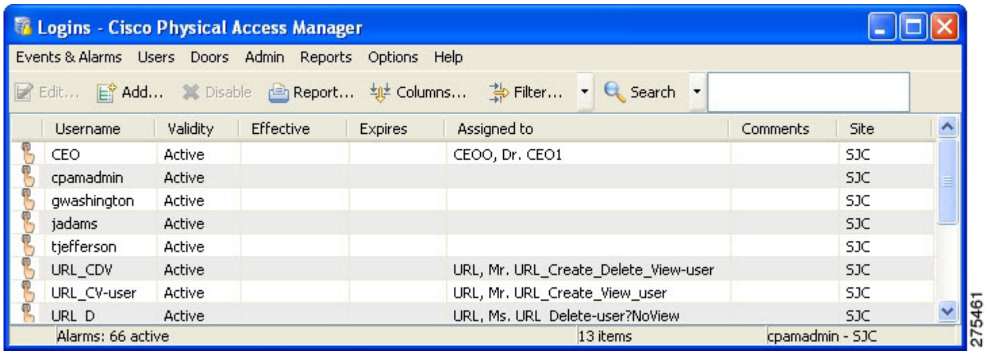
**Step 10** Assign the profile to one or more Cisco PAM operators using the Logins module. (See the following section).

### Creating User Login Accounts and Assigning Profiles

To give users access to Cisco PAM functionality, create a login account and assign one or more access profiles to the username.

**Step 1** Select **Logins** from the Users menu. The main window (Figure 5-20) lists all the usernames in the system.

*Figure 5-20 Logins Module Main Window*



| Username | Validity | Effective | Expires | Assigned to | Comments | Site |
|---|---|---|---|---|---|---|
| CEO | Active | | | CEOO, Dr. CEO1 | | SJC |
| cpamadmin | Active | | | | | SJC |
| gwashington | Active | | | | | SJC |
| jadams | Active | | | | | SJC |
| tjefferson | Active | | | | | SJC |
| URL_CDV | Active | | | URL, Mr. URL_Create_Delete_View-user | | SJC |
| URL_CV-user | Active | | | URL, Mr. URL_Create_View_user | | SJC |
| URL_D | Active | | | URL, Ms. URL_Delete-user?NoView | | SJC |

Alarms: 66 active 13 items cpamadmin - SJC

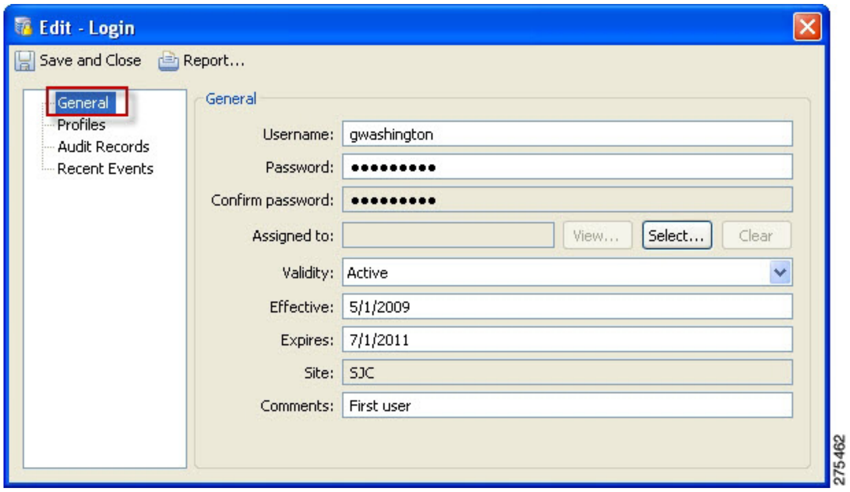
**Step 2** To add a login, choose **Add**.

- To modify an existing login, select the entry and choose **Edit**.
- To remove a login, select the entry and choose **Delete**.

**Note** Most properties of the *cpamadmin* login are read-only.

**Step 3** Complete fields in the General tab, as shown in Figure 5-21. Table 5-12 describes the field properties.

*Figure 5-21 Logins Module—General Tab*



General

Username: gwashington
Password: ●●●●●●●●●
Confirm password: ●●●●●●●●●
Assigned to:
Validity: Active
Effective: 5/1/2009
Expires: 7/1/2011
Site: SJC
Comments: First user

**Note** The Username, Password, and Confirm password fields are required.

*Table 5-12 General Tab Fields*

| Field | Description |
|---|---|
| Username | Required—The username of the login. |
| Password | Required—Password to access the system. |
| Confirm password | Required—The value must be entered exactly as it was in the Password field. |
| Assigned to | The personnel record the login is assigned to.<br>If the login is for an operator already entered in the Personnel module, click the **Select...** button. For more information on adding personnel to the system, see Chapter 8, "Configuring Personnel and Badges" of the CPAM User guide. |
| Validity | Active or Inactive—Only active accounts can access the system. |
| Effective | The beginning date the user can log in—If left blank, the user can log in immediately. |
| Expires | The day the login expires and access is denied—If left blank, access is allowed indefinitely. |
| Site | Read-only—A site is a single instance of a Cisco PAM database. |
| Comments | Comments or notes about the login. |

**Step 4** Assign access privileges for the login:

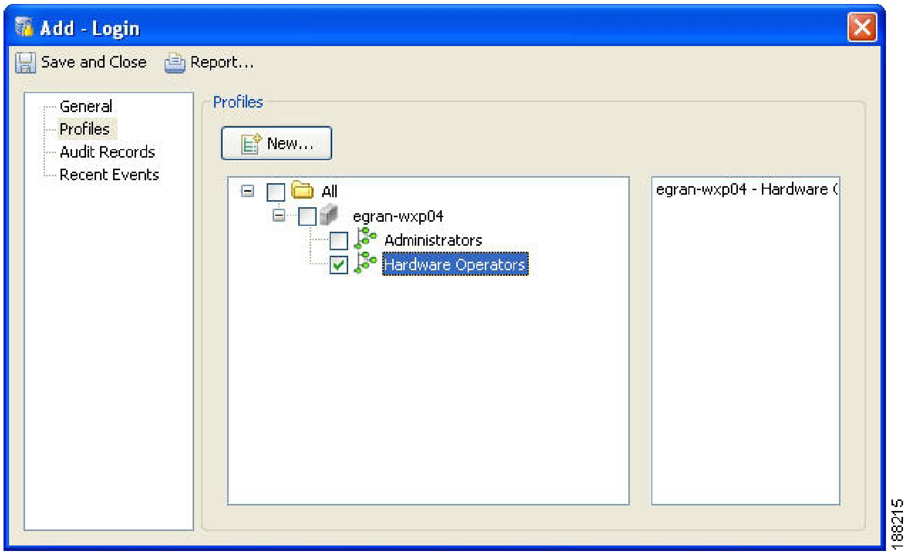
**a.** Select the **Profiles** tab, as shown in Figure 5-22.

**b.** Select the checkbox next to each profile to enable or disable access rights as defined by the access profile. For more information, see Defining User Profiles for Desktop Application Access.

**c.** Click **Save and Close** to save the changes and close the window.

**Tip** To create a new access profile, click the New button to open the Profiles module and refer to Defining User Profiles for Desktop Application Access.

*Figure 5-22 Assigning One or More Profiles*



**Step 5** To verify the changes, log off and then log in with the new username and password. Verify that you can access the modules and functions specified by the assigned profiles.

- **PCI 7.2—***Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:*
  - **PCI 7.2.1—***Coverage of all system components*
  - **PCI 7.2.2—***Assignment of privileges to individuals based on job classification and function*
  - **PCI 7.2.3—***Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco PAM has a default policy of "Deny-all". If a specific badge has to get access to certain set of doors, an access policy must be created.

### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance with the sub-requirements in this section was achieved within the solution by implementing LDAP connectivity for AAA services and Microsoft Active Directory for user account services. Configure AAA services via LDAP, as shown in Requirement 8.2.

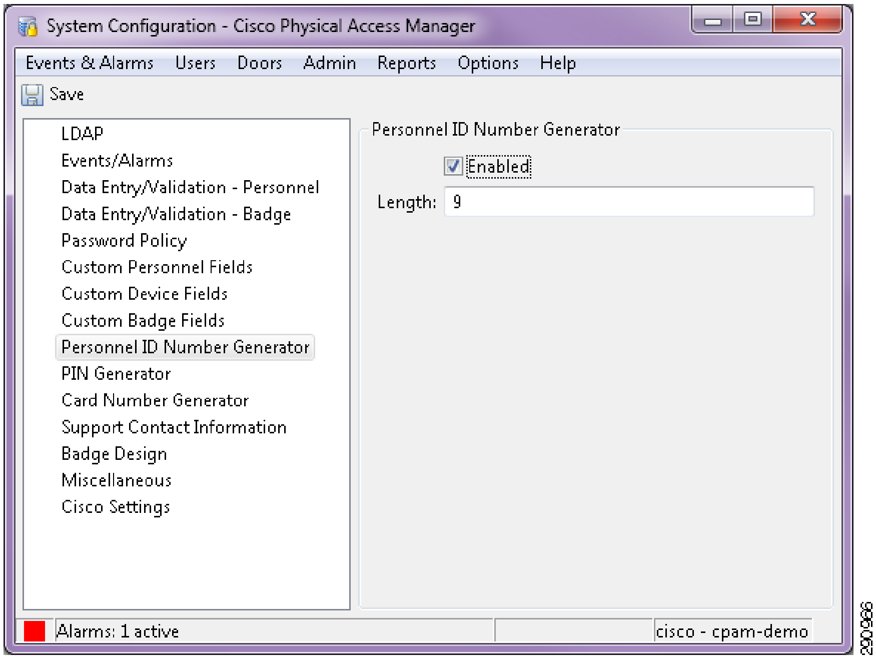
- **PCI 8.1—***Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco PAM integrates with Microsoft Active Directory (MS AD) to pull user information into CPAM. MS AD supports creation of unique ID for users. Cisco PAM has an option to generate a unique number for users using the Personnel ID Number Generator. It is disabled by default. Following are the instructions to enable and use this feature.

**Step 1** On the Cisco PAM client application, open the System Configuration module by clicking **Admin -> System Configuration**.

**Step 2** Click **Personnel ID Number Generator** on the left (see Figure 5-23) and check **Enabled**. Click **Save**.

*Figure 5-23 Using the Personnel ID Number Generator*



Personnel ID Number Generator

☑ Enabled

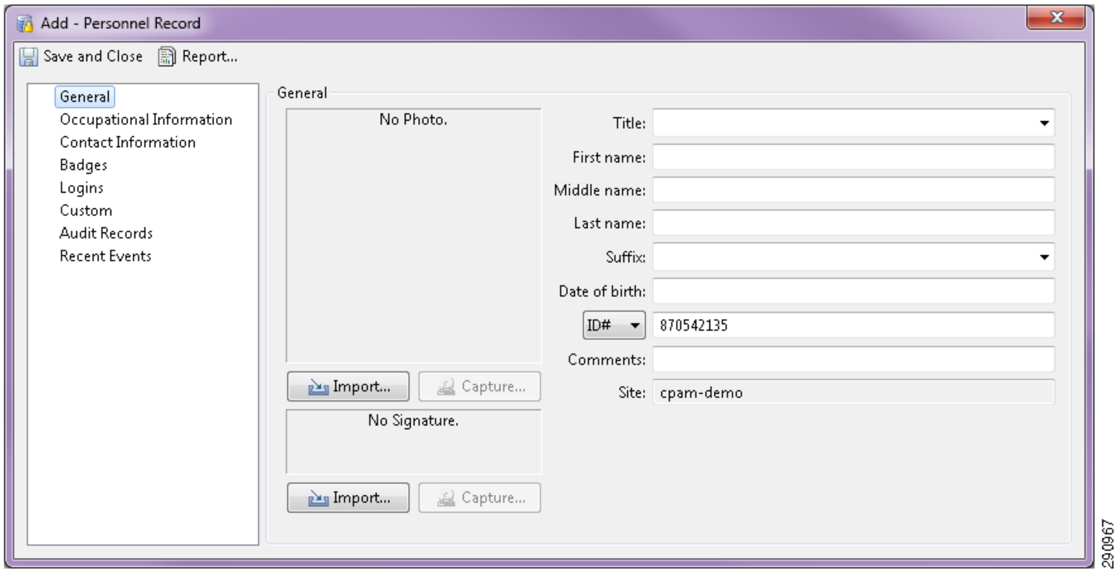
Length: 9

**Step 3** Log out and log back into the Cisco PAM client to get the Personnel ID Number Generator featured working.

**Step 4** Click on **Users -> Personnel**.

**Step 5** Click **Add**. You should see a unique number generated automatically in the ID# field, as shown in Figure 5-24.

*Figure 5-24 Unique ID Number*



General

| | |
|---|---|
| Title: | |
| First name: | |
| Middle name: | |
| Last name: | |
| Suffix: | |
| Date of birth: | |
| ID# | 870542135 |
| Comments: | |
| Site: | cpam-demo |

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Cisco PAM supports authentication through LDAP. Because LDAP supports this feature, Cisco supports the methods listed above.

### Configuring LDAP User Authentication on Cisco PAM

To authenticate users using a Lightweight Directory Access Protocol (LDAP) server, do the following:

1. Configure the LDAP Server
2. Create the LDAP User Account in Cisco PAM

### Configure the LDAP Server

Enter the LDAP server settings to configure the LDAP server connection and user authentication, as described in the following steps.

**Step 1** Select **System Configuration** from the Admin menu, and then select the **LDAP** tab.

**Step 2** Enter the LDAP user authentication settings. The LDAP configuration depends on the authentication mode:

- User principal name (recommended method)—The user principal name is unique in the organization.
- sAMAccountName—The sAMAccount username is unique only in the search domain.

LDAP uses a principle to authenticate. The principle is formed from the username: prefix + username + suffix. The exact format of the principle varies based on the type of LDAP server, and the domain.

For OpenLDAP, the prefix should be: uid=
The suffix should be changed to reflect the actual domain.
So for my-domain.com, this would be:
,dc=my-domain, dc=com

For more information, see the following:

- LDAP Example: User Principal Name
- LDAP Example: sAMAccountName

**Step 3** Enter the other LDAP server settings, as listed in Table 5-13.

*Table 5-13 LDAP System Configuration Settings*

| Field | Description |
|---|---|
| Enable LDAP | Click the checkbox to enable or disable LDAP support. |
| LDAP server URL | URL of LDAP server, must begin with ldap://<br>Example: ldap://192.168.1.1:389<br>**Note** 389 is the port number. |
| Principle suffix | Appended to the username for authentication. See above. |

*Table 5-13 LDAP System Configuration Settings (continued)*

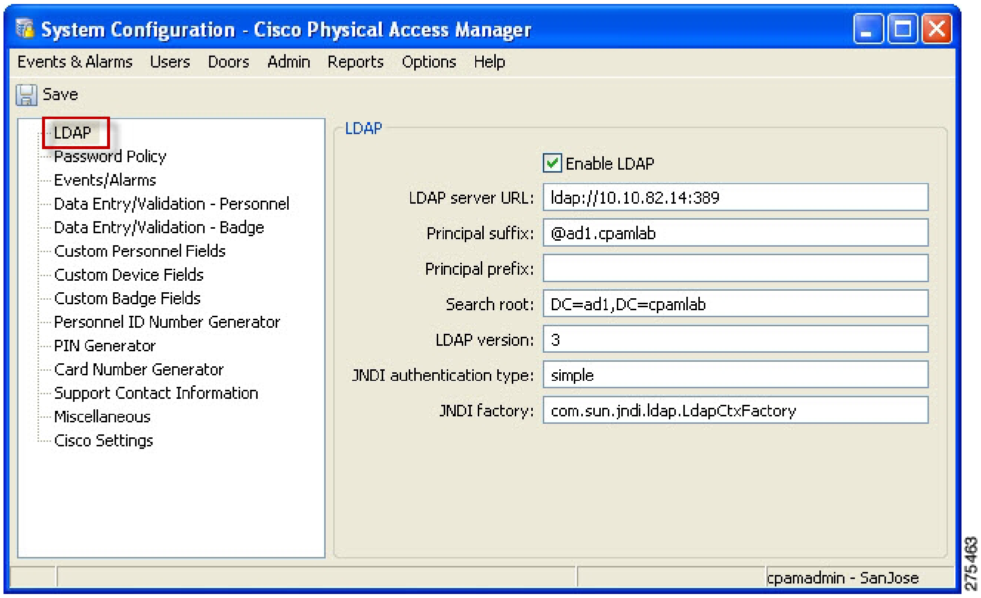
| | |
|---|---|
| Principle prefix | Prepended to the username for authentication. See above. |
| Search root | LDAP search root. The search root is the node in the LDAP tree, the subtree under which the user account should be found.<br>• For Active Directory, the dc components should be changed to match the full domain name managed by the directory. The following example is for my-domain.com: cn=Users, dc=my-domain, dc=com.<br>• For OpenLDAP, the 2 dc components should be changed to match the full domain name managed by the directory. The following example is for my-domain.com:dc=my-domain,dc=com. |
| LDAP version | An advanced setting that generally should be left unchanged. |
| JNDI authentication type | An advanced setting that generally should be left unchanged as simple. |
| JNDI factory | An advanced setting that generally should be left unchanged as com.sun.jndi.ldap.LdapCtxFactory |

**Step 4** Log out and log back in to the Cisco PAM application to enable the changes (select **Logout** from the Options menu).

### LDAP Example—User Principal Name

In the example shown in Figure 5-25, the user principal name is *cpsm.user@ad1.cpamlab*. The Cisco PAM user login must be the same (*cpsm.user*).

*Figure 5-25 User Principal LDAP Configuration Example*



LDAP

☑ Enable LDAP

LDAP server URL: ldap://10.10.82.14:389

Principal suffix: @ad1.cpamlab

Principal prefix:

Search root: DC=ad1,DC=cpamlab

LDAP version: 3

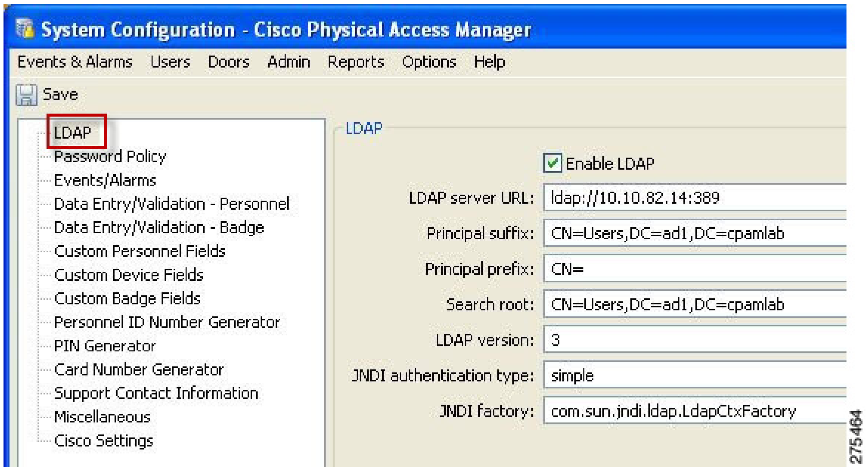
JNDI authentication type: simple

JNDI factory: com.sun.jndi.ldap.LdapCtxFactory

### LDAP Example—sAMAccountName

In the example shown in Figure 5-26, the user login is the same as the samaccount name (*cpsmuser*).

*Figure 5-26 sAMAccountName—LDAP Configuration Example*



☑ Enable LDAP

LDAP server URL: ldap://10.10.82.14:389

Principal suffix: CN=Users,DC=ad1,DC=cpamlab

Principal prefix: CN=

Search root: CN=Users,DC=ad1,DC=cpamlab

LDAP version: 3

JNDI authentication type: simple

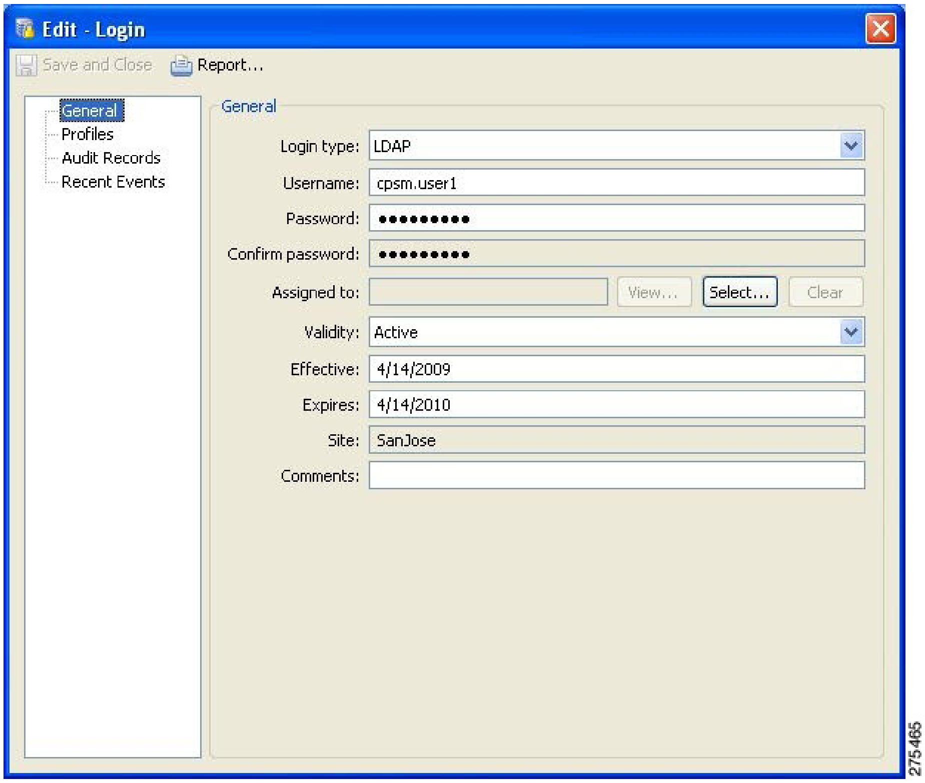
JNDI factory: com.sun.jndi.ldap.LdapCtxFactory

### Creating the LDAP User Account in Cisco PAM

Create the user account to be authenticated using an LDAP server with the following steps.

**Step 1** Select **Logins** from the Users menu. (See Figure 5-27.)

*Figure 5-27 Login Window: LDAP Login Type*



Login type: LDAP

Username: cpsm.user1

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

Assigned to:

Validity: Active

Effective: 4/14/2009

Expires: 4/14/2010

Site: SanJose

Comments:

**Step 2** Click **Add**, or select an existing login and click **Edit**.

**Step 3** Select the Login type **LDAP**. The Login type field appears only if LDAP was enabled and the Cisco PAM application was restarted (see Configure the LDAP Server).

**Step 4** Enter the username, password, and other settings for the LDAP login. See Creating User Login Accounts and Assigning Profiles.

**Note** Although a password must be entered for all user Login records, it is not used for LDAP authentication. LDAP servers use the password entered when the user logs in to Cisco PAM.

**Step 5** Click **Profiles** and select the user's Cisco PAM profiles. See Defining User Profiles for Desktop Application Access for more information.

**Note** Cisco PAM does not synchronize the LDAP profiles.

**Step 6** Click **Save and Close**.

The following requirements (8.4, 8.5.5, 8.5.9–14) are all met through the use of LDAP as the authentication services:

- **PCI 8.4—***Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5—***Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9—***Change user passwords at least every 90 days.*
- **PCI 8.5.10—***Require a minimum password length of at least seven characters.*
- **PCI 8.5.11—***Use passwords containing both numeric and alphabetic characters.PCI Sub-Requirements with Compensating Controls*
- **PCI 8.5.12—***Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13—***Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14—***Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15—***If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco PAM has a hard-coded session timeout of 30 minutes in the configuration for the version validated. Administration time limits would need to be enabled systemically through an active directory policy to the admin workstation desktops, locking them when there is no activity after 15 minutes.

### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco PAM is able to track and monitor all administrative user access and events to meet the following requirements**:**

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*

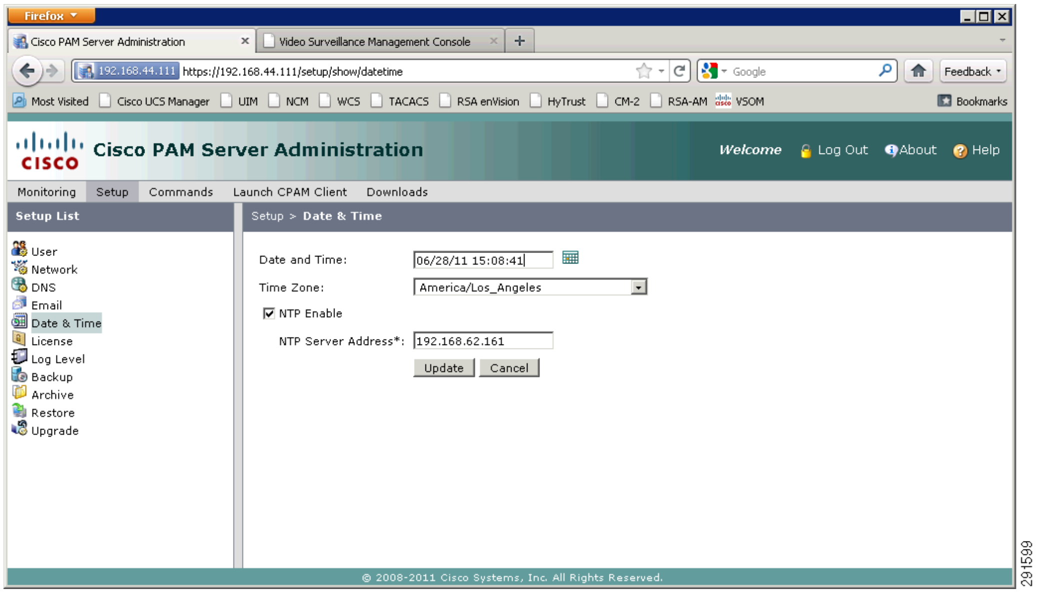
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco PAM and the gateways use the local clock facilities to meet the following requirements**:**

- **PCI 10.4.2—***Time data is protected.*
- **PCI 10.4.3—***Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. All the events in the Access Control system have a time stamp associated to them. Cisco PAM and the gateway are configured to use NTP, as shown in Figure 5-28.

***Figure 5-28 Cisco PAM NTP Configuration***



Date and Time: 06/28/11 15:08:41

Time Zone: America/Los_Angeles

☑ NTP Enable

NTP Server Address*: 192.168.62.161

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects logging information from all devices to ensure the integrity and correlation of events.

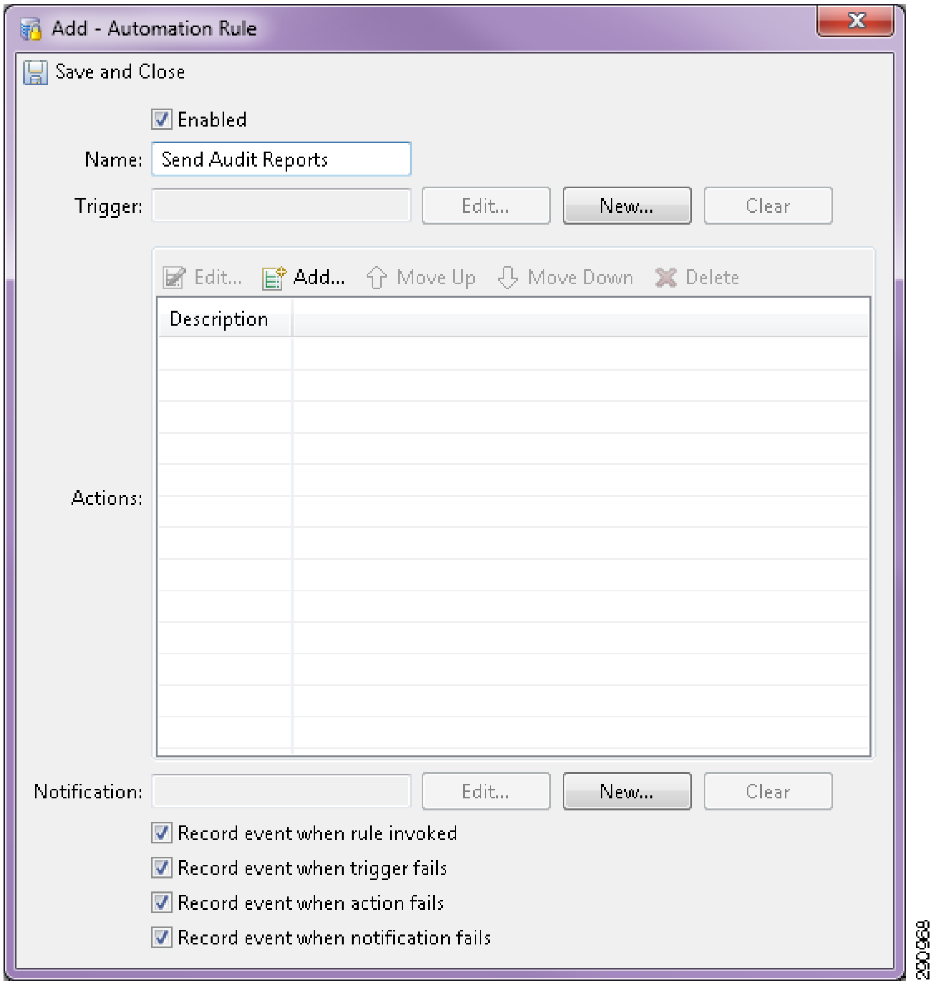
- **PCI 10.5—***Secure audit trails so they cannot be altered.*
- **PCI 10.5.1—***Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2—***Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3—***Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5—***Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  Cisco PAM allows for the creation of global I/O rules to trigger sending audit reports to a centralized server. Following are the instructions to create a global I/O with audit reports.

**Step 1** In the Cisco PAM client, click **Events & Alarms -> Global I/O > Add**.

**Step 2** Enter a name and click **New** in the Trigger field. (See Figure 5-29.)

***Figure 5-29 Creating a Global I/O with Audit Reports***



Add - Automation Rule

☑ Enabled

Name: Send Audit Reports

Trigger:

Notification:

☑ Record event when rule invoked

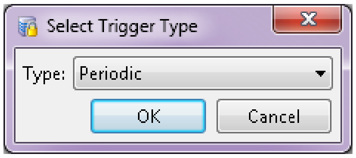
☑ Record event when trigger fails

☑ Record event when action fails

☑ Record event when notification fails

**Step 3** Select **Periodic** and click **OK**. (See Figure 5-30.)

***Figure 5-30 Selecting Periodic***

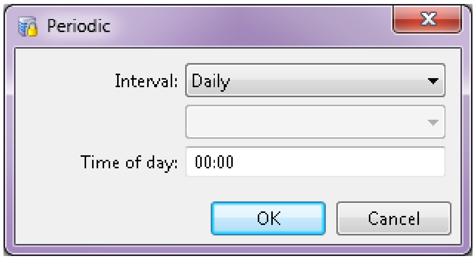


Select Trigger Type

Type: Periodic

**Step 4** Choose the Interval and enter the Time of Day. Click **OK**. (See Figure 5-31.)

***Figure 5-31 Selecting Interval and Time of Day***



Periodic

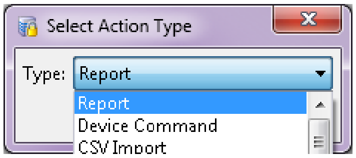
Interval: Daily

Time of day: 00:00

**Step 5** Under Actions, Click **Add…**

**Step 6** Select **Report.** (See Figure 5-32.)

***Figure 5-32 Selecting Action Type***

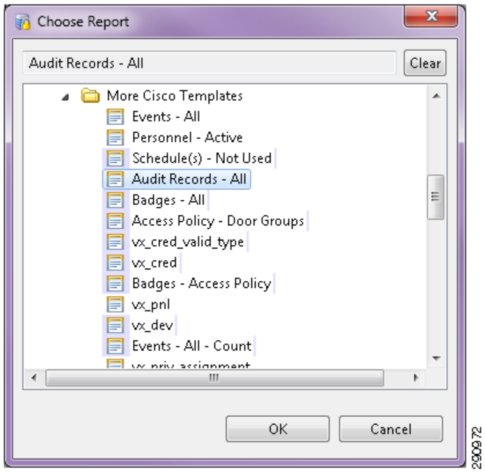


Select Action Type

Type: Report

**Step 7** Choose **Audit Records–All** and click **OK**. (See Figure 5-33.)

***Figure 5-33 Audit Records–All***

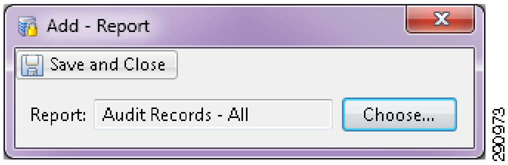


Choose Report

Audit Records - All

**Step 8** Click **Save and Close**. (See Figure 5-34.)

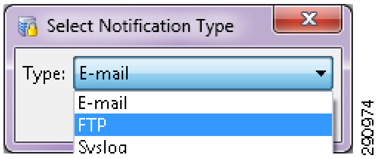
*Figure 5-34 Save and Close*



Report: Audit Records - All

**Step 9** Under Notification section of the Global I/O, click **New** and Choose **FTP**. Click **OK**. (See Figure 5-35.)

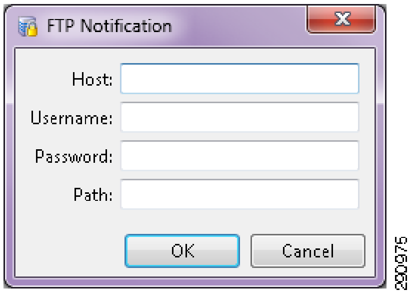
*Figure 5-35 Select Notification Type*



Type: E-mail

**Step 10** Enter the FTP Host, Username, Password, and Path. Click **OK**. (See Figure 5-36.)

*Figure 5-36 FTP Notification*



**Step 11** Click **Save and Close**. You should see a new entry created. You can create similar global I/O rules for every hour.

The audit report is read into RSA enVision server, which then maintains and protects the integrity of the file.

## PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

## PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

# E-mail

## Cisco IronPort Email Security Solution

Cisco IronPort Email Security Solution uses data loss prevention (DLP) technology to block e-mail that is inadvertently sent containing cardholder data information.

**Note** The Cisco IronPort Email Security Solution was initially reviewed by Verizon Business and determined to be outside the scope of the PCI Audit. There is no Assessment Summary or Capability Assessment details for this product. However, Cisco IronPort Email Security Solution could potentially store or transmit sensitive cardholder data if used with the default settings for message tracking. Sensitive information in messages would be automatically forwarded in clear text to administrators, and recipients. These same messages would also be stored un-encrypted. The design considerations below detail how to properly configure the Cisco IronPort Email Security Solution to avoid this pitfall.

Cisco IronPort Email Security Solution provides sophisticated and scalable mechanisms that help to minimize the downtime associated with e-mail-borne malware and simplify the administration of corporate e-mail systems, while offering insight into the e-mail system operation. Capabilities include the following:

- Spam protection
- Data loss prevention (DLP)
- Virus defense
- E-mail encryption tracking and reporting tools

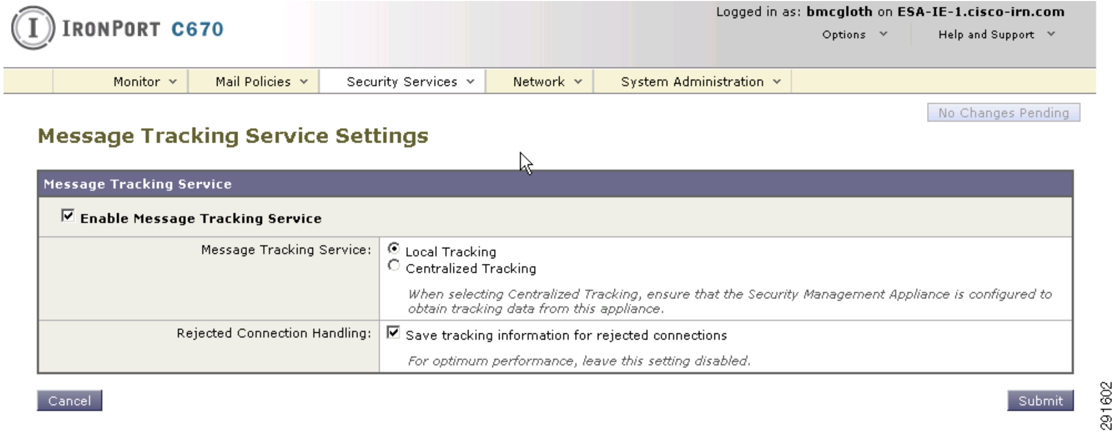
### Primary PCI Function

Although data loss prevention is not covered by a specific PCI requirement, Cisco IronPort Email Security Solution helps in achieving PCI compliance by preventing the transmission of cardholder data over open public networks via e-mail.

### Design Considerations

- Do not enable logging, storage, or forwarding messages identified as containing cardholder data.
- For IronPort to analyze messages passing through it, message tracking must be enabled, as shown in Figure 5-37.

*Figure 5-37 Enable IronPort Message Tracking*



Message Tracking Service Settings

Message Tracking Service

☑ Enable Message Tracking Service

Message Tracking Service: ● Local Tracking ○ Centralized Tracking

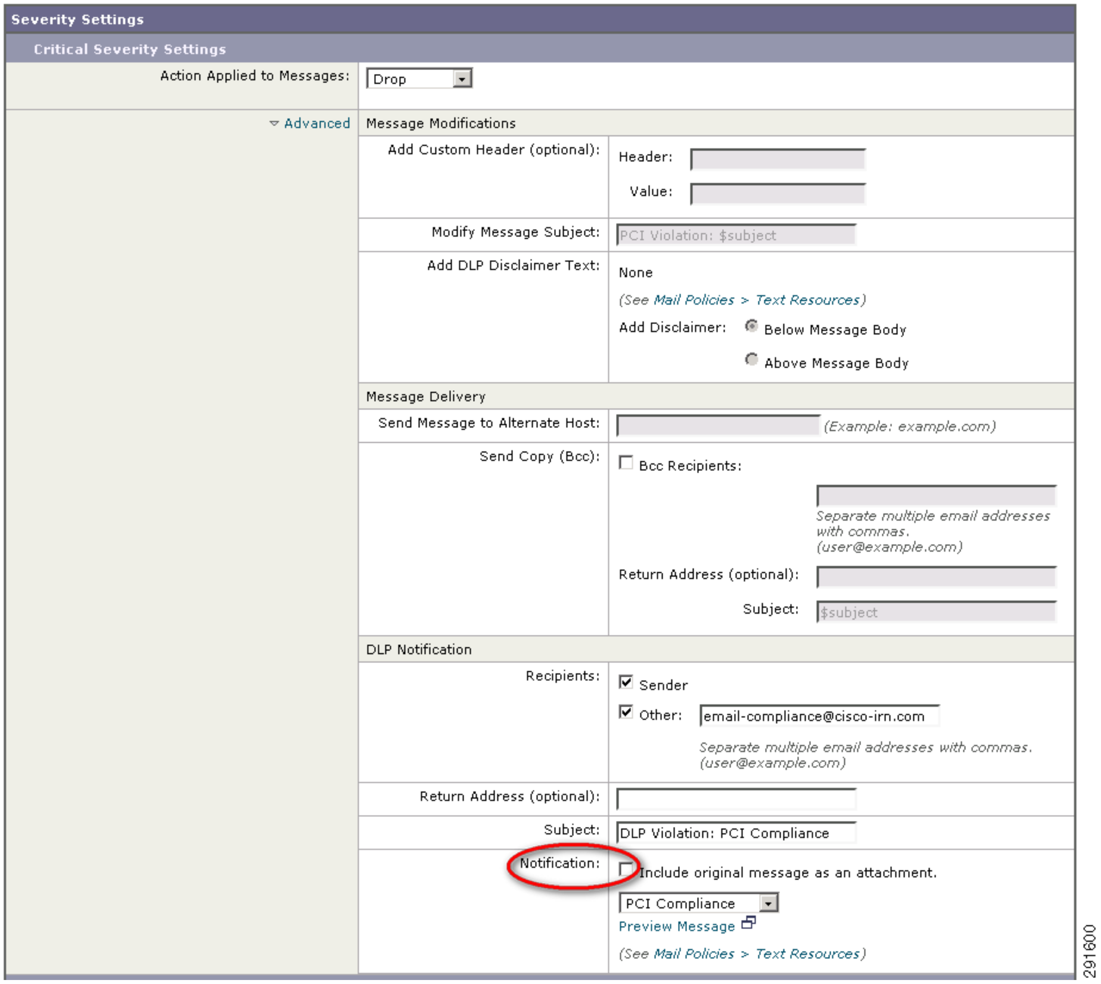
*When selecting Centralized Tracking, ensure that the Security Management Appliance is configured to obtain tracking data from this appliance.*

Rejected Connection Handling: ☑ Save tracking information for rejected connections

*For optimum performance, leave this setting disabled.*

- Create policy in IronPort to drop messages containing credit card numbers, but not to forward that message to administrators. Ensure that the “include original message” checkbox is not selected, as shown in Figure 5-38.

*Figure 5-38 Policy in IronPort Excluding Original Message*



Severity Settings

Critical Severity Settings

Action Applied to Messages: Drop

Message Modifications

Add Custom Header (optional): Header: Value:

Modify Message Subject: PCI Violation: $subject

Add DLP Disclaimer Text: None

*(See Mail Policies > Text Resources)*

Add Disclaimer: ● Below Message Body ○ Above Message Body

Message Delivery

Send Message to Alternate Host: *(Example: example.com)*

Send Copy (Bcc): □ Bcc Recipients:

*Separate multiple email addresses with commas. (user@example.com)*

Return Address (optional):

Subject: $subject

DLP Notification

Recipients: ☑ Sender

☑ Other: email-compliance@cisco-irn.com

*Separate multiple email addresses with commas. (user@example.com)*

Return Address (optional):

Subject: DLP Violation: PCI Compliance

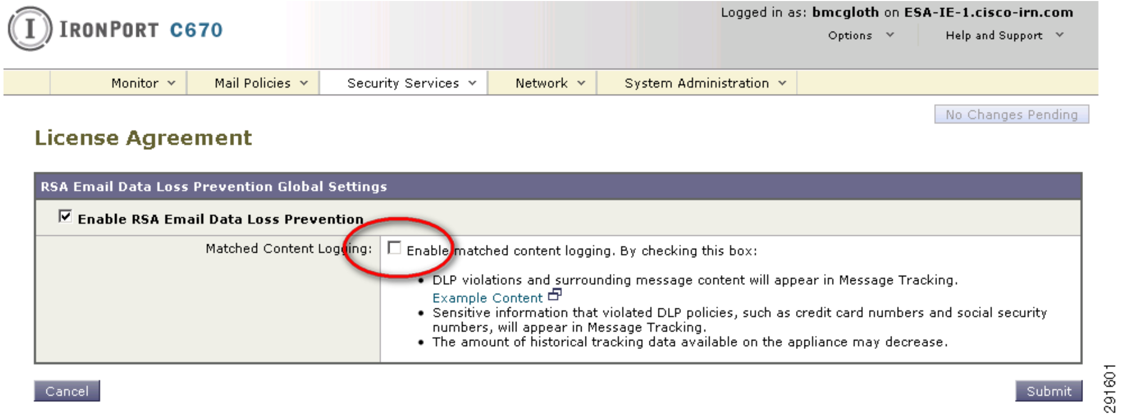
Notification: □ Include original message as an attachment.

PCI Compliance

*(See Mail Policies > Text Resources)*

- To ensure that messages identified as containing credit card information are not stored in the local system, you must disable logging of matched content, as shown in Figure 5-39. The local log of the IronPort server is not a safe encrypted place to store cardholder data.

*Figure 5-39 IronPort DLP—Matched Content Logging Disabled*



License Agreement

RSA Email Data Loss Prevention Global Settings

☑ Enable RSA Email Data Loss Prevention

Matched Content Logging: ☐ Enable matched content logging. By checking this box:

- DLP violations and surrounding message content will appear in Message Tracking. Example Content
- Sensitive information that violated DLP policies, such as credit card numbers and social security numbers, will appear in Message Tracking.
- The amount of historical tracking data available on the appliance may decrease.

# Hosts

## Cisco Unified Computing System

The Cisco Unified Computing System (UCS) is used to securely deploy sensitive and compliance-related applications. Provisioning options, including virtualization technology, allow the mixing of sensitive and non-sensitive applications without compromising scope boundaries.

Improve IT responsiveness to rapidly changing business demands with this next-generation data center platform. Cisco UCS accelerates the delivery of new services simply, reliably, and securely through end-to-end provisioning and migration support.

Benefits include the following:

- Streamlines data center resources to reduce total cost of ownership
- Scales service delivery to increase business agility
- Radically reduces the number of devices requiring setup, management, power, cooling, and cabling

*Table 5-14 PCI Assessment Summary—Cisco UCS*

| **Models Assessed** | |
|---|---|
| Cisco UCS Manager version 1.3(1p) | |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |

*Table 5-14 PCI Assessment Summary—Cisco UCS (continued)*

| | |
|---|---|
| **PCI 10** | 10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

## Primary PCI Function

The main function of Cisco UCS is to securely host one primary compliance-related function per physical or virtual server.

It provides segmentation of sensitive applications from out-of-scope applications via physical and virtualization technology. Although technically, a firewall or ACL is used to enforce PCI Requirement 1, Cisco UCS extends Layer 3 boundaries to virtual network and storage adapters within the chassis. Using VLANs and VSANs, Cisco UCS allows a retailer to separate its payment systems (in-scope) from other non-sensitive data (out-of-scope).

Table 5-14 lists the component assessment details for Cisco UCS.

*Table 5-15 Component Capability Assessment—Cisco Unified Computing System*

| Cisco Unified Computing System | |
|---|---|
| PRIMARY FUNCTION | Requirement N/A |
| Securely host payment applications. | |
| CAPABILITY | ASSESSMENT |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

### Design Considerations

- Cisco UCS allows for the provisioning of individual servers on blades. Each blade can host a native operating system such as Windows 2008 server, or a virtualization hypervisor system such as VMware ESX/ESXi. These provisioning options represent a primary function for the server blade. In the lab validation, VMware ESX was installed on each of the Cisco UCS blades, and several VM hosts were then configured, each with one primary function. Each server blade is provisioned via a profile. Profiles can be created locally in Cisco UCS Manager or centrally using the Vblock provisioning utility, Unified Infrastructure Manager (UIM), which provides simplified Vblock management by combining provisioning with configuration, change, and compliance management.
- EMC SAN is a primary component of the VCE architecture for Vblock Infrastructure Platforms. Vblock 1 is designed for medium to high numbers of virtual machines, and is ideally suited to a broad range of usage scenarios, including shared services, e-mail, file and print, virtual desktops, and collaboration.
- Cisco UCS allows for the provisioning of individual servers on blades. Each blade can host a native operating system such as Windows 2008 server, or a virtualization hypervisor system such as VMware ESX/ESXi.
- Each Cisco UCS server blade is provisioned via a profile. Profiles can be created locally in Cisco UCS Manager or centrally using the Vblock provisioning utility, EMC Unified Infrastructure Manager (UIM), which provides simplified Vblock management by combining provisioning with configuration, change, and compliance management.
- The PCI standard requires one primary function per server. When using virtualization technology, the single primary server function is extended to individual virtual machines.
- The hypervisor of an individual blade is considered insecure for segmenting scopes of compliance. Therefore, when putting non-sensitive VM servers with sensitive VM servers on the same physical blade, the non-sensitive would be included in the scope of the audit.
- The UCS system securely segments network and storage to each blade, which allows mixing of sensitive and non-sensitive applications across different physical blades of the chassis.
- PCI requires a 15-minute timeout for administrative functions. Cisco UCS does not feature an explicit session timeout. Administration time limits would need to be enabled systemically through active directory policy to the admin workstation desktops, locking them when there is no activity.

  Cisco UCS was implemented using the Cisco UCS installation guides: http://www.cisco.com/en/US/products/ps10276/prod_installation_guides_list.html

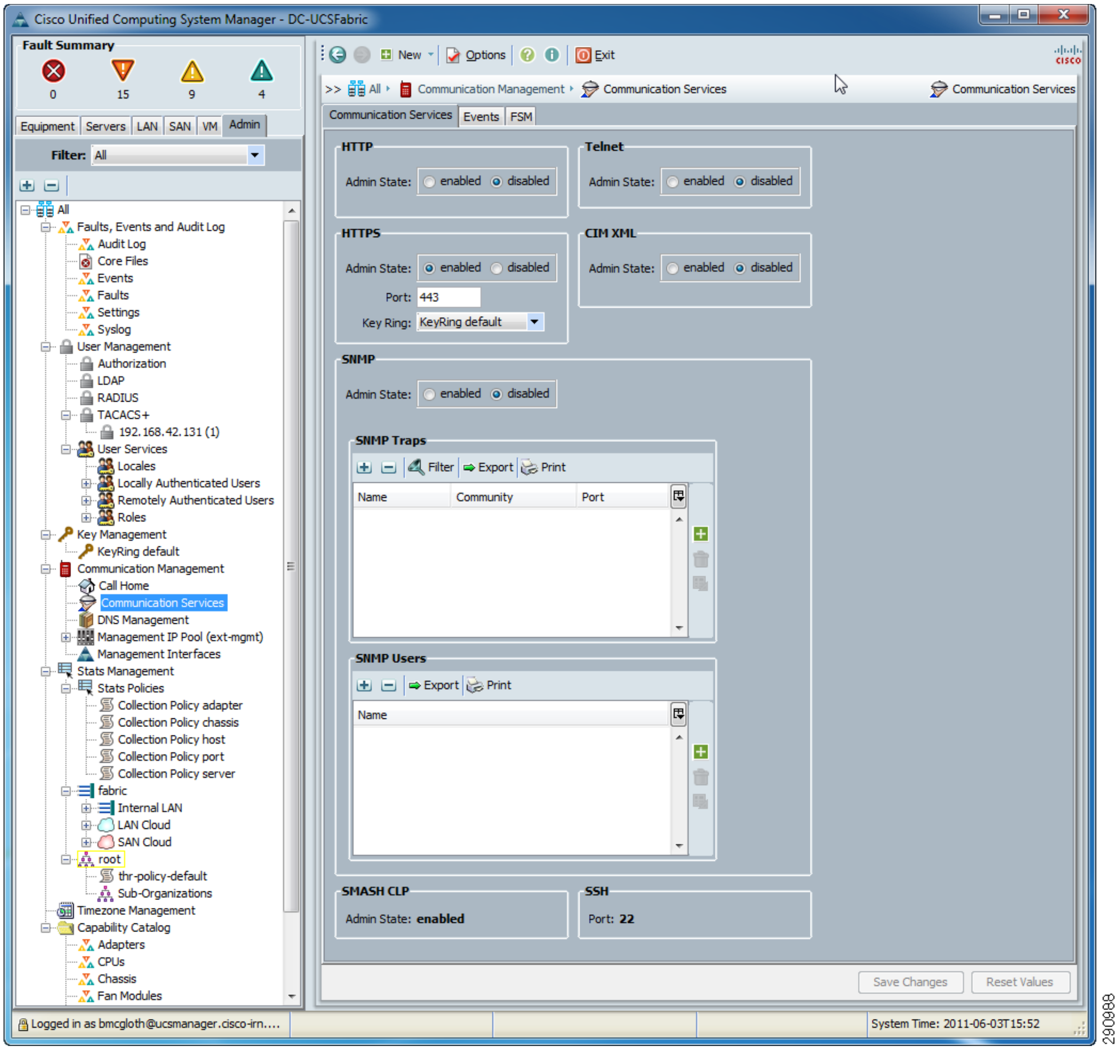
### PCI Assessment Detail—PCI Sub-Requirements Satisfied

#### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco UCS allows for the disabling of non-secure administrative interfaces. Figure 5-40 shows the secure management protocols of SSH and HTTPS for administration. Telnet, HTTP, and other unused protocols are disabled.

*Figure 5-40 Secure Management Protocols*



**HTTP**
Admin State: ○ enabled ● disabled

**Telnet**
Admin State: ○ enabled ● disabled

**HTTPS**
Admin State: ● enabled ○ disabled
Port: 443
Key Ring: KeyRing default

**CIM XML**
Admin State: ○ enabled ● disabled

**SNMP**
Admin State: ○ enabled ● disabled

**SMASH CLP**
Admin State: **enabled**

**SSH**
Port: **22**

Logged in as bmcgloth@ucsmanager.cisco-irn....
System Time: 2011-06-03T15:52

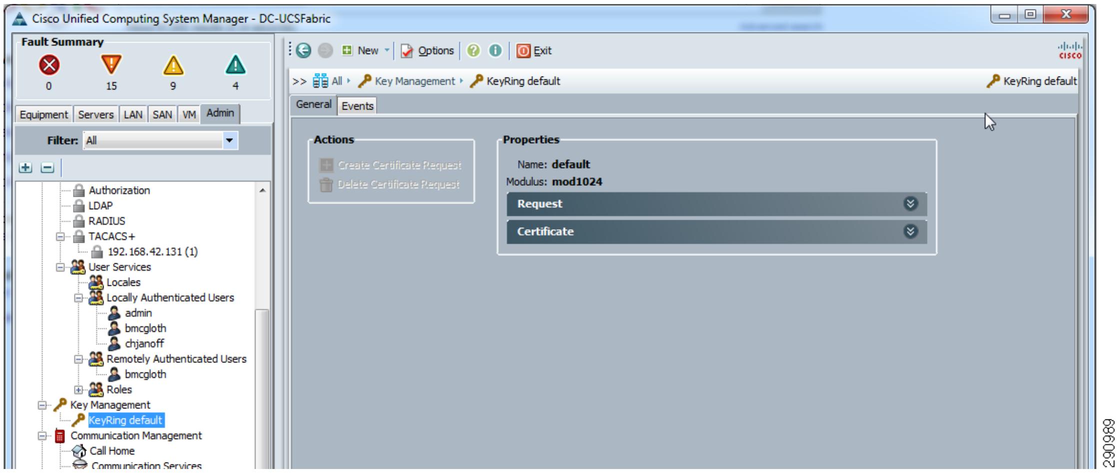
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco UCS does not have any unnecessary services enabled by default.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco UCS uses strong encryption for SSH and HTTPS connections. Encryption keys are created and managed under the Key Management feature. (See Figure 5-41.)

*Figure 5-41 1024-Bit Mod Key Default Keyring*



Name: default
Modulus: mod1024

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco UCS. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at: http://www.cisco.com/cisco/software/navigator.html

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

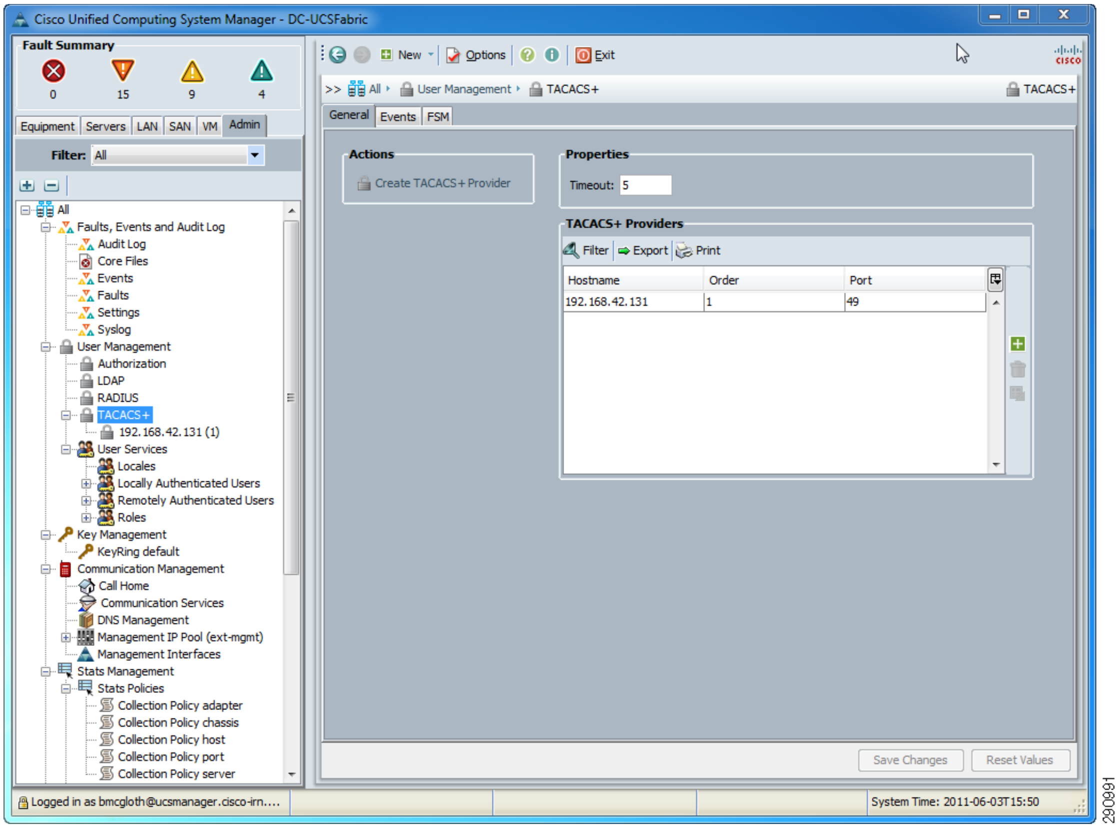
The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*

- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Add the Cisco Secure ACS server under the TACACS+ protocol option, as shown in Figure 5-42.

***Figure 5-42 Adding the Cisco Secure ACS Server***



Cisco Unified Computing System Manager - DC-UCSFabric

>> All ▸ User Management ▸ TACACS+

Properties

Timeout: 5

TACACS+ Providers

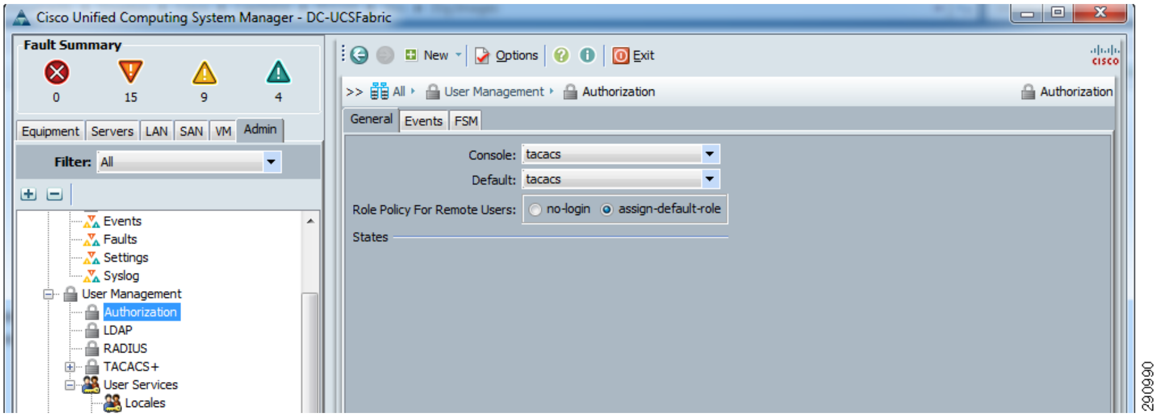
| Hostname | Order | Port |
|---|---|---|
| 192.168.42.131 | 1 | 49 |

Logged in as bmcgloth@ucsmanager.cisco-irn....

System Time: 2011-06-03T15:50

Select **tacacs** from the Console and Default dropdown menus on the Authorization page, as shown in Figure 5-43.

***Figure 5-43 Authorization—Selecting Console and Default Settings***



Cisco Unified Computing System Manager - DC-UCSFabric

>> All ▸ User Management ▸ Authorization

Console: tacacs

Default: tacacs

Role Policy For Remote Users: ○ no-login ● assign-default-role

States

On the TACACS+ server, create custom attributes defining the desired role for the user or group accessing the Cisco UCS Manager (see Figure 5-44):

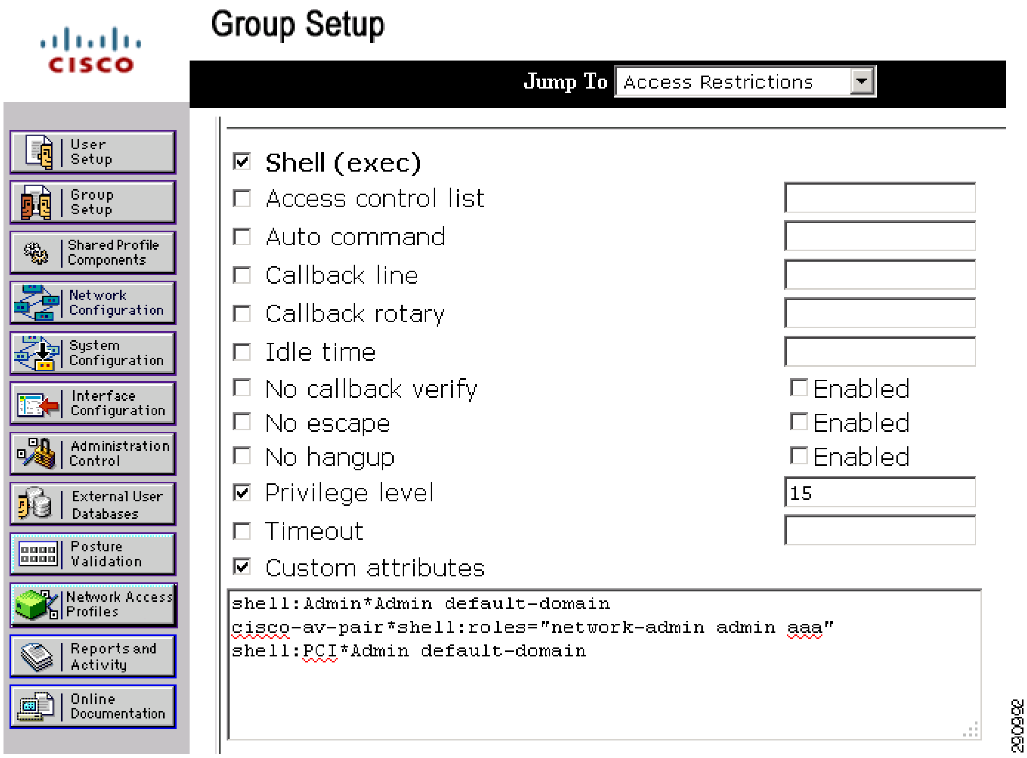
- TACACS+ custom attributes for UCS Manager:

```
cisco-av-pair*shell:roles="admin aaa"
```

- If combined with other systems roles, such as for the Nexus;

```
cisco-av-pair*shell:roles="network-admin admin aaa"
```

**Figure 5-44 Group Configuration Page on TACACS+ Server**



Group Setup

Jump To: Access Restrictions

☑ Shell (exec)
□ Access control list
□ Auto command
□ Callback line
□ Callback rotary
□ Idle time
□ No callback verify □ Enabled
□ No escape □ Enabled
□ No hangup □ Enabled
☑ Privilege level 15
□ Timeout
☑ Custom attributes

```
shell:Admin*Admin default-domain
cisco-av-pair*shell:roles="network-admin admin aaa"
shell:PCI*Admin default-domain
```

### Requirement 8: Assign a Unique ID to Each Person with Computer Access

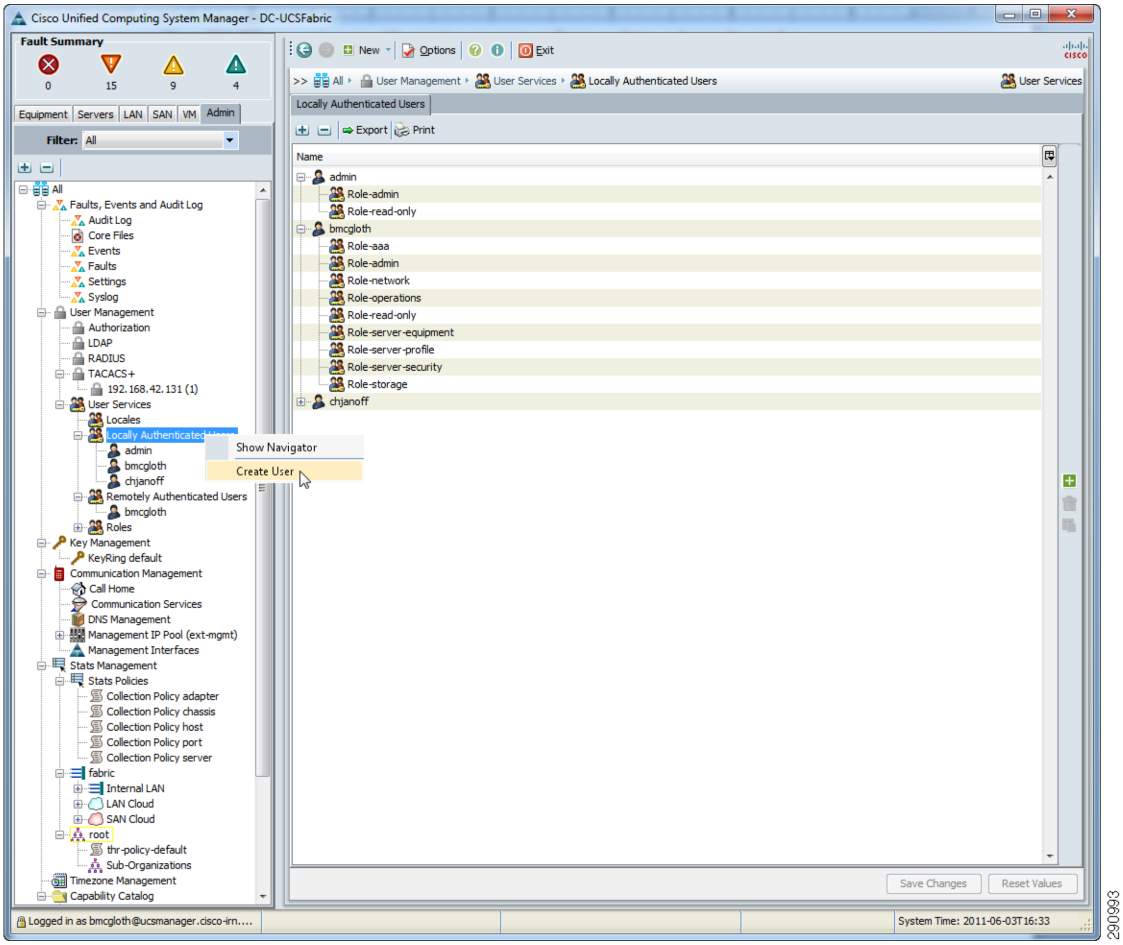
Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown above in Requirement 7.

The Cisco UCS is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco UCS supports the creation of local user accounts with unique IDs through the use of the Create User option when you alt-click on Locally Authenticated Users (see Figure 5-45). These can be used for local fallback user accounts.

*Figure 5-45 Create User*



- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco UCS require setting of a password for admin role accounts.

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  Local passwords are stored encrypted on the Cisco UCS system and are not displayed.

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco UCS servers allow for an administrator to specify an expiration date for the local user accounts passwords, effectively disabling their accounts after a specified period of time.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco UCS does not support an automated capability to perform this function at this time; user passwords management would have to be manually performed every 90 days per a company policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco UCS servers require a minimum of eight characters for local passwords.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters. PCI Sub-Requirements with Compensating Controls*

  Cisco UCS servers require at least three of the following character types for passwords:

  - Lower case letters
  - Upper case letters
  - Digits
  - Special characters

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco UCS does not support an automated capability to perform this function at this time; user account management would have to follow this policy manually if a centralized authentication service with this capability could not be used.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco UCS does not support the ability to lock out local accounts after failed login attempts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco UCS does not support the ability to lock out local accounts after failed login attempts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco UCS does not feature an explicit session timeout. Administration time limits would need to be enabled systemically through an Active Directory policy to the admin workstation desktops, locking them when there is no activity after 15 minutes.

#### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco UCS is able to track and monitor all administrative user access, events such as profile creation, interface up/down, and device authentications.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*

  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco UCS is able to track and monitor all administrative user access and events.

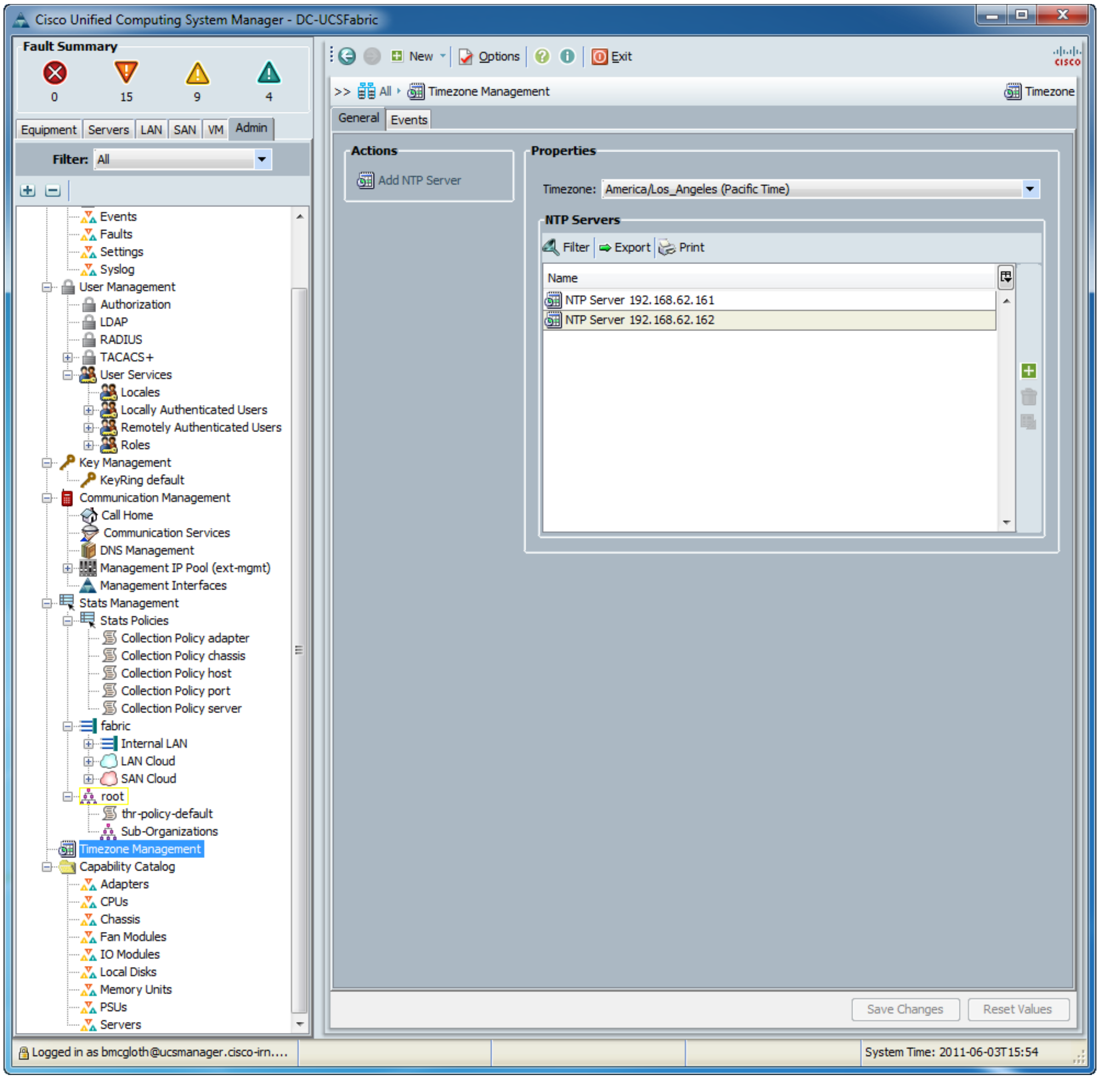
- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco UCS uses NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices (see Figure 5-46). This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

*Figure 5-46 NTP Screen*



Timezone: America/Los_Angeles (Pacific Time)

| Name |
|---|
| NTP Server 192.168.62.161 |
| NTP Server 192.168.62.162 |

Logged in as bmcgloth@ucsmanager.cisco-irn....
System Time: 2011-06-03T15:54

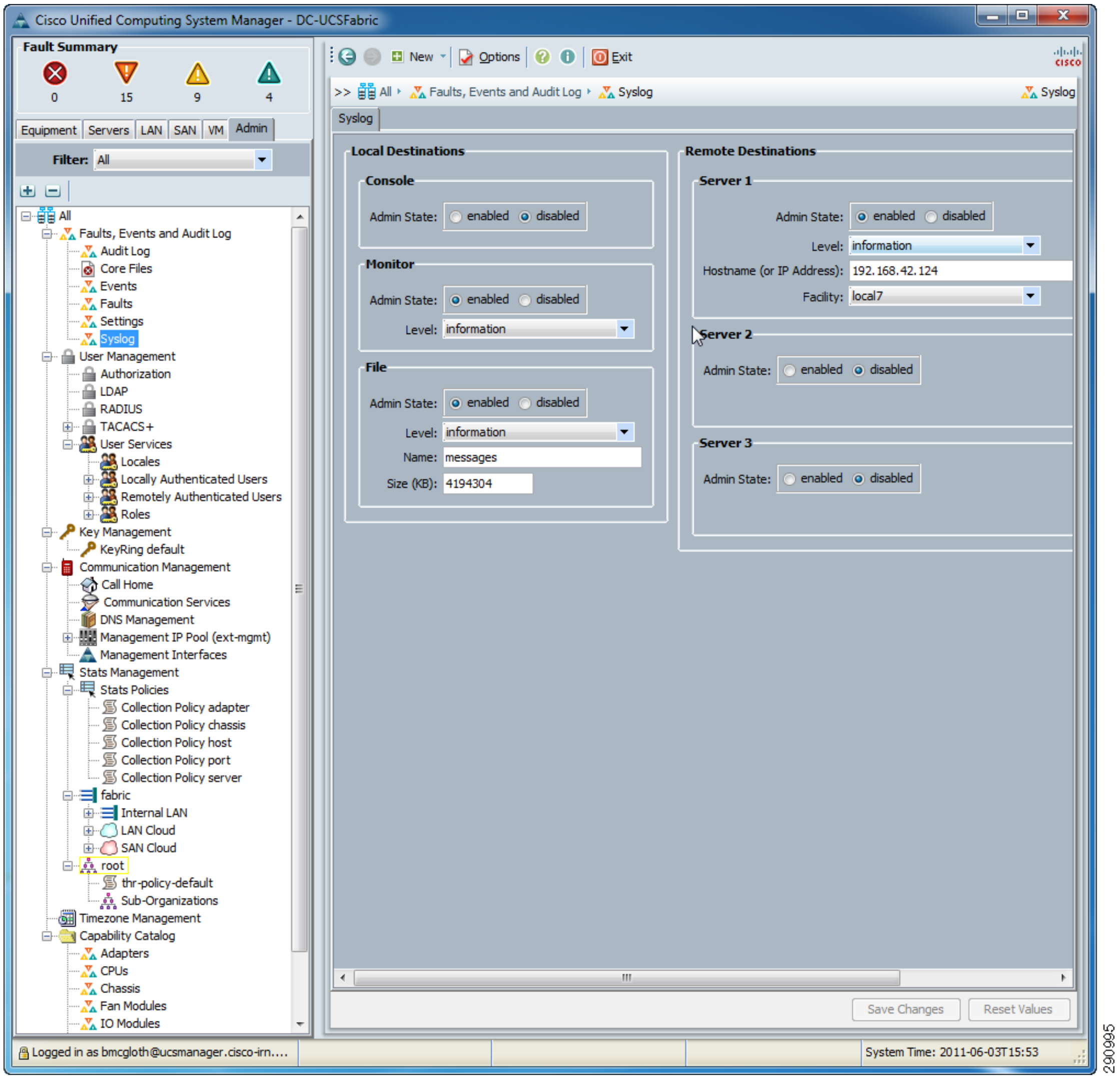
To learn more about NTP, visit:
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Requirement 10.5 was met using RSA enVision, which is a central logging repository that collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

Cisco UCS is capable of sending system events to a centralized repository using the syslog function and/or SNMP traps. In the solution, only syslog was used. (See Figure 5-47.)

*Figure 5-47 Using Syslog*



Local Destinations

Console

Admin State: ○ enabled ● disabled

Monitor

Admin State: ● enabled ○ disabled

Level: information

File

Admin State: ● enabled ○ disabled

Level: information

Name: messages

Size (KB): 4194304

Remote Destinations

Server 1

Admin State: ● enabled ○ disabled

Level: information

Hostname (or IP Address): 192.168.42.124

Facility: local7

Server 2

Admin State: ○ enabled ● disabled

Server 3

Admin State: ○ enabled ● disabled

## PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

## PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

## Cisco UCS Express on Services Ready Engine

The Cisco Unified Computing System Express (UCS Express) and Services Ready Engine (SRE) allows retailers to securely deploy sensitive applications directly within the routing platform. By using UCS Express, retailers can remove legacy compute resources in the store, saving space, energy, and operational costs.

Cisco UCS Express is a converged networking, computing, and virtualization platform for hosting essential business applications in the store location. The SRE modules are router blades for the second generation of Cisco Integrated Services Routers (ISR G2) that provide the capability to host Cisco, third-party, and custom applications. A service-ready deployment model enables store applications to be provisioned remotely on the modules at any time. Cisco SRE modules have their own processors, storage, network interfaces, and memory, which operate independently of the host router resources and help ensure maximum concurrent routing and application performance.

*Table 5-16 PCI Assessment Summary—Cisco UCS Express and Cisco SRE*

| **Models Assessed** | |
|---|---|
| Cisco UCS Express version 1.1 on SRE900 | |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.15 |
| **PCI 10** | 10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| **PCI 8** | 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14 |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

### Primary PCI Function

The main function of Cisco UCS Express is to securely host one primary compliance-related function per physical or virtual server.

It provides segmentation of sensitive applications from out-of-scope applications via physical and virtualization technology. Although technically, a firewall or ACL is used to enforce PCI Requirement 1, UCS extends Layer 3 boundaries to virtual NIC and storage adapters within the chassis. Using VLANs and VSANs, Cisco UCS allows a retailer to separate its payment systems (in-scope) from other non-sensitive data (out-of-scope).

Table 5-16 lists the component assessment details for the Cisco UCS Express and Cisco SRE.

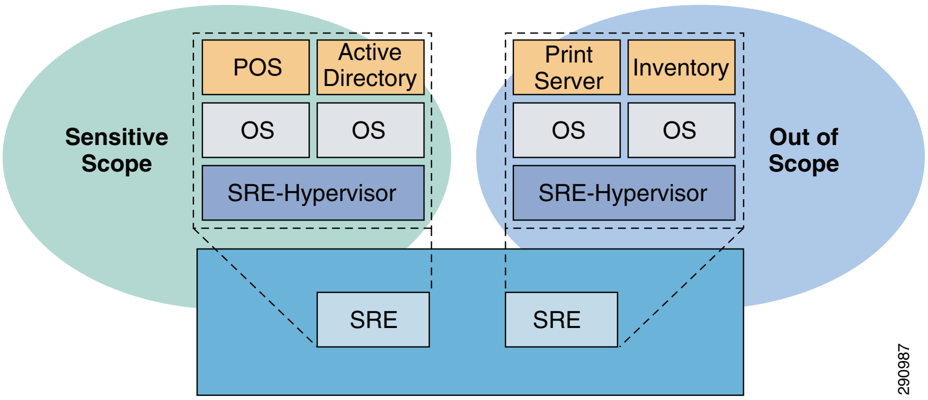
*Table 5-17 Component Capability Assessment—Cisco UCS Express and Cisco SRE*

| Cisco UCS Express and Cisco SRE | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement N/A** |
| Securely host payment applications. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ▼ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

The major consideration when using Cisco UCS Express with sensitive applications is the security of the hypervisor. PCI considers all hypervisors to be insecure. Therefore, use separate Cisco UCS Express implementations when scooping. Although it is acceptable to mix non-sensitive applications onto a Cisco UCS Express deployment with sensitive applications, that brings those applications into scope and audit. (See Figure 5-48.)

*Figure 5-48 Using UCS Express with Cisco SRE*



- The audited version 1.1 of UCS Express has several limitations with local user accounts. There is no capability to use central authentication or management. This resulted in a need for compensating controls that are detailed below.

**Note** Newer versions of UCS Express (version 1.5 +) enable central management of the VMware ESXi on Cisco UCS Express through vCenter (upgrade license required) as well as eliminate the Cisco console VM and local user management/VMware ESXi management restrictions. With the new release, Cisco UCS can manage users on VMware ESXi exactly as it would on a standalone VMware ESXi 4.1 server. This feature was not able to be validated before publishing of this guide, and has not been assessed by Verizon Business or tested in the Cisco PCI solution lab.

**Note** The Cisco UCS Express module comes installed with VMware ESXi. This is the primary function for the server module. Each module can host several independent operating systems as virtual servers. Each virtual server should have only one primary function.

- Cisco UCS Express requires the use of VLANs in the router. Depending on the deployment within the store, this may require the use of bridged virtual interfaces.
- Cisco UCS Express is based on VMware's ESXi and uses vSphere client for management.

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco UCS Express and the underlying VMware ESXi have no unnecessary services enabled by default.
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The Cisco UCS Express appliance does not allow changes to the operating system, installation of unsupported hardware, or of unsupported third-party software.
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco UCS Express uses strong encryption for SSH and HTTPS connections.

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for* *example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco UCS Express. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

Software support for all Cisco products can be located at: http://www.cisco.com/cisco/software/navigator.html.

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using the internal database for administrator users. Individual administrative user IDs are created and assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

Cisco UCS Express includes extensive controls for defining user privileges and by default denies access to all individuals without a system user ID.

### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution through configuration of local accounts in the database.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco UCS Express supports the creation of local user accounts with unique IDs through the use of the VMware vSphere client editing the local users and groups database.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco UCS Express require setting of a password.

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  All passwords are stored using strong encryption.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Administrative time limits would need to be enabled systemically through an active directory policy to the admin workstation desktops, locking them when there is no activity.

#### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco UCS Express is able to track and monitor all administrative user access, events such as profile creation, interface up/down, and device authentications.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

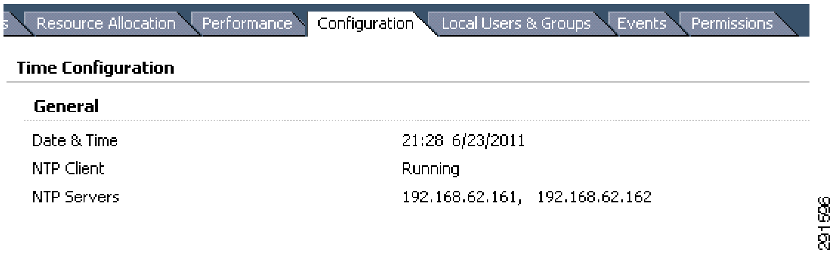
Cisco UCS Express uses the local clock facilities to meet the following requirements:

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*

  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers, as shown in Figure 5-49.

***Figure 5-49 UCS Express NTP Servers***



Time Configuration

General

| | |
|---|---|
| Date & Time | 21:28 6/23/2011 |
| NTP Client | Running |
| NTP Servers | 192.168.62.161, 192.168.62.162 |

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

## PCI Assessment Detail—PCI Sub-Requirements with Compensating Controls

### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved using policies implemented through manual administration.

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

**Note** Newer versions of UCS Express (version 1.5 +) enable central management of the VMware ESXi on UCS Express through vCenter (upgrade license required) as well as eliminate the Cisco console VM and local user management/VMware ESXi management restrictions. With the new release, Cisco UCS can manage users on VMware ESXi exactly as it would on a standalone VMware ESXi 4.1 server. This feature was not able to be validated before publishing of this guide, and has not been assessed by Verizon Business or tested in the Cisco PCI solution lab.

#### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

# Scope Administration

## Authentication

### Cisco Secure Access Control Server

Cisco Secure Access Control Server (ACS) was used as a central authentication system for the majority of products validated in this solution. It links user authentication to Windows Active Directory using group mapping that segments users based on their role and function.

Cisco Secure ACS is an access policy control platform that helps you comply with growing regulatory and corporate requirements. By using a single authentication method for all system devices, insight into who made changes is simplified for internal administration, assessors, and post-breach audits. It supports multiple scenarios simultaneously, including the following:

- Device administration—Authenticates administrators, authorizes commands, and provides an audit trail
- Remote access—Works with VPN and other remote network access devices to enforce access policies
- Wireless—Authenticates and authorizes wireless users and hosts and enforces wireless-specific policies
- Network admission control—Communicates with posture and audit servers to enforce admission control policies

Cisco Secure ACS lets you centrally manage access to network resources for a growing variety of access types, devices, and user groups. These key features address the current complexities of network access control:

- Support for a range of protocols including Extensible Authentication Protocol (EAP) and non-EAP protocols provides the flexibility to meet all your authentication requirements

- Integration with Cisco products for device administration access control allows for centralized control and auditing of administrative actions
- Support for external databases, posture brokers, and audit servers centralizes access policy control and lets you integrate identity and access control systems

*Table 5-18 PCI Assessment Summary—Cisco Secure Access Control Server*

| **Models Assessed** | |
|---|---|
| Cisco Secure Access Control Server | Release 4.2(1) Build 15 Patch 3 |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

## Primary PCI Function

The main function of Cisco Secure ACS is to securely authenticate users toi the systems within the cardholder environment.

Table 5-18 lists the component assessment details for Cisco Secure ACS.

*Table 5-19 Component Capability Assessment—Cisco Secure ACS*

| Cisco Secure ACS | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 7, 8 (7.1, 7.2, 8.2)** |
| Securely authenticate users to systems in the cardholder environment. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***“Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

- Cisco Secure ACS has been configured to authenticate individual users using Active Directory (AD). This is accomplished by creating user groups in AD and mapping them to role-based groups in Cisco Secure ACS. This provides the granularity of secure authentication needed to address the PCI specification.
- The solution used the windows versions of Cisco Secure ACS. The CSA client was installed to protect and alert on unauthorized access of the log and audit trail.
- Remove the default accounts for administration.
- Enable HTTPS and disable HTTP.
- User authentication services for Cisco Secure ACS are linked to a centralized Active Directory user database

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*

If Cisco Secure ACS is deployed on a server, it should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

If Cisco Secure ACS is deployed as an appliance, no unnecessary services are enabled by default.

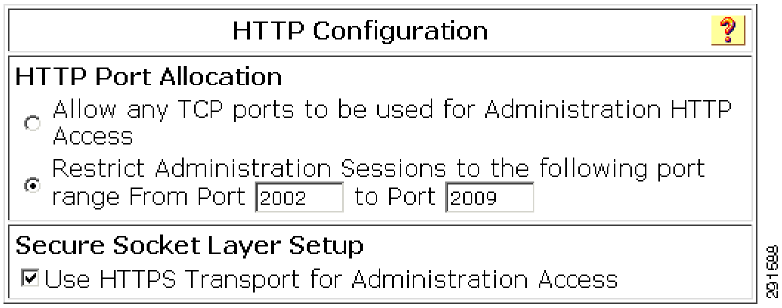
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco Secure ACS should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

  If Cisco Secure ACS is deployed as an appliance, no unnecessary services are enabled by default.
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  The management console was configured to support HTTPS access, with HTTP access disabled. Cisco Secure ACS is configured to use SSL as a highly secure management portal technology (see Figure 5-50). Cisco Secure ACS employs port hopping to a random high port for secured communication transport.

*Figure 5-50 HTTP Configuration*



HTTP Configuration

HTTP Port Allocation

○ Allow any TCP ports to be used for Administration HTTP Access

● Restrict Administration Sessions to the following port range From Port 2002 to Port 2009

Secure Socket Layer Setup

☑ Use HTTPS Transport for Administration Access

**Note** Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant/service provider.

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Secure ACS. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

Software support for all Cisco products can be located at:
http://www.cisco.com/cisco/software/navigator.html

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using the Cisco Secure ACS internal database for administrator users. Within Cisco Secure ACS, individual administrative user IDs were created and assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco Secure ACS includes extensive controls for defining user privileges and by default denies access to all individuals without a system User ID.

### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution through configuration of local accounts in the database as shown below.

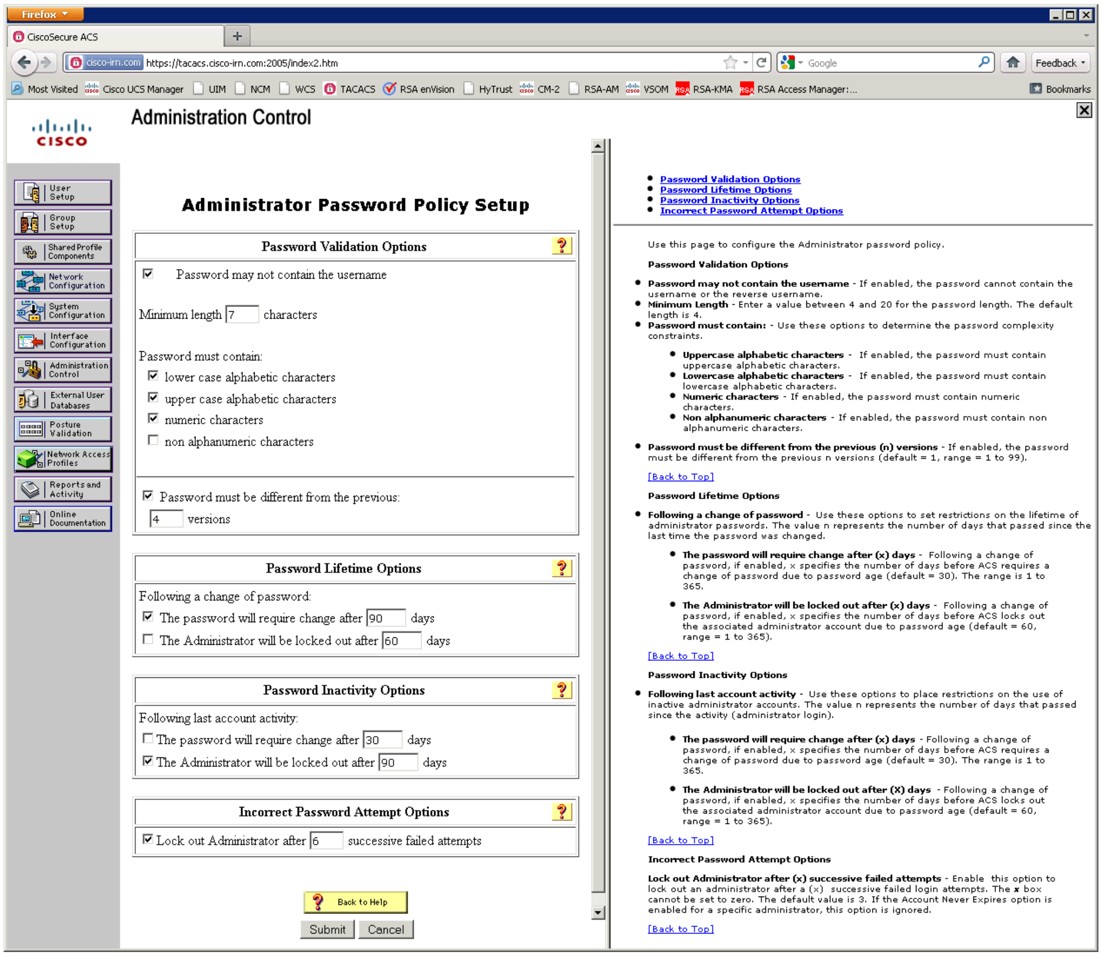
- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco Secure ACS supports the creation of local users. Through company policy, each user must be assigned a unique ID.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local administrator user accounts in Cisco Secure ACS require setting of a password according to the password requirements, as shown in Figure 5-51.

*Figure 5-51 Administrator Password Requirements*



https://tacacs.cisco-irn.com:2005/index2.htm

**Administrator Password Policy Setup**

**Password Validation Options**

☑ Password may not contain the username

Minimum length 7 characters

Password must contain:

☑ lower case alphabetic characters

☑ upper case alphabetic characters

☑ numeric characters

☐ non alphanumeric characters

☑ Password must be different from the previous: 4 versions

**Password Lifetime Options**

Following a change of password:

☑ The password will require change after 90 days

☐ The Administrator will be locked out after 60 days

**Password Inactivity Options**

Following last account activity:

☐ The password will require change after 30 days

☑ The Administrator will be locked out after 90 days

**Incorrect Password Attempt Options**

☑ Lock out Administrator after 6 successive failed attempts

- Password Validation Options
- Password Lifetime Options
- Password Inactivity Options
- Incorrect Password Attempt Options

Use this page to configure the Administrator password policy.

**Password Validation Options**

- **Password may not contain the username** - If enabled, the password cannot contain the username or the reverse username.
- **Minimum Length** - Enter a value between 4 and 20 for the password length. The default length is 4.
- **Password must contain:** - Use these options to determine the password complexity constraints.
  - **Uppercase alphabetic characters** - If enabled, the password must contain uppercase alphabetic characters.
  - **Lowercase alphabetic characters** - If enabled, the password must contain lowercase alphabetic characters.
  - **Numeric characters** - If enabled, the password must contain numeric characters.
  - **Non alphanumeric characters** - If enabled, the password must contain non alphanumeric characters.
- **Password must be different from the previous (n) versions** - If enabled, the password must be different from the previous n versions (default = 1, range = 1 to 99).

[Back to Top]

**Password Lifetime Options**

- **Following a change of password** - Use these options to set restrictions on the lifetime of administrator passwords. The value n represents the number of days that passed since the last time the password was changed.
  - **The password will require change after (x) days** - Following a change of password, if enabled, x specifies the number of days before ACS requires a change of password due to password age (default = 30). The range is 1 to 365.
  - **The Administrator will be locked out after (x) days** - Following a change of password, if enabled, x specifies the number of days before ACS locks out the associated administrator account due to password age (default = 60, range = 1 to 365).

[Back to Top]

**Password Inactivity Options**

- **Following last account activity** - Use these options to place restrictions on the use of inactive administrator accounts. The value n represents the number of days that passed since the activity (administrator login).
  - **The password will require change after (x) days** - Following a change of password, if enabled, x specifies the number of days before ACS requires a change of password due to password age (default = 30). The range is 1 to 365.
  - **The Administrator will be locked out after (X) days** - Following a change of password, if enabled, x specifies the number of days before ACS locks out the associated administrator account due to password age (default = 60, range = 1 to 365).

[Back to Top]

**Incorrect Password Attempt Options**

**Lock out Administrator after (x) successive failed attempts** - Enable this option to lock out an administrator after a (x) successive failed login attempts. The **x** box cannot be set to zero. The default value is 3. If the Account Never Expires option is enabled for a specific administrator, this option is ignored.

[Back to Top]

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  Passwords are not readable within Cisco Secure ACS; it uses strong cryptography.

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Through company policy inactive users should be removed or disabled every 90 days. As shown in Figure 5-51, Cisco Secure ACS password policy also enables setting of an inactivity option where an administrator will be locked out after 90 days of inactivity.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  The password lifetime option must be enabled configured to require users to change their password every 90 days. This setting can be configured as shown in Figure 5-51.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  The default password policy for length specifies a minimum password length of 4 characters; this must be changed to 7 characters, as shown in Figure 5-51.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  The password policy must be updated to require both alphabetic and numeric characters, as shown in Figure 5-51.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  The password history option must be enabled and configured and set to 4 versions, as shown in Figure 5-51.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  The Incorrect Password Attempt Options must be enabled and the default of 3 attempts must be changed to 6 successive failed authentications attempts, as shown in Figure 5-51.

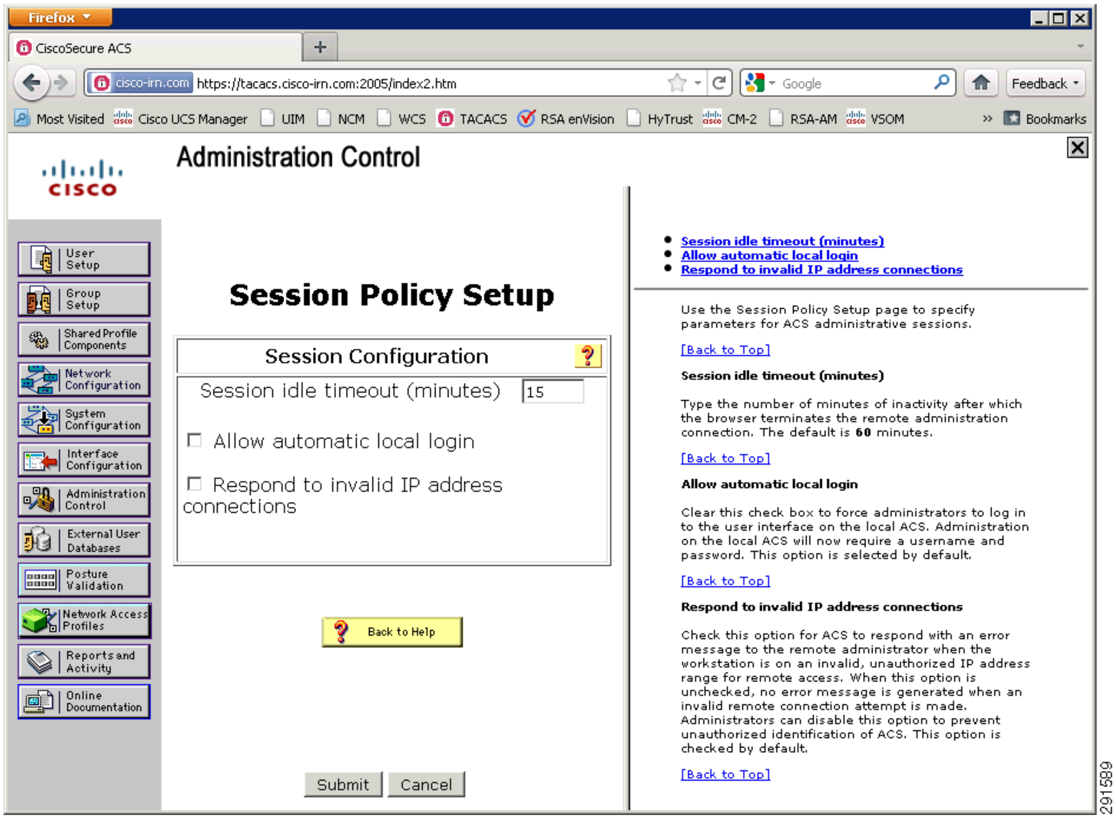
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  By default, Cisco Secure ACS requires another administrator to re-enable locked out accounts.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco Secure ACS supports session policies under the Administration Control/Session tab. Change the Session Time-out to 15 minutes from the default 60 minutes, as shown in Figure 5-52.

***Figure 5-52 Session Timeout***



Administration Control

**Session Policy Setup**

Session Configuration

Session idle timeout (minutes) 15

□ Allow automatic local login

□ Respond to invalid IP address connections

- Session idle timeout (minutes)
- Allow automatic local login
- Respond to invalid IP address connections

Use the Session Policy Setup page to specify parameters for ACS administrative sessions.

[Back to Top]

**Session idle timeout (minutes)**

Type the number of minutes of inactivity after which the browser terminates the remote administration connection. The default is **60** minutes.

[Back to Top]

**Allow automatic local login**

Clear this check box to force administrators to log in to the user interface on the local ACS. Administration on the local ACS will now require a username and password. This option is selected by default.

[Back to Top]

**Respond to invalid IP address connections**

Check this option for ACS to respond with an error message to the remote administrator when the workstation is on an invalid, unauthorized IP address range for remote access. When this option is unchecked, no error message is generated when an invalid remote connection attempt is made. Administrators can disable this option to prevent unauthorized identification of ACS. This option is checked by default.

[Back to Top]

### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco Secure ACS is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*

- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco Secure ACS uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.4**—*Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  Time synchronization for Windows servers is specified through the domain policy. Servers synchronize their clocks with the domain controller, which in turn is synchronized using NTP. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

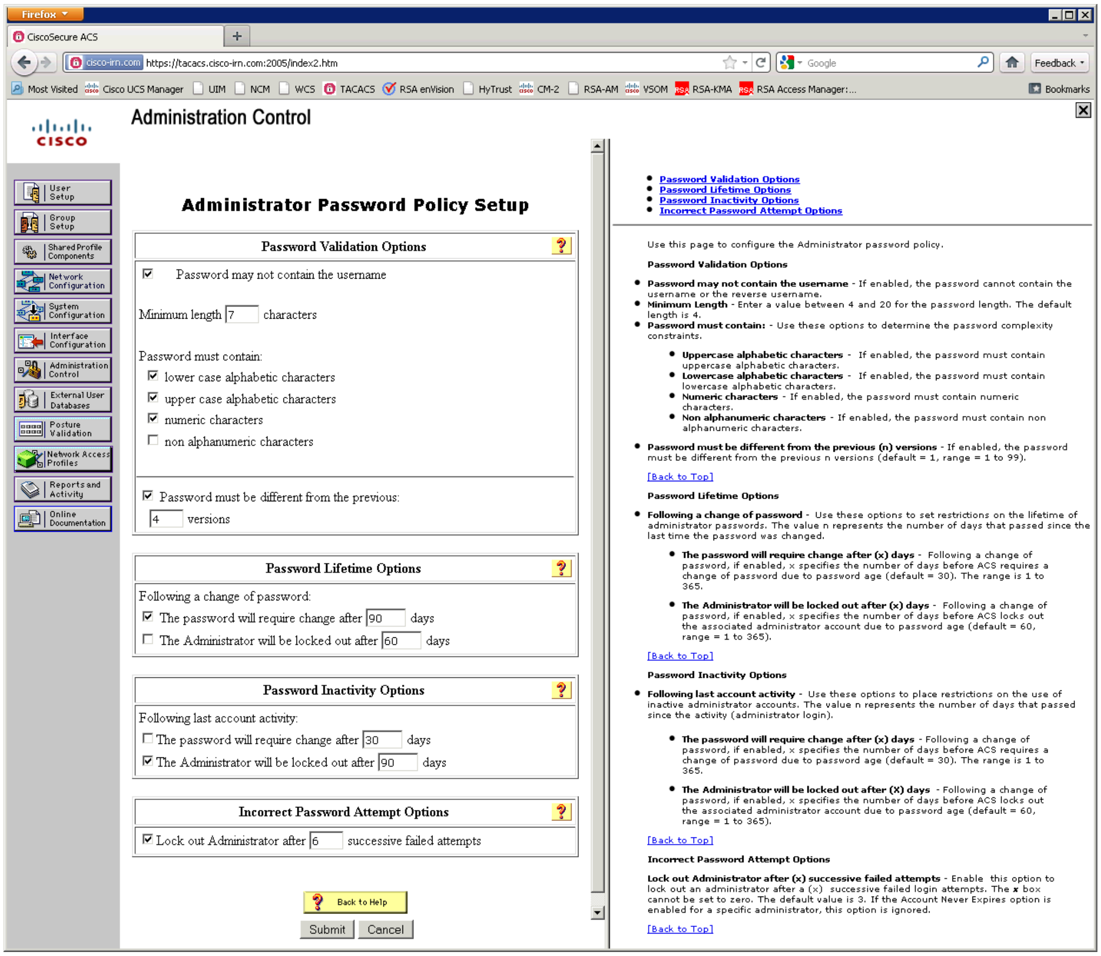
Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

Cisco Secure ACS can be configured to send its log data to the RSA enVision log management platform to meet the above requirements. The configuration procedure is documented in the RSA enVision Event Source Configuration Guide for Cisco Secure ACS, which can be found at RSA Secure Care Online (https://knowledge.rsasecurity.com/).

RSA enVision requires that specific attributes for each reporting function to be specified and configured in a particular order. Figure 5-53 shows the required items for generating Syslog Passed Authentications. Settings for other event types are available in the RSA enVision Event Source Configuration Guide for Cisco Secure ACS.

*Figure 5-53 Syslog for Passed Authentications*



Administration Control

**Administrator Password Policy Setup**

**Password Validation Options**

☑ Password may not contain the username

Minimum length 7 characters

Password must contain:

☑ lower case alphabetic characters
☑ upper case alphabetic characters
☑ numeric characters
☐ non alphanumeric characters

☑ Password must be different from the previous:
4 versions

**Password Lifetime Options**

Following a change of password:
☑ The password will require change after 90 days
☐ The Administrator will be locked out after 60 days

**Password Inactivity Options**

Following last account activity:
☐ The password will require change after 30 days
☑ The Administrator will be locked out after 90 days

**Incorrect Password Attempt Options**

☑ Lock out Administrator after 6 successive failed attempts

- Password Validation Options
- Password Lifetime Options
- Password Inactivity Options
- Incorrect Password Attempt Options

Use this page to configure the Administrator password policy.

**Password Validation Options**

- **Password may not contain the username** - If enabled, the password cannot contain the username or the reverse username.
- **Minimum Length** - Enter a value between 4 and 20 for the password length. The default length is 4.
- **Password must contain:** - Use these options to determine the password complexity constraints.
  - **Uppercase alphabetic characters** - If enabled, the password must contain uppercase alphabetic characters.
  - **Lowercase alphabetic characters** - If enabled, the password must contain lowercase alphabetic characters.
  - **Numeric characters** - If enabled, the password must contain numeric characters.
  - **Non alphanumeric characters** - If enabled, the password must contain non alphanumeric characters.
- **Password must be different from the previous (n) versions** - If enabled, the password must be different from the previous n versions (default = 1, range = 1 to 99).

[Back to Top]

**Password Lifetime Options**

- **Following a change of password** - Use these options to set restrictions on the lifetime of administrator passwords. The value n represents the number of days that passed since the last time the password was changed.
  - **The password will require change after (x) days** - Following a change of password, if enabled, x specifies the number of days before ACS requires a change of password due to password age (default = 30). The range is 1 to 365.
  - **The Administrator will be locked out after (x) days** - Following a change of password, if enabled, x specifies the number of days before ACS locks out the associated administrator account due to password age (default = 60, range = 1 to 365).

[Back to Top]

**Password Inactivity Options**

- **Following last account activity** - Use these options to place restrictions on the use of inactive administrator accounts. The value n represents the number of days that passed since the activity (administrator login).
  - **The password will require change after (x) days** - Following a change of password, if enabled, x specifies the number of days before ACS requires a change of password due to password age (default = 30). The range is 1 to 365.
  - **The Administrator will be locked out after (X) days** - Following a change of password, if enabled, x specifies the number of days before ACS locks out the associated administrator account due to password age (default = 60, range = 1 to 365).

[Back to Top]

**Incorrect Password Attempt Options**

**Lock out Administrator after (x) successive failed attempts** - Enable this option to lock out an administrator after a (x) successive failed login attempts. The ***x*** box cannot be set to zero. The default value is 3. If the Account Never Expires option is enabled for a specific administrator, this option is ignored.

[Back to Top]

## PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

## PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

## RSA Authentication Manager

RSA Authentication Manager is the management component of the RSA SecurID®, a two-factor authentication solution, which provides a much more reliable level of user authentication than reusable passwords. SecurID authentication is based on something you know (a password or PIN) and something you have (an authenticator), and can be used to achieve compliance to PCI requirement 8.3, which requires two-factor authentication for remote access to the network by employees, administrators, and third parties. As the management component, RSA Authentication Manager is used to verify authentication requests and centrally administer authentication policies for enterprise networks.

*Table 5-20 PCI Assessment Summary—RSA Authentication Manager*

| **Models Assessed** | |
|---|---|
| RSA Authentication Manager 7.1 Service Pack 2 | |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.3, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

### Primary PCI Function

The main function of RSA Authentication Manager is to securely authenticate remote users using two-factor authentication.

Table 5-20 lists the component assessment details for RSA Authentication Manager.

*Table 5-21 Component Capability Assessment—RSA Authentication Manager*

| RSA Authentication Manager | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 8 (8.3)** |
| Securely authenticate remote users using two-factor authentication. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

RSA Authentication Manager stores and processes highly sensitive authentication information and should be deployed and operated in a secure manner. Detailed recommendations are found in the RSA Authentication Manager Security Best Practices Guide, which can be downloaded from RSA Secure Care Online (https://knowledge.rsasecurity.com/).

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  There are no unnecessary services enabled by default on RSA Authentication Manager. RSA Authentication Manager should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  RSA Authentication Manager should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  RSA Authentication Manager web consoles are protected with SSL.

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  RSA Authentication Manager publishes security patches on RSA Secure Care Online (https://knowledge.rsasecurity.com/) in accordance with industry best practices to manage and respond to security vulnerabilities to minimize customers' risk of exposure.

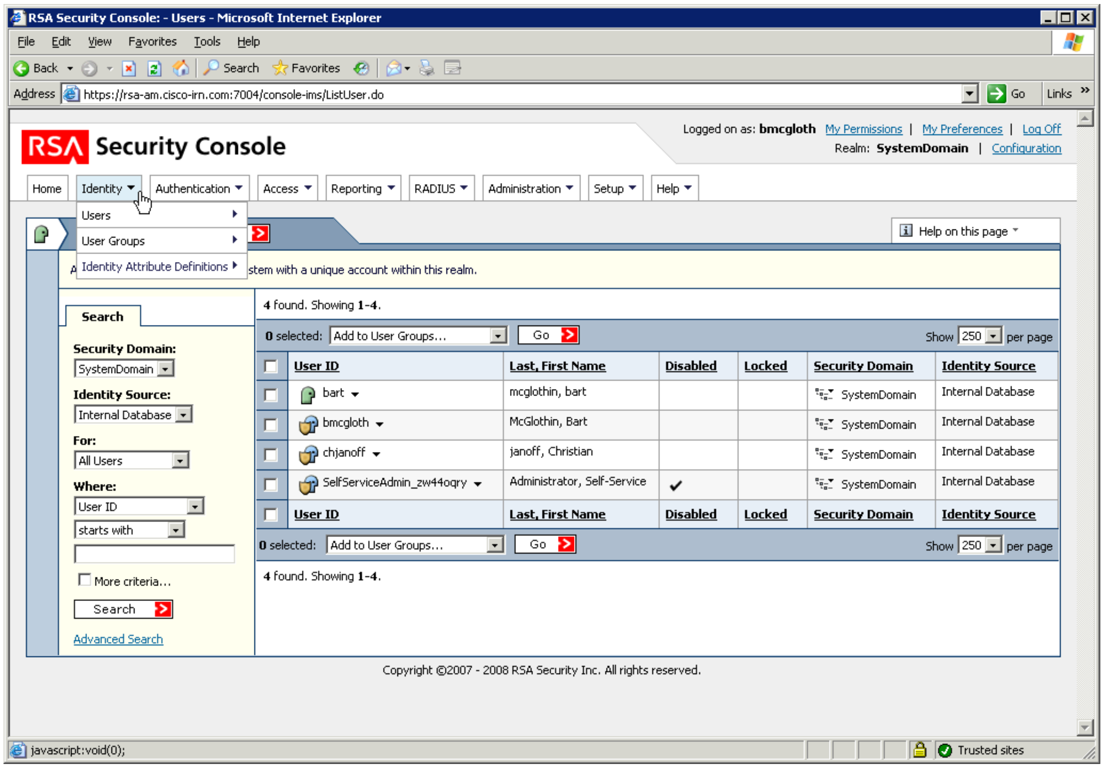
### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using the RSA Authentication Manager's internal database. RSA Authentication Manager also supports linking to a centralized user database such as Active Directory using LDAP. Within RSA Authentication Manager, individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

RSA Authentication Manager has powerful access control capabilities to limit access to system components and cardholder data based on user role or group membership. Users and groups are created under the Identity tab of the Security console, as shown in Figure 5-54.

*Figure 5-54 Users and Groups*


RSA Security Console: - Users - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go Links
RSA Security Console
Home Identity Authentication Access Reporting RADIUS Administration Setup Help
Users
User Groups
Identity Attribute Definitions
Help on this page
javascript:void(0);
Trusted sites

Address: https://rsa-am.cisco-irn.com:7004/console-ims/ListUser.do

Logged on as: **bmcgloth** My Permissions | My Preferences | Log Off
Realm: **SystemDomain** | Configuration

stem with a unique account within this realm.

**Search**

**Security Domain:** SystemDomain
**Identity Source:** Internal Database
**For:** All Users
**Where:** User ID, starts with

□ More criteria...

Search

Advanced Search

4 found. Showing **1-4**.

**0** selected: Add to User Groups... Go Show 250 per page

| □ | User ID | Last, First Name | Disabled | Locked | Security Domain | Identity Source |
|---|---|---|---|---|---|---|
| □ | bart | mcglothin, bart | | | SystemDomain | Internal Database |
| □ | bmcgloth | McGlothin, Bart | | | SystemDomain | Internal Database |
| □ | chjanoff | janoff, Christian | | | SystemDomain | Internal Database |
| □ | SelfServiceAdmin_zw44oqry | Administrator, Self-Service | ✓ | | SystemDomain | Internal Database |
| □ | User ID | Last, First Name | Disabled | Locked | Security Domain | Identity Source |

**0** selected: Add to User Groups... Go Show 250 per page

4 found. Showing **1-4**.

Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.

291567

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

RSA Authentication Manager's access control system defaults to deny access.

### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution through configuration of local accounts in the database as shown below.

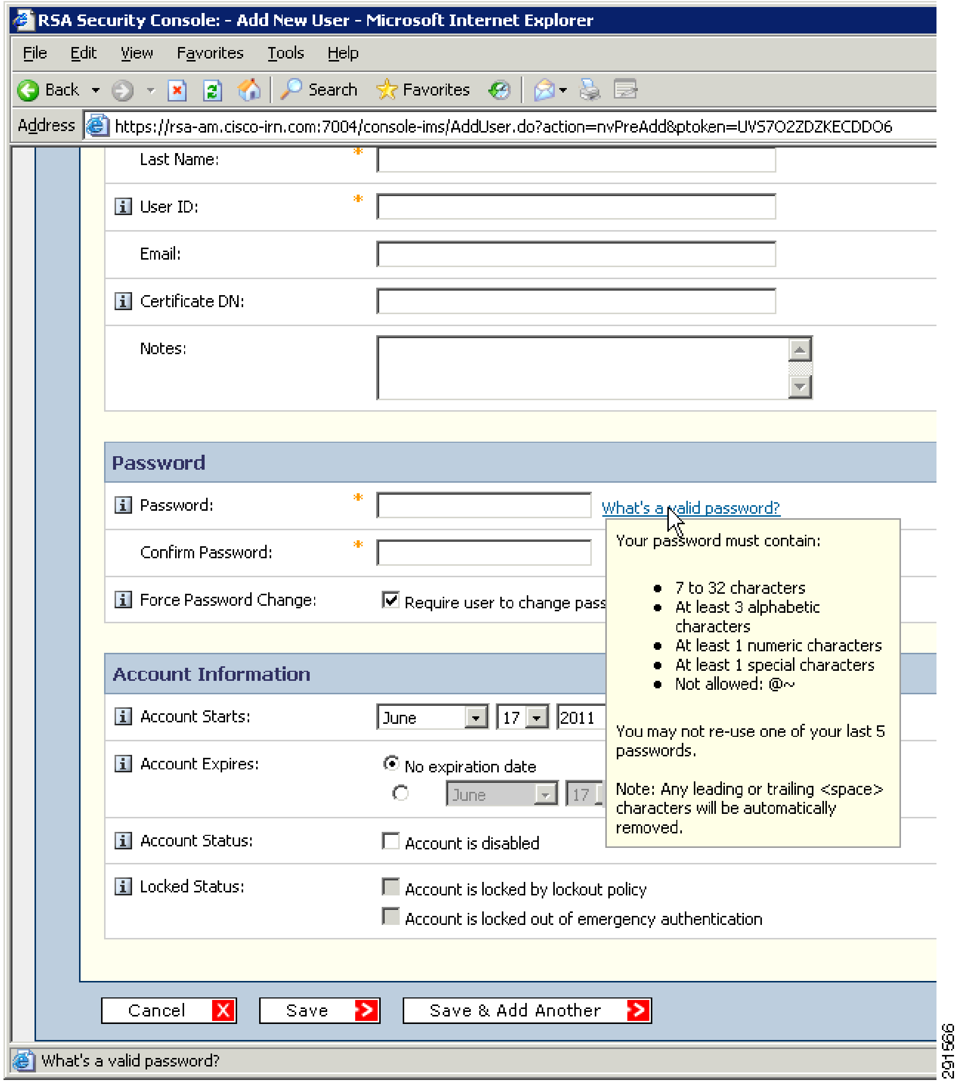
- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  RSA Authentication Manager supports the creation of local users or linking to a central repository of users. Through company policy, each user must be assigned a unique ID.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts in RSA Authentication Manager require setting of a password according to the assigned password policy as shown in Figure 5-55.

*Figure 5-55 User Password Requirements Based on Policy*


RSA Security Console: - Add New User - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Cancel
Save
Save & Add Another
291566

Address: https://rsa-am.cisco-irn.com:7004/console-ims/AddUser.do?action=nvPreAdd&ptoken=UVS7O2ZDZKECDDO6

Last Name: *

User ID: *

Email:

Certificate DN:

Notes:

**Password**

Password: * What's a valid password?

Confirm Password: *

Force Password Change: ☑ Require user to change pass

Your password must contain:

- 7 to 32 characters
- At least 3 alphabetic characters
- At least 1 numeric characters
- At least 1 special characters
- Not allowed: @~

You may not re-use one of your last 5 passwords.

Note: Any leading or trailing <space> characters will be automatically removed.

**Account Information**

Account Starts: June 17 2011

Account Expires: ● No expiration date
○ June 17

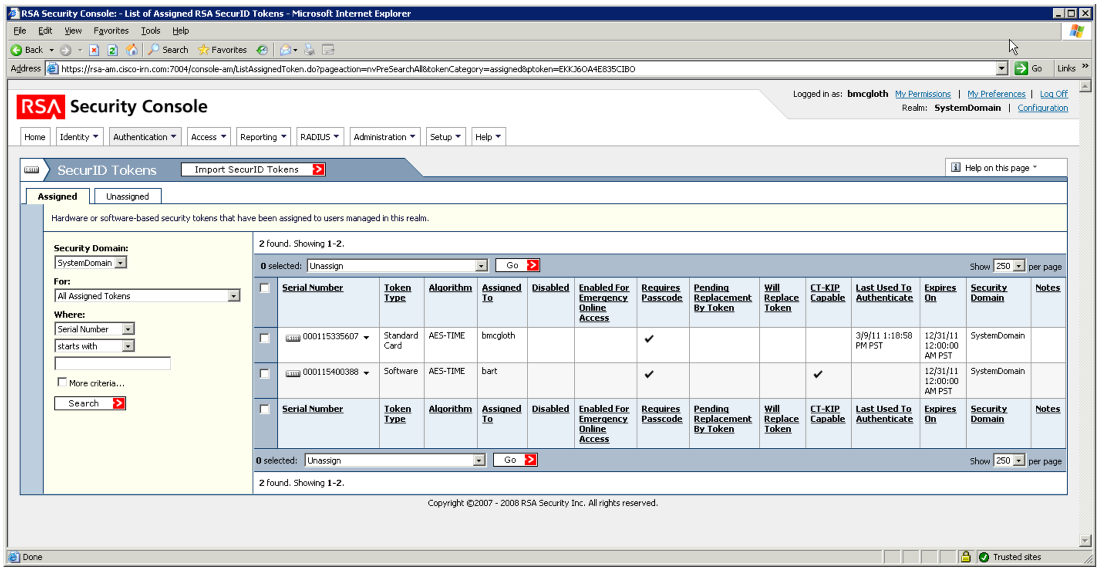
Account Status: □ Account is disabled

Locked Status: □ Account is locked by lockout policy
□ Account is locked out of emergency authentication

What's a valid password?

Additional authentication tokens can also be assigned to each user, as shown in Figure 5-56.

*Figure 5-56 Assigned Tokens*


RSA Security Console: - List of Assigned RSA SecurID Tokens - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go Links
RSA Security Console
My Permissions | My Preferences | Log Off
Configuration
Home Identity Authentication Access Reporting RADIUS Administration Setup Help
SecurID Tokens
Import SecurID Tokens
Help on this page
Assigned Unassigned
More criteria...
Search
Go
Done
Trusted sites

Address: https://rsa-am.cisco-irn.com:7004/console-am/ListAssignedToken.do?pageaction=nvPreSearchAll&tokenCategory=assigned&ptoken=EKKJ6OA4E835CIBO

Logged in as: bmcgloth
Realm: SystemDomain

Hardware or software-based security tokens that have been assigned to users managed in this realm.

Security Domain: SystemDomain

For: All Assigned Tokens

Where: Serial Number
starts with

2 found. Showing **1-2**.

**0** selected: Unassign

Show 250 per page

| □ | Serial Number | Token Type | Algorithm | Assigned To | Disabled | Enabled For Emergency Online Access | Requires Passcode | Pending Replacement By Token | Will Replace Token | CT-KIP Capable | Last Used To Authenticate | Expires On | Security Domain | Notes |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | 000115335607 | Standard Card | AES-TIME | bmcgloth | | | ✓ | | | | 3/9/11 1:18:58 PM PST | 12/31/11 12:00:00 AM PST | SystemDomain | |
| □ | 000115400388 | Software | AES-TIME | bart | | | ✓ | | | ✓ | | 12/31/11 12:00:00 AM PST | SystemDomain | |
| □ | Serial Number | Token Type | Algorithm | Assigned To | Disabled | Enabled For Emergency Online Access | Requires Passcode | Pending Replacement By Token | Will Replace Token | CT-KIP Capable | Last Used To Authenticate | Expires On | Security Domain | Notes |

**0** selected: Unassign

Show 250 per page

2 found. Showing **1-2**.

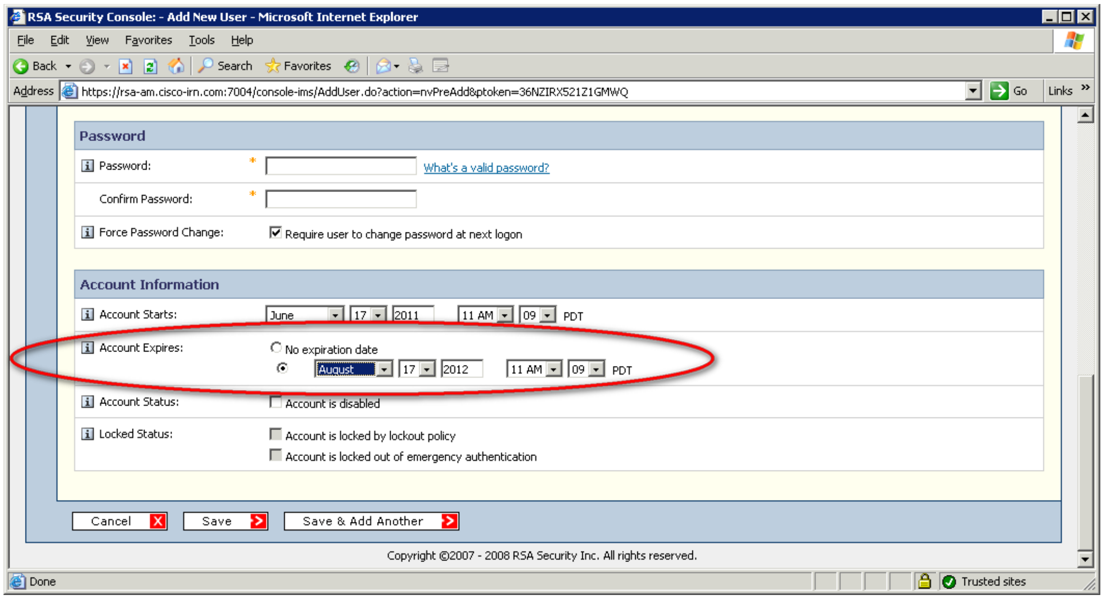
Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.

291563

- **PCI 8.3**—*Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) Note: Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

Through company policy, inactive users should be removed or disabled every 90 days. RSA Authentication Manager also enables setting of an account expiration date for individual accounts, as shown in Figure 5-57.

*Figure 5-57 User Account Expiration*


RSA Security Console: - Add New User - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://rsa-am.cisco-irn.com:7004/console-ims/AddUser.do?action=nvPreAdd&ptoken=36NZIRX521Z1GMWQ
Go Links
Done
Trusted sites
291565

**Password**

Password: * What's a valid password?

Confirm Password: *

Force Password Change: ☑ Require user to change password at next logon

**Account Information**

Account Starts: June 17 2011 11 AM 09 PDT

Account Expires: ○ No expiration date
● August 17 2012 11 AM 09 PDT

Account Status: □ Account is disabled

Locked Status: □ Account is locked by lockout policy
□ Account is locked out of emergency authentication

Cancel Save Save & Add Another

Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.

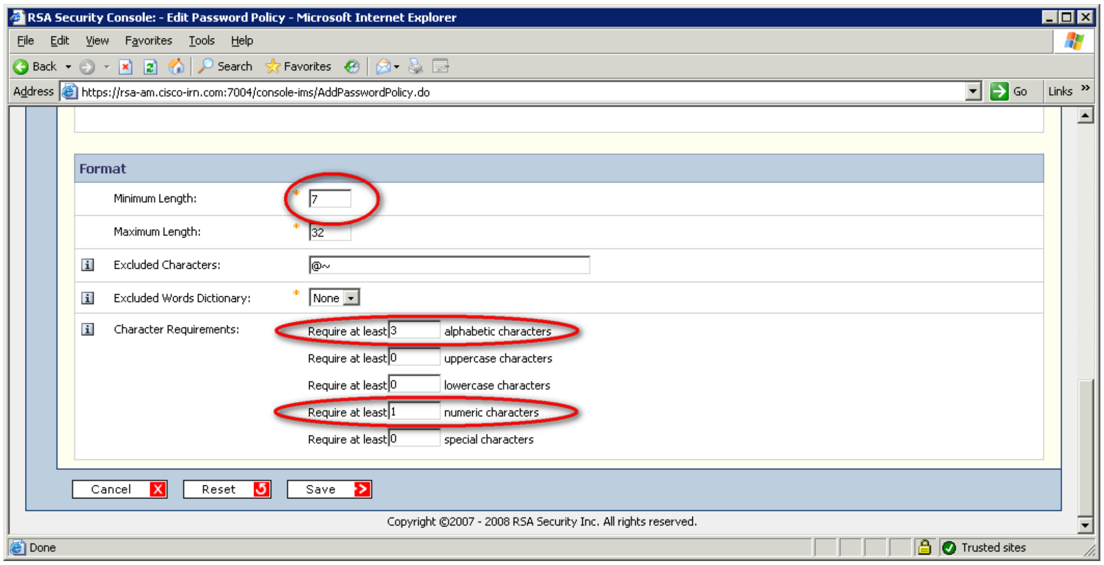
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  The default Initial Password Policy is created when a new realm is established, and requires users to change their passwords every 90 days.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  The default Initial Password Policy must be updated to set a minimum password length of 7 characters, as shown in Figure 5-58.

*Figure 5-58 Initial Password Policy*


RSA Security Console: - Edit Password Policy - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://rsa-am.cisco-irn.com:7004/console-ims/AddPasswordPolicy.do
Go Links
Done
Trusted sites
291560

**Format**

Minimum Length: * 7

Maximum Length: * 32

Excluded Characters: @~

Excluded Words Dictionary: * None

Character Requirements: Require at least 3 alphabetic characters
Require at least 0 uppercase characters
Require at least 0 lowercase characters
Require at least 1 numeric characters
Require at least 0 special characters

Cancel Reset Save

Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  The default Initial Password Policy must be updated to require both alphabetic and numeric characters, as shown in Figure 5-58.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  The default Initial Password Policy is created when a new realm is established, and restricts users from re-using their last five passwords.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

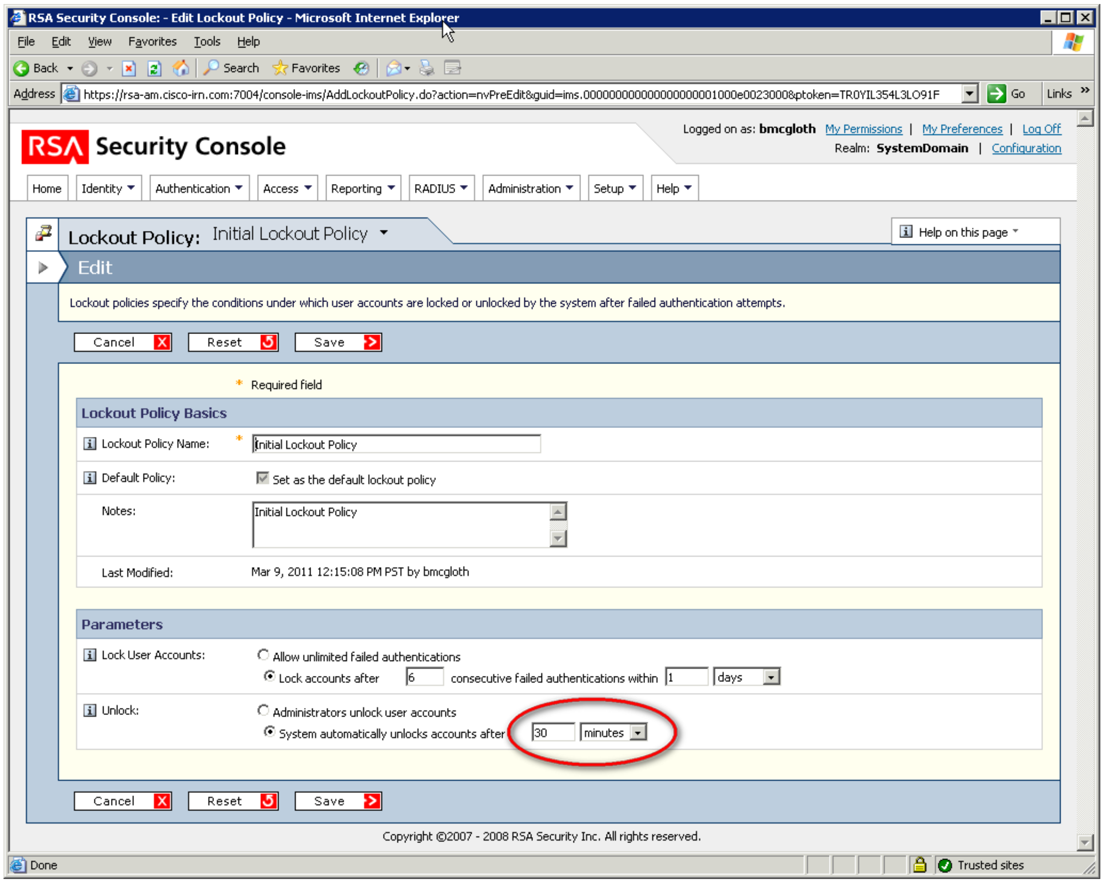
  The Initial Lockout policy is enabled by default and locks accounts after six consecutive failed authentications within one day.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  The Initial Lockout policy is enabled by default; the only change for PCI compliance is to change the auto-unlock parameter from 15 minutes to 30 minutes. This change is made under the Authentication > Policies > Lockout Policies.

  Figure 5-59 shows an appropriate policy for PCI compliance.

***Figure 5-59 Revised Initial Lockout Policy Edited for PCI***



RSA Security Console: - Edit Lockout Policy - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go Links
RSA Security Console
Logged on as: bmcgloth My Permissions | My Preferences | Log Off
Realm: SystemDomain | Configuration
Home Identity Authentication Access Reporting RADIUS Administration Setup Help
Help on this page
Edit
Cancel Reset Save
Done
Trusted sites
291561

https://rsa-am.cisco-irn.com:7004/console-ims/AddLockoutPolicy.do?action=nvPreEdit&guid=ims.000000000000000000001000e0023000&ptoken=TR0YIL354L3LO91F

Lockout Policy: Initial Lockout Policy

Lockout policies specify the conditions under which user accounts are locked or unlocked by the system after failed authentication attempts.

* Required field

**Lockout Policy Basics**

Lockout Policy Name: * Initial Lockout Policy

Default Policy: ☑ Set as the default lockout policy

Notes: Initial Lockout Policy

Last Modified: Mar 9, 2011 12:15:08 PM PST by bmcgloth

**Parameters**

Lock User Accounts:
○ Allow unlimited failed authentications
● Lock accounts after 6 consecutive failed authentications within 1 days

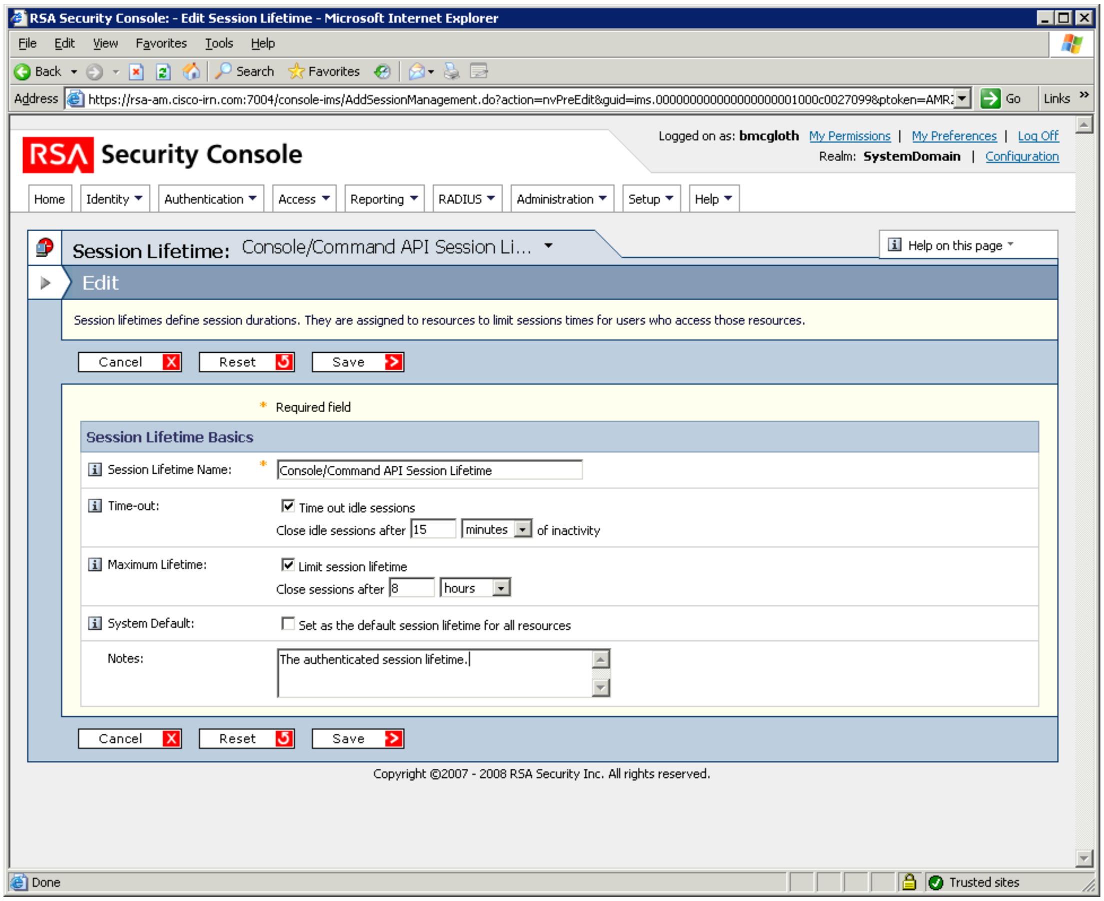
Unlock:
○ Administrators unlock user accounts
● System automatically unlocks accounts after 30 minutes

Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  RSA Authentication Manager supports session policies under the Access tab. Change the Session Time-out for the Console/Command API to 15 minutes from the default, as shown in Figure 5-60.

*Figure 5-60 Session Lifetime for Console*


RSA Security Console: - Edit Session Lifetime - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://rsa-am.cisco-irn.com:7004/console-ims/AddSessionManagement.do?action=nvPreEdit&guid=ims.0000000000000000001000c0027099&ptoken=AMR
Go Links
RSA Security Console
Logged on as: bmcgloth | My Permissions | My Preferences | Log Off
Realm: SystemDomain | Configuration
Home Identity Authentication Access Reporting RADIUS Administration Setup Help
Session Lifetime: Console/Command API Session Li...
Help on this page
Edit
Cancel Reset Save
Done
Trusted sites
291564

Session lifetimes define session durations. They are assigned to resources to limit sessions times for users who access those resources.

* Required field

Session Lifetime Basics

| | |
|---|---|
| Session Lifetime Name: * | Console/Command API Session Lifetime |
| Time-out: | ☑ Time out idle sessions<br>Close idle sessions after 15 minutes of inactivity |
| Maximum Lifetime: | ☑ Limit session lifetime<br>Close sessions after 8 hours |
| System Default: | ☐ Set as the default session lifetime for all resources |
| Notes: | The authenticated session lifetime. |

Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.

RSA Authentication Manager has very powerful and flexible capabilities to define password and account lockout policies to meet all of the above criteria.

### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

RSA Authentication Manager is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*

  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

RSA Authentication Manager uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  Time synchronization for Windows servers is specified through the domain policy. Servers synchronize their clocks with the domain controller, which in turn is synchronized using NTP. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

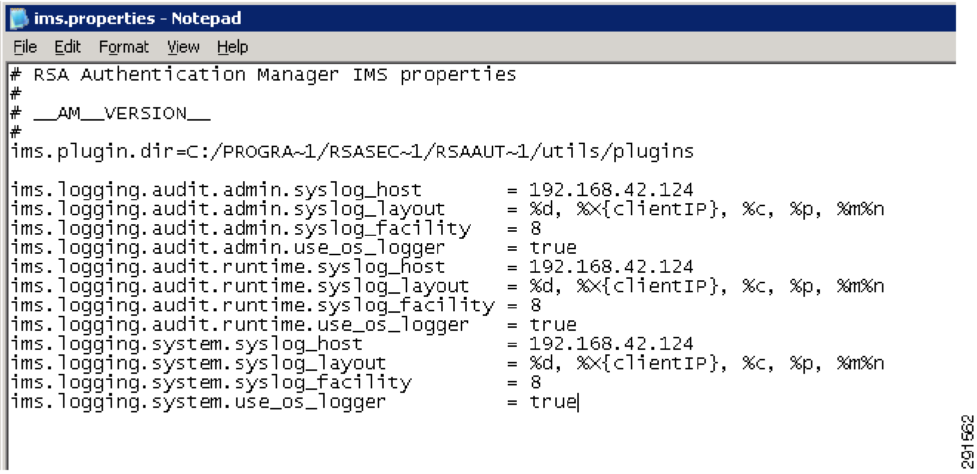
- **PCI 10.5**—*Secure audit trails so they cannot be altered.*

  Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  RSA Authentication Manager can be configured to send its log data to the RSA enVision log management platform to meet the above requirements. The configuration procedure is documented in the enVision Event Source Configuration Guide for RSA Authentication Manager, which can be found at RSA Secure Care Online (https://knowledge.rsasecurity.com/). One step is editing the IMS.Properties file, as shown in Figure 5-61.

*Figure 5-61 IMS Properties File*



```
# RSA Authentication Manager IMS properties
#
# __AM__VERSION__
#
ims.plugin.dir=C:/PROGRA~1/RSASEC~1/RSAAUT~1/utils/plugins

ims.logging.audit.admin.syslog_host       = 192.168.42.124
ims.logging.audit.admin.syslog_layout     = %d, %X{clientIP}, %c, %p, %m%n
ims.logging.audit.admin.syslog_facility   = 8
ims.logging.audit.admin.use_os_logger     = true
ims.logging.audit.runtime.syslog_host     = 192.168.42.124
ims.logging.audit.runtime.syslog_layout   = %d, %X{clientIP}, %c, %p, %m%n
ims.logging.audit.runtime.syslog_facility = 8
ims.logging.audit.runtime.use_os_logger   = true
ims.logging.system.syslog_host            = 192.168.42.124
ims.logging.system.syslog_layout          = %d, %X{clientIP}, %c, %p, %m%n
ims.logging.system.syslog_facility        = 8
ims.logging.system.use_os_logger          = true
```

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

## Cisco TrustSec

Cisco TrustSec, the security component of the Cisco Borderless Network architecture, provides visibility and control into who and what is connected to the network. Cisco TrustSec allows organizations to embrace the rapidly changing business environment of mobility, virtualization, and collaboration while enforcing compliance, maintaining data integrity and confidentiality, and establishing a consistent global access policy. Cisco TrustSec allows businesses to gain complete control over the access points into their networks. This includes all wired, wireless, and VPN network entry points.

Cisco TrustSec ensures that you know what devices and users are on your network, and that those devices and users comply with your security policies via the following components:

- Cisco Identity Services Engine (ISE)—The Cisco ISE is a next-generation policy manager that delivers authentication, authorization, and accounting (AAA); posture; profiling; and guest management services on a single platform. The Cisco ISE automatically discovers and classifies endpoints, provides the right level of access based on identity, and provides the ability to enforce endpoint compliance by checking a device's posture. The Cisco ISE also provides advanced authorization and enforcement capabilities, including Security Group Access (SGA) through the use of security group tags (SGTs) and security group access control lists (ACLs). Administrators can centrally create and manage access control policies for users and endpoints in a consistent fashion, and gain end-to-end visibility into everything that is connected to the network.
- Cisco TrustSec Identity on Cisco Networking Infrastructure—Identity-based networking services on the Cisco routing, switching and wireless infrastructure provides the ability to authenticate users and devices via features such as 802.1x, MAC authentication bypass (MAB), and Web Authentication. In addition, this same infrastructure enforces the appropriate access into parts of the network via VLANs, downloadable or named ACLs, and security group ACLs.

- Client—Cisco AnyConnect VPN Client is a software client that enables you to deploy a single 802.1x authentication framework to access wired and wireless networks while the Cisco NAC agent delivers endpoint posture information. The Cisco TrustSec architecture also supports native OS supplicants.

The Cisco TrustSec solution offers the following benefits:

- Allows enterprises to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise
- Prevents unauthorized network access to protect corporate assets
- Provides complete guest lifecycle management by empowering sponsors to on-board guests, thus reducing IT workload
- Discovers, classifies, and controls endpoints connecting to the network to enable the appropriate services per endpoint type
- Enforces security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without needing administrator attention
- Offers a built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations.

Figure 5-62 shows an example of a Cisco ISE-based TrustSec LAN deployment.

***Figure 5-62 Cisco ISE-Based TrustSec LAN Deployment***

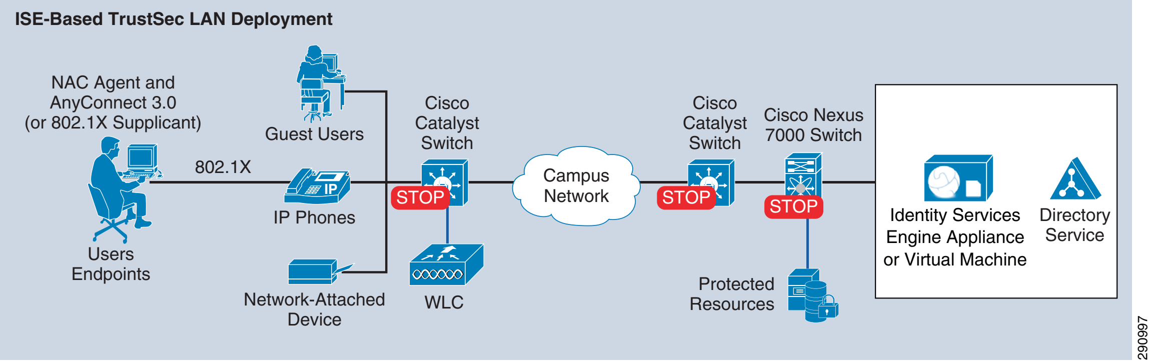


***Table 5-22 PCI Assessment Summary—Cisco Identity Services Engine***

| **Models Assessed** | |
|---|---|
| Cisco Identity Service Engine version 1.0.3.377 | |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 9** | 9.1.2 |
| **PCI 10** | 10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3 |
| **PCI 11** | 11.1.b, 11.1.d |

*Table 5-22 PCI Assessment Summary—Cisco Identity Services Engine (continued)*

| **PCI Sub-Requirements Requiring Compensating Controls** |
|---|
| No compensating controls were required to satisfy any sub-requirements. |
| **PCI Sub-Requirements Failed** |
| No sub-requirements were failed. |

## Primary PCI Function

Cisco ISE and TrustSec identity features detect and prevent rogue wireless devices from connecting to in-scope PCI networks (11.1); in addition, Cisco ISE locks down publicly accessible network ports to only authorized devices and users (9.1.2). In addition to its primary focus, Cisco ISE can also help with compliance and enforcement of requirements 6.1, 7.1, 7.2, 8.3, 8.5, and 10.

Table 5-22 lists the component assessment details for the Cisco TrustSec Solution.

*Table 5-23 Component Capability Assessment—Cisco TrustSec*

| **Cisco TrustSec** | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 7, 11 (7.1, 7.2, 11.1)** |
| Authenticate and authorize users and endpoints via wired, wireless, and VPN. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

For the purposes of this guide, Cisco ISE is configured to authenticate individual users and ISE Admin users using Active Directory (AD). Cisco ISE is also used to profile and assess the posture of individual wired and wireless devices to ensure that they comply with the PCI standard. Cisco ISE relies on

TrustSec wired and wireless identity features such as 802.1x, MAB, and web portal authentication on Cisco infrastructure to collect user identity information. It relies on the Cisco ISE NAC agent and the Cisco ISE profiler engine to collect posture and profiling information from devices. Note the following:

- The solution tested used the virtual machine appliance version of Cisco ISE running on an ESX platform.
- The default accounts for administration are removed.
- HTTPS is enabled and HTTP disabled.
- Cisco ISE communicates with the Cisco switches and wireless controllers using RADIUS.
- Cisco ISE can use dynamic VLAN and port or VLAN access control rules to provide PCI segmentation of a network. For example, members of the PCI active directory group are automatically moved to the PCI VLAN when they connect to the network. Cisco ISE can then apply strong access lists to this VLAN or directly to the user switch port to accomplish segmentation.
- Access control rule sets must adhere to a “least amount of access necessary” policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports required for the cardholder data environment on the point-of-sale networks.
- Configure appropriate banner messages on login, incoming, and exec modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- The Cisco ISE system is configured to be compliance with all of the access controls, logging controls, and other general system controls required by PCI DSS 2.0.

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure. (For example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.)*
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.*

  The Cisco Identity Service Engine appliance does not allow changes to the operating system, to the database, installation of unsupported hardware, or of unsupported third-party software.

  The Cisco ISE management console supports only HTTPS access.

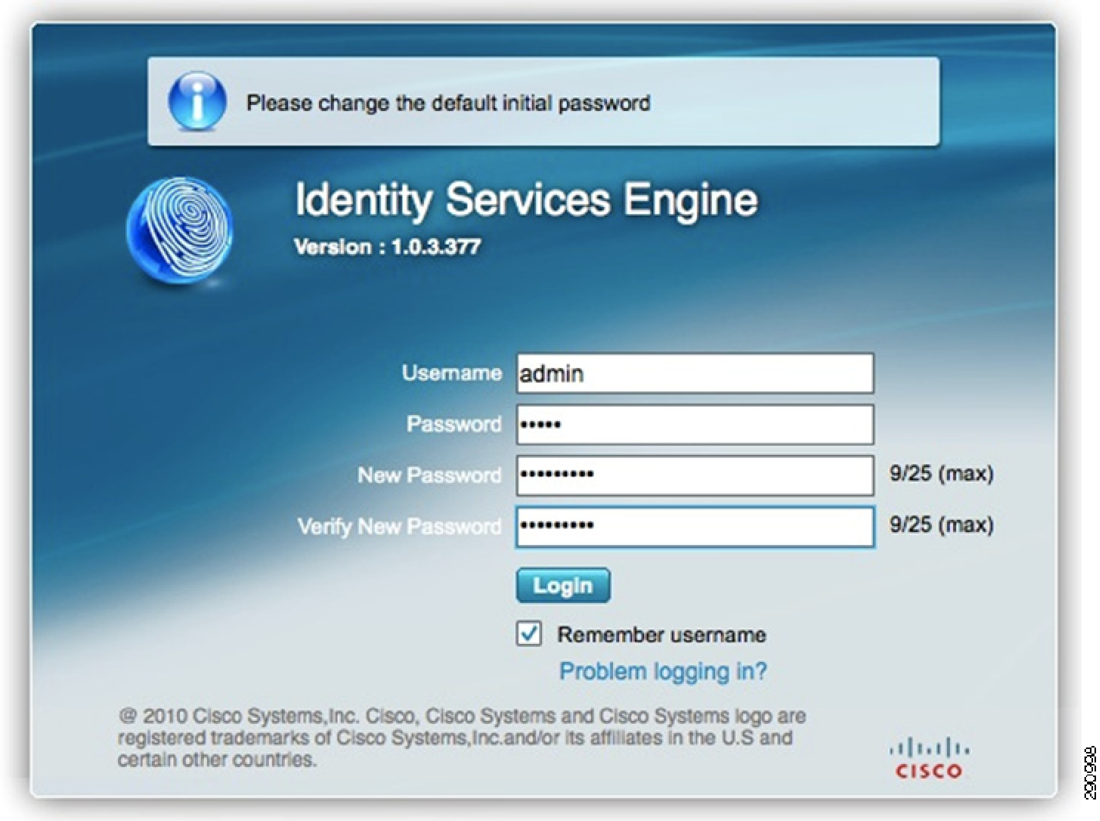
  Cisco ISE is configured to use SSL as a highly secure management portal technology.

  Role-based administration is configured for administrative tasks.

  Cisco ISE was locked down according to generally accepted industry standards and the above PCI requirements.

  Figure 5-63 shows the Cisco ISE login screen.

*Figure 5-63 Cisco ISE Login*



Please change the default initial password

Identity Services Engine

Version : 1.0.3.377

Username admin

Password •••••

New Password ••••••••• 9/25 (max)

Verify New Password ••••••••• 9/25 (max)

Login

☑ Remember username

Problem logging in?

@ 2010 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems,Inc.and/or its affiliates in the U.S and certain other countries.

**Requirement 6: Develop and maintain secure systems and applications**

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release*.

**Note** An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices, systems, and databases) and higher than less-critical internal devices, ensuring that high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.

Cisco ISE itself has several auto-update configuration options you can use to keep it current. Cisco ISE can also be upgraded manually.

The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in the Cisco Identity Service Engine. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

Software support for all Cisco products can be located at:
http://www.cisco.com/cisco/software/navigator.html

More importantly, Cisco ISE is able to check all hosts connecting to the network to make sure they are compliant with requirement 6.1. Operating system patches and application patches can be enforced before allowing network access. Cisco ISE can offer remediation options to users who are out of compliance.

### Requirement 7: Restrict access to cardholder data by business need to know

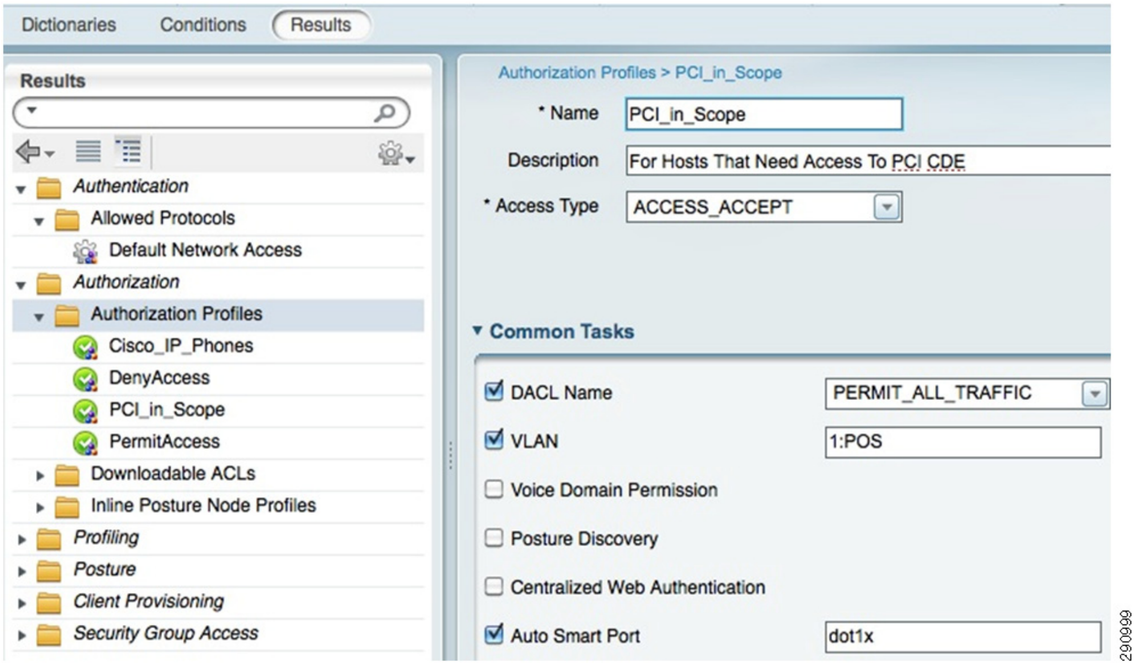
To meet all of the requirements listed below, the Cisco PCI Solution for Retail uses a centralized user database in the Active Directory. This server is located in the data center. Individual user IDs are assigned, and roles are based on group membership. Cisco ISE connects to this resource via native Windows services to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities.*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function.*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system.*

TrustSec identity features and ISE ensure that only privileged users can access the CDE. This is done using the authentication credentials supplied by the wired and wireless infrastructure, along with the AD attributes of a user connecting to the network. Based on a Cisco ISE authorization profile match, that user is put onto the proper VLAN and given a group-specific port access control list to control where they can go on the network. Additionally, a Cisco SmartPort macro can be run on the switchport to ensure they have the proper configuration.

Figure 5-64 shows the Authorization Profiles screen.

*Figure 5-64 Authorization Profiles*



* Name: PCI_in_Scope

Description: For Hosts That Need Access To PCI CDE

* Access Type: ACCESS_ACCEPT

☑ DACL Name: PERMIT_ALL_TRAFFIC

☑ VLAN: 1:POS

☐ Voice Domain Permission

☐ Posture Discovery

☐ Centralized Web Authentication

☑ Auto Smart Port: dot1x

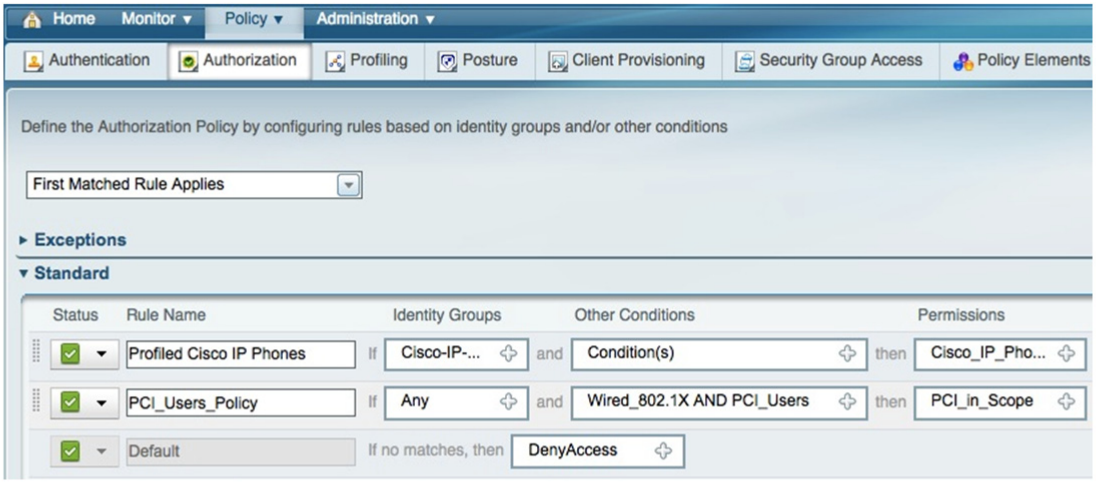
- **PCI 7.2.1**—*Coverage of all system components.*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function.*

- **PCI 7.2.3**—*Default "deny-all" setting.*

  If Cisco ISE does not explicitly match an authorization policy, network access is denied.

  Figure 5-65 shows the Authorization Policy screen.

***Figure 5-65 Authorization Policy***



Define the Authorization Policy by configuring rules based on identity groups and/or other conditions

First Matched Rule Applies

▸ Exceptions

▾ Standard

| Status | Rule Name | | Identity Groups | | Other Conditions | | Permissions |
|---|---|---|---|---|---|---|---|
| ☑ | Profiled Cisco IP Phones | If | Cisco-IP-... | and | Condition(s) | then | Cisco_IP_Pho... |
| ☑ | PCI_Users_Policy | If | Any | and | Wired_802.1X AND PCI_Users | then | PCI_in_Scope |
| ☑ | Default | If no matches, then | DenyAccess | | | | |

#### Requirement 8: Assign a unique ID to each person with computer access

The relevant sub-requirements below were met using the Cisco ISE linked to the windows Active Directory domain. Cisco ISE also supports linking to other authentication servers.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco ISE supports the creation of local user accounts with unique IDs through the use of the **username** command in the CLI or via the Web GUI. These can be used for local fallback user accounts if connectivity to Active directory is lost.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*

  – *Something you know, such as a password or passphrase*

  – *Something you have, such as a token device or smart card*

  – *Something you are, such as a biometric*

  When configuring local user accounts, you must specify a password to achieve PCI compliance.

  Cisco ISE can use any of the methods indicated above to authenticate RADIUS users. The audited configuration for this guide used passwords stored on an Active directory server.

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*All local passwords on the Cisco ISE are stored using strong encryption

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco ISE supports tracking of a users last activity; accounts reviewed as having no activity can then be easily disabled or removed.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

The Cisco ISE password policy support the setting of a password expiration that forces the user to change their password every 90 days.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  The Cisco ISE password policy is configurable to specify a minimum password length.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  The Cisco ISE password policy is configurable to specify an appropriate complexity of numbers and characters.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  The Cisco ISE password policy is configurable to track and prevent the re-use of historical password as configured in the Web GUI.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Compliance with these sub-requirements regarding account lockout was achieved within the solution by implementing the LDAP/AD authentication to Microsoft Active Directory for user account services. The version of Cisco ISE that was validated does not support account lockout for 802.1x authenticated clients, or Web GUI clients.

  Authentications can occur at the switch port level on the wired infrastructure, and on wireless ports via identity features such as 802.1x, MAB, or web authentication.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco ISE is configured to re-authenticate both admin users and RADIUS users every 15 minutes.

  The following is a sample configuration of the Cisco ISE password policy from the CLI:

```
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  no-previous-password
  password-expiration-enabled
  password-expiration-days 90
  password-expiration-warning 10
  min-password-length 7
  password-lock-enabled
  password-lock-retry-count 6
```

### Requirement 9: Restrict Physical Access to Cardholder Data

- **PCI 9.1.2**—*Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.*

### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco ISE uses the local clock facilities of the host server on which it is installed to meet the following requirements.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco ISE uses the local clock facilities to meet the following requirements.

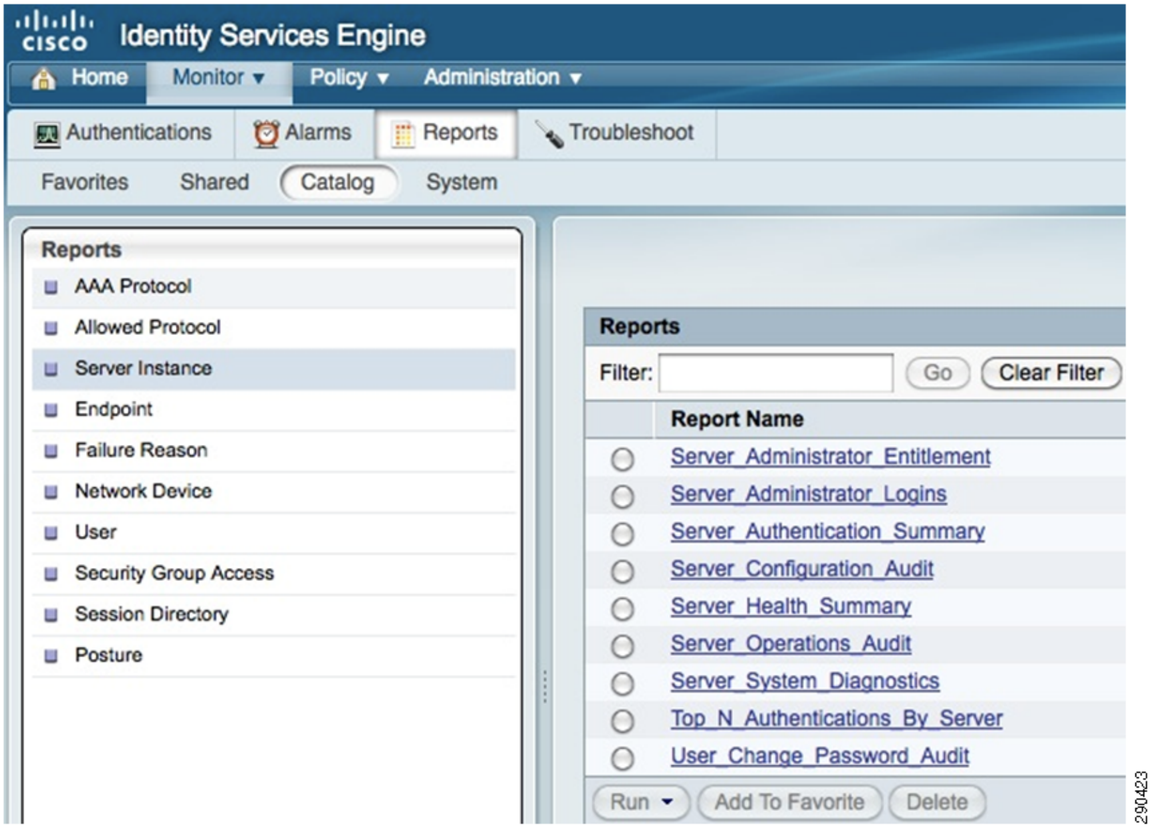
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco ISE uses NTP to meet these requirements by implementing the following configuration statement:

```
ntp server 192.168.62.161 192.168.62.162
```

Figure 5-66 shows the Server Instance screen.

*Figure 5-66 Server Instance*



Reports

- AAA Protocol
- Allowed Protocol
- Server Instance
- Endpoint
- Failure Reason
- Network Device
- User
- Security Group Access
- Session Directory
- Posture

Reports

| | Report Name |
|---|---|
| ○ | Server_Administrator_Entitlement |
| ○ | Server_Administrator_Logins |
| ○ | Server_Authentication_Summary |
| ○ | Server_Configuration_Audit |
| ○ | Server_Health_Summary |
| ○ | Server_Operations_Audit |
| ○ | Server_System_Diagnostics |
| ○ | Top_N_Authentications_By_Server |
| ○ | User_Change_Password_Audit |

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  There is a robust local audit trail configured for Cisco ISE changes. Cisco ISE is configured to audit all RADIUS device access using RADIUS accounting. Note that Cisco ACS can use TACACS+ to accomplish this as well. You need not deploy both solutions.

  Audit log files are backed up daily to a backup server (RSA enVision). Cisco ISE is configured to send change logs to this server as well as provide a list of built-in and custom audit reports on the Cisco ISE system itself.

  The following is a sample configuration:

```
logging 192.168.42.124
logging loglevel 6
```

**Requirement 11: Regularly test security systems and processes.**

The following requirements can be addressed using Cisco network admission control.

- **PCI 11.1.b**—*Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:*
- *WLAN cards inserted into system components*
- *Portable wireless devices connected to system components (for example, by USB, etc.)*
- *Wireless devices attached to a network port or network device*
- **PCI 11.1.d**—*If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel.*

  Cisco NAC capabilities can be configured on the store switches to automate the verification of approved devices being attached to the network. In addition to configuring the NAC authentication services in the data center, add the following configurations to the switch and switch interface ports where NAC is to be used (for example, publicly accessible ports):

```
Pre-requirements for NAC (domain name, name server, time settings, crypto keys):
 ip domain-name cisco-irn.com
 ip name-server 192.168.42.130
 Crypto key generate rsa 1024
 ntp server 192.168.62.161 prefer
 ntp server 192.168.62.162
 clock timezone PST -8
 clock summer-time PDT recurring
!
! ----Configurations to add for NAC ----
!
aaa new-model
!
!
aaa authentication dot1x default group radius local
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
 client 192.168.42.111
 server-key 7 <removed>
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 5 tries 3
radius-server host 192.168.42.111 auth-port 1812 acct-port 1813 key 7 <removed>
radius-server vsa send accounting
radius-server vsa send authentication
!
authentication mac-move permit
!
!
ip device tracking
ip admission name ise proxy http inactivity-time 60
!
cts sxp enable
cts sxp default source-ip 10.10.111.13 {use Switch Management IP}
!
dot1x system-auth-control
!
fallback profile ise
 ip access-group ACL-DEFAULT in
 ip admission ise
!
! ----Auto Smart Ports Macro method for port configurations-------
!
macro name dot1x
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout tx-period 5
```

**Note** Methods that may be used in the process include but are not limited to wireless network scans, physical site inspections, Network Admission Control (NAC), or wireless IDS/IPS.

Cisco TrustSec Identity features were enabled on the wired infrastructure to authenticate users and devices. The Cisco ISE Policy Manager was configured to not allow an unauthorized access point to connect to the wired network. Cisco ISE was also configured to detect and identify the presence of wireless USB or wireless LAN cards on PC systems acting as peer-to-peer wireless networks. Cisco ISE was configured to alert and mitigate this rogue wireless threat.

Cisco ISE was configured to profile all devices connected to the network. Any access points detected were allowed only if they were in the approved list. All wired ports were set up to authenticate and posture-assess users and devices connecting to the network switches. The device posture assessment included checks for the setup of peer-to-peer wireless network and the setup of a wireless card as an access point on the device. If either of these were true, the device would be denied network access.

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

# Management

## Cisco Security Manager

The Cisco Security Manager is a powerful yet easy-to-use solution for configuring firewall, VPN, and IPS policies on Cisco security appliances, firewalls, routers, and switch modules.

Cisco Security Manager helps enable enterprises to manage and scale security operations efficiently and accurately. Its end-to-end tools provide consistent policy enforcement, quick troubleshooting of security events, and summarized reports from across the security deployment.

Cisco Security Manager enables you to centrally manage security policies over 250 types and models of Cisco security devices. Cisco Security Manager supports integrated provisioning of firewall, IPS, and VPN (most site-to-site, remote access, and SSL) services across the following:

- Cisco IOS/ISR/ASR routers
- Cisco Catalyst switches
- Cisco ASA and PIX security appliances
- Cisco Catalyst Service Modules related to firewall, VPN, and IPS
- Cisco IPS appliances and various service modules for routers and ASA devices

For a complete list of devices and OS versions supported by Cisco Security Manager, see *Supported Devices and Software Versions for Cisco Security Manager* at the following URL: http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html.

The high-performance and easy-to-use integrated event viewer allows you to centrally monitor events from IPS, ASA, and FWSM devices and correlate them to the related configuration policies. This helps identify problems and troubleshoot configurations. Then, using Configuration Manager, you can make adjustments to the configurations and deploy them. Event Viewer supports event management for Cisco ASA, IPS, and FWSM devices.

In addition to the Primary Event Data Store, events can be copied and stored in the Extended Event Data Store. The Extended Event Data Store can be used to back up and archive a larger number of events. This is useful for historical review and analysis of events where Event Viewer can gather event data from both the Primary Event Data Store and the Extended Event Data Store. The Extended Event Data Store can be enabled in Event Management in Security Manager's Administration settings.

For supported platforms and more information, see the “Monitoring and Diagnostics” section of the *User Guide for Cisco Security Manager 4.1* at the following URL: http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html.

The new integrated report management allows you to generate and schedule ASA, IPS, and remote access VPN reports. Reports for ASA and IPS devices are created by aggregating and summarizing events collected by the Event Viewer. Security reports can be used to efficiently monitor, track, and audit network use and security problems reported by managed devices. Report Manager helps in developing and customizing reports for Cisco ASA and IPS devices.

For supported platforms and more information, see the “Monitoring and Diagnostics” part of the *User Guide for Cisco Security Manager 4.1* at the following URL: http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html.

*Table 5-24 PCI Assessment Summary—Cisco Security Manager*

| Models Assessed |
|---|
| Cisco Security Manager version 4.0.1 |

Table 5-24 PCI Assessment Summary—Cisco Security Manager (continued)

| PCI Sub-Requirements Passed | |
|---|---|
| **PCI 2** | 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

## Primary PCI Function

The primary function of Cisco Security Manager is to implement security configuration in firewalls, routers, and intrusion detection devices based on policy templates to secure the cardholder data environment. (1.2) Table 5-24 lists the component assessment details for Cisco Security Manager.

Table 5-25 Component Capability Assessment—Cisco Security Manager

| Cisco Security Manager | |
|---|---|
| PRIMARY FUNCTION | Requirement 1 (1.2) |
| Implement security configuration based on policy templates to secure the cardholder data environment. | |
| CAPABILITY | ASSESSMENT |
| Secure Services | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| Authentication | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| Logs | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

- Use descriptive notes for each rule set. These are displayed as remarks in the running configuration.
- Virtualize firewall rule set deployment by using a consistent interface naming standard.
- Apply the anti-spoofing feature to all interfaces using FlexConfig.

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  There are no unnecessary services enabled by default Cisco Security Manager. Cisco Security Manager should be installed on a hardened operating system.

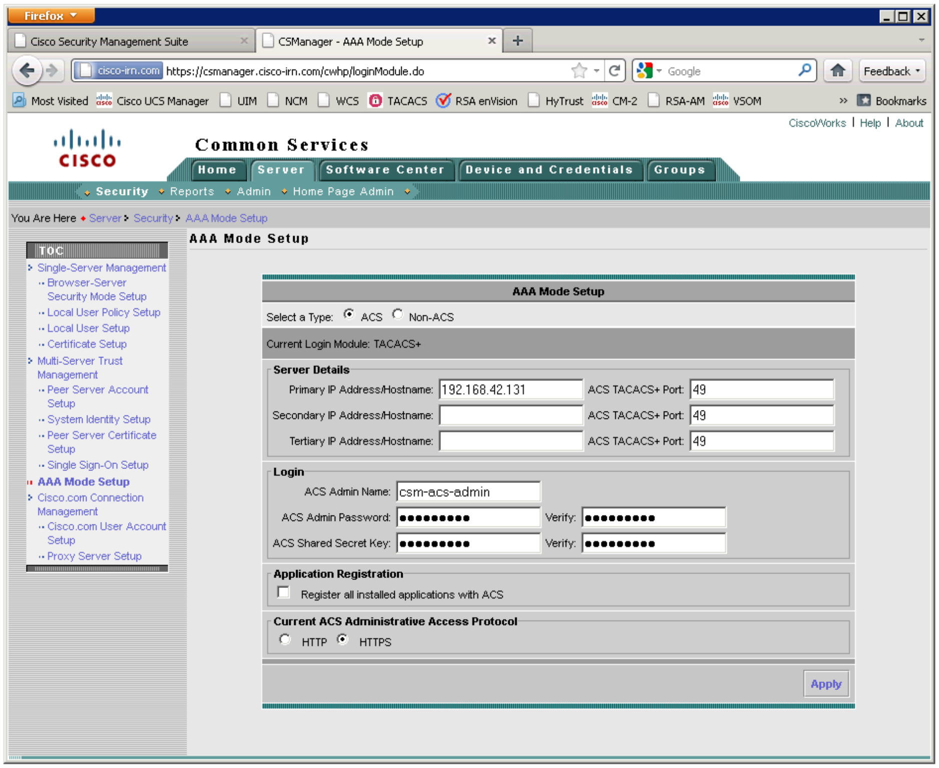
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco Security Manager should be installed on a hardened operating system.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Figure 5-67 shows how the Cisco Security Manager is configured in Common Services for ensuring that only encrypted communications for administration are used.

*Figure 5-67 CSM Secure Administration and AAA Policy*



AAA Mode Setup

AAA Mode Setup

Select a Type: ● ACS ○ Non-ACS

Current Login Module: TACACS+

**Server Details**

Primary IP Address/Hostname: 192.168.42.131 ACS TACACS+ Port: 49

Secondary IP Address/Hostname: ACS TACACS+ Port: 49

Tertiary IP Address/Hostname: ACS TACACS+ Port: 49

**Login**

ACS Admin Name: csm-acs-admin

ACS Admin Password: ●●●●●●●●● Verify: ●●●●●●●●●

ACS Shared Secret Key: ●●●●●●●●● Verify: ●●●●●●●●●

**Application Registration**

☐ Register all installed applications with ACS

**Current ACS Administrative Access Protocol**

○ HTTP ● HTTPS

#### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Security Manager. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at: http://www.cisco.com/cisco/software/navigator.html

#### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

Figure 5-67 shows that Cisco Security Manager AAA role setup type was implemented as Cisco Secure ACS, and identified the appropriate Cisco Secure ACS servers.

#### Requirement 8: Assign a Unique ID to Each Person with Computer Access

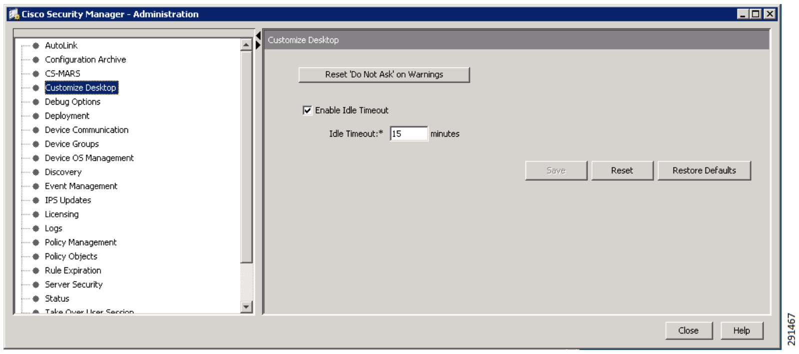
Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

Figure 5-68 shows the configuration setting in the client for setting the idle timeout.

***Figure 5-68 Customize Desktop***



☑ Enable Idle Timeout

Idle Timeout:* 15 minutes

### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco Security Manager is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*

- **PCI 10.3.1**—*User identification*
- **PCI 10.3.2**—*Type of event*
- **PCI 10.3.3**—*Date and time*
- **PCI 10.3.4**—*Success or failure indication*
- **PCI 10.3.5**—*Origination of event*
- **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco Security Manager uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

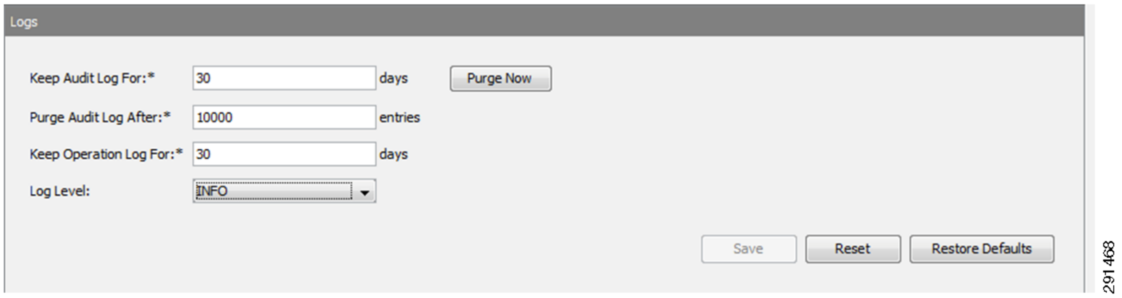
  Time synchronization for Windows servers is specified through the domain policy. Servers synchronize their clocks with the domain controller, which in turn is synchronized using NTP. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

Figure 5-69, Figure 5-70, and Figure 5-71 shows the Logs, Audit Report, and View Settings screens.

***Figure 5-69 Logs***



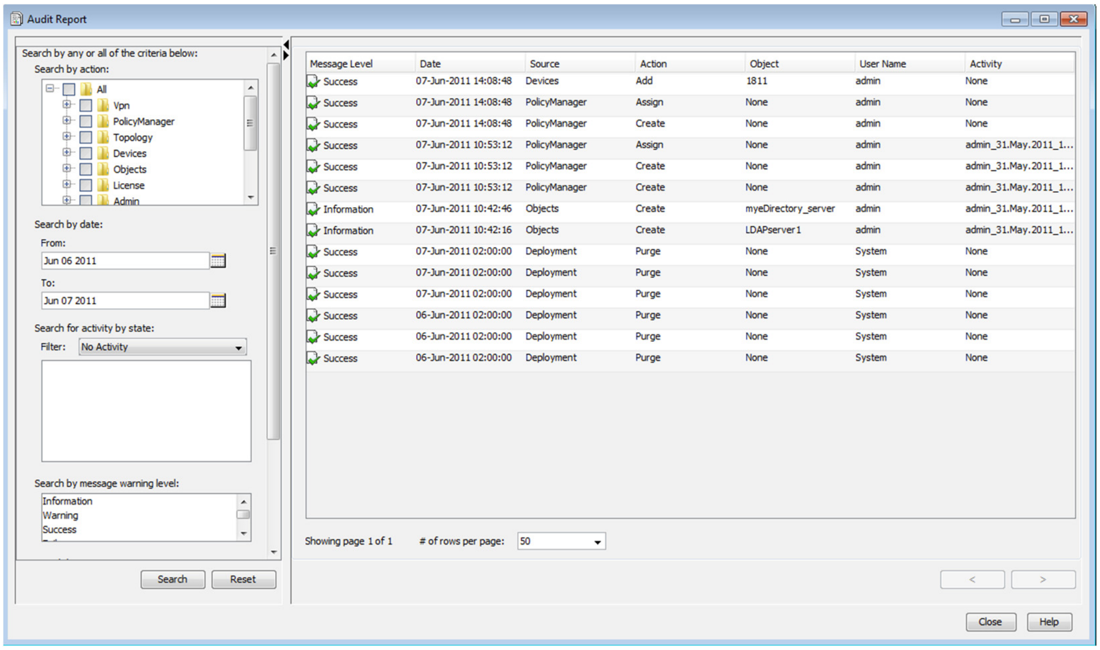
Keep Audit Log For:* 30 days

Purge Audit Log After:* 10000 entries

Keep Operation Log For:* 30 days

Log Level: INFO

*Figure 5-70 Audit Report*



Audit Report

Search by any or all of the criteria below:

Search by action:

- □ All
  - □ Vpn
  - □ PolicyManager
  - □ Topology
  - □ Devices
  - □ Objects
  - □ License
  - □ Admin

Search by date:

From: Jun 06 2011

To: Jun 07 2011

Search for activity by state:

Filter: No Activity

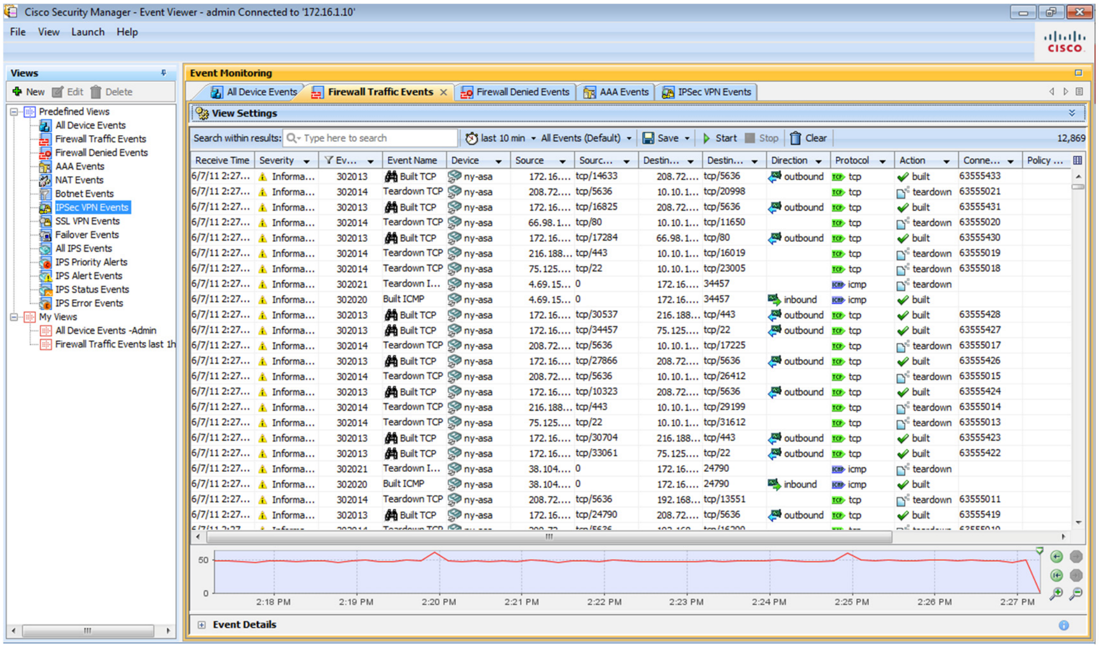
Search by message warning level:

Information
Warning
Success

| Message Level | Date | Source | Action | Object | User Name | Activity |
|---|---|---|---|---|---|---|
| Success | 07-Jun-2011 14:08:48 | Devices | Add | 1811 | admin | None |
| Success | 07-Jun-2011 14:08:48 | PolicyManager | Assign | None | admin | None |
| Success | 07-Jun-2011 14:08:48 | PolicyManager | Create | None | admin | None |
| Success | 07-Jun-2011 10:53:12 | PolicyManager | Assign | None | admin | admin_31.May.2011_1... |
| Success | 07-Jun-2011 10:53:12 | PolicyManager | Create | None | admin | admin_31.May.2011_1... |
| Success | 07-Jun-2011 10:53:12 | PolicyManager | Create | None | admin | admin_31.May.2011_1... |
| Information | 07-Jun-2011 10:42:46 | Objects | Create | myeDirectory_server | admin | admin_31.May.2011_1... |
| Information | 07-Jun-2011 10:42:16 | Objects | Create | LDAPserver1 | admin | admin_31.May.2011_1... |
| Success | 07-Jun-2011 02:00:00 | Deployment | Purge | None | System | None |
| Success | 07-Jun-2011 02:00:00 | Deployment | Purge | None | System | None |
| Success | 07-Jun-2011 02:00:00 | Deployment | Purge | None | System | None |
| Success | 06-Jun-2011 02:00:00 | Deployment | Purge | None | System | None |
| Success | 06-Jun-2011 02:00:00 | Deployment | Purge | None | System | None |
| Success | 06-Jun-2011 02:00:00 | Deployment | Purge | None | System | None |

Showing page 1 of 1 # of rows per page: 50

*Figure 5-71 View Settings*



Cisco Security Manager - Event Viewer - admin Connected to '172.16.1.10'

- Predefined Views
  - All Device Events
  - Firewall Traffic Events
  - Firewall Denied Events
  - AAA Events
  - NAT Events
  - Botnet Events
  - IPSec VPN Events
  - SSL VPN Events
  - Failover Events
  - All IPS Events
  - IPS Priority Alerts
  - IPS Alert Events
  - IPS Status Events
  - IPS Error Events
- My Views
  - All Device Events -Admin
  - Firewall Traffic Events last 1h

Event Monitoring

Search within results: Type here to search | last 10 min | All Events (Default) | Save | Start | Stop | Clear | 12,869

| Receive Time | Severity | Ev... | Event Name | Device | Source | Sourc... | Destin... | Destin... | Direction | Protocol | Action | Conne... | Policy ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 6/7/11 2:27... | Informa... | 302013 | Built TCP | ny-asa | 172.16.... | tcp/14633 | 208.72.... | tcp/5636 | outbound | tcp | built | 63555433 | |
| 6/7/11 2:27... | Informa... | 302014 | Teardown TCP | ny-asa | 208.72.... | tcp/5636 | 10.10.1... | tcp/20998 | | tcp | teardown | 63555021 | |
| 6/7/11 2:27... | Informa... | 302013 | Built TCP | ny-asa | 172.16.... | tcp/16825 | 208.72.... | tcp/5636 | outbound | tcp | built | 63555431 | |
| 6/7/11 2:27... | Informa... | 302014 | Teardown TCP | ny-asa | 66.98.1... | tcp/80 | 10.10.1... | tcp/11650 | | tcp | teardown | 63555020 | |
| 6/7/11 2:27... | Informa... | 302013 | Built TCP | ny-asa | 172.16.... | tcp/17284 | 66.98.1... | tcp/80 | outbound | tcp | built | 63555430 | |
| 6/7/11 2:27... | Informa... | 302014 | Teardown TCP | ny-asa | 216.188... | tcp/443 | 10.10.1... | tcp/16019 | | tcp | teardown | 63555019 | |
| 6/7/11 2:27... | Informa... | 302014 | Teardown TCP | ny-asa | 75.125.... | tcp/22 | 10.10.1... | tcp/23005 | | tcp | teardown | 63555018 | |
| 6/7/11 2:27... | Informa... | 302021 | Teardown I... | ny-asa | 4.69.15... | 0 | 172.16.... | 34457 | | icmp | teardown | | |
| 6/7/11 2:27... | Informa... | 302020 | Built ICMP | ny-asa | 4.69.15... | 0 | 172.16.... | 34457 | inbound | icmp | built | | |
| 6/7/11 2:27... | Informa... | 302013 | Built TCP | ny-asa | 172.16.... | tcp/30537 | 216.188... | tcp/443 | outbound | tcp | built | 63555428 | |
| 6/7/11 2:27... | Informa... | 302013 | Built TCP | ny-asa | 172.16.... | tcp/34457 | 75.125.... | tcp/22 | outbound | tcp | built | 63555427 | |
| 6/7/11 2:27... | Informa... | 302014 | Teardown TCP | ny-asa | 208.72.... | tcp/5636 | 10.10.1... | tcp/17225 | | tcp | teardown | 63555017 | |
| 6/7/11 2:27... | Informa... | 302013 | Built TCP | ny-asa | 172.16.... | tcp/27866 | 208.72.... | tcp/5636 | outbound | tcp | built | 63555426 | |
| 6/7/11 2:27... | Informa... | 302014 | Teardown TCP | ny-asa | 208.72.... | tcp/5636 | 10.10.1... | tcp/26412 | | tcp | teardown | 63555015 | |
| 6/7/11 2:27... | Informa... | 302013 | Built TCP | ny-asa | 172.16.... | tcp/10323 | 208.72.... | tcp/5636 | outbound | tcp | built | 63555424 | |
| 6/7/11 2:27... | Informa... | 302014 | Teardown TCP | ny-asa | 216.188... | tcp/443 | 10.10.1... | tcp/29199 | | tcp | teardown | 63555014 | |
| 6/7/11 2:27... | Informa... | 302014 | Teardown TCP | ny-asa | 75.125.... | tcp/22 | 10.10.1... | tcp/31612 | | tcp | teardown | 63555013 | |
| 6/7/11 2:27... | Informa... | 302013 | Built TCP | ny-asa | 172.16.... | tcp/30704 | 216.188... | tcp/443 | outbound | tcp | built | 63555423 | |
| 6/7/11 2:27... | Informa... | 302013 | Built TCP | ny-asa | 172.16.... | tcp/33061 | 75.125.... | tcp/22 | outbound | tcp | built | 63555422 | |
| 6/7/11 2:27... | Informa... | 302021 | Teardown I... | ny-asa | 38.104.... | 0 | 172.16.... | 24790 | | icmp | teardown | | |
| 6/7/11 2:27... | Informa... | 302020 | Built ICMP | ny-asa | 38.104.... | 0 | 172.16.... | 24790 | inbound | icmp | built | | |
| 6/7/11 2:27... | Informa... | 302014 | Teardown TCP | ny-asa | 208.72.... | tcp/5636 | 192.168... | tcp/13551 | | tcp | teardown | 63555011 | |
| 6/7/11 2:27... | Informa... | 302013 | Built TCP | ny-asa | 172.16.... | tcp/24790 | 208.72.... | tcp/5636 | outbound | tcp | built | 63555419 | |

## PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

## EMC Ionix Network Configuration Manager

EMC Ionix Network Configuration Manager is a model-based, automated network compliance, change, and configuration management product. It delivers features, advantages, and benefits that ensure the compliance, operational efficiency, security, and availability of your network.

Ionix Network Configuration Manager supplies industry-recognized best practices, enhancing collaborative network infrastructure design, verifying controlled change processes, providing network device and service configuration transparency, and ensuring compliance with corporate and regulatory requirements.

*Table 5-26 PCI Assessment Summary—EMC Ionix NCM*

| **Models Assessed** | |
|---|---|
| EMC Ionix Network Configuration Manager version 4.1.0.863 HF7 | |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

### Primary PCI Function

The primary function is to manage network device configuration and verify configuration against policy templates.

Table 5-26 lists the component assessment details for EMC Ionix Network Configuration Manager.

*Table 5-27 Component Capability Assessment—EMC Ionix NCM*

| EMC Ionix NCM | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 1** |
| Manage network device configuration and verify configuration against policy templates. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

No specific design considerations apply when implementing EMC Ionix NCM.

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

#### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  Cisco SMARTnet services provide ongoing access to software updates and security patches.

#### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

#### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

#### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

EMC Ionix Network Configuration Manager is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*
- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

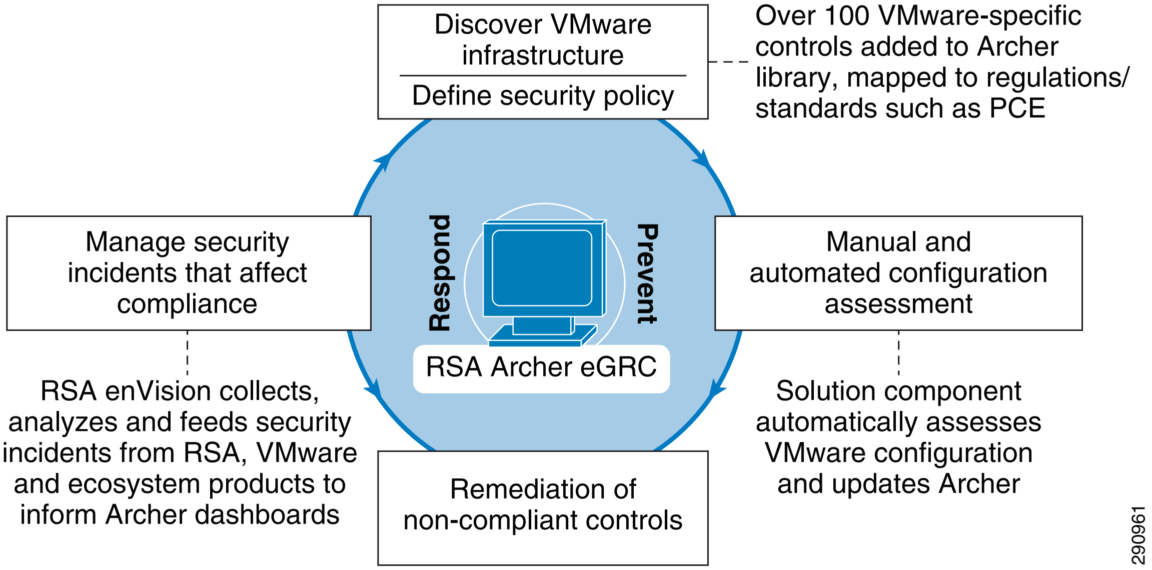
## RSA Archer

The RSA Archer eGRC Suite for enterprise governance, risk, and compliance allows your organization to jumpstart your PCI compliance program by conducting continuous, automated assessments to gain the visibility you need to manage and mitigate risk.

**Note** RSA Archer was initially reviewed by Verizon Business and determined to be outside the scope of the PCI Audit. RSA Archer does store, process, or transmit sensitive cardholder data. There are no Assessment Summary or Capability Assessment details for this product.

RSA Archer provides a comprehensive library of policies, control standards, procedures, and assessments mapped to PCI DSS and other regulatory standards. RSA Archer is designed to orchestrate and visualize the security of both VMware virtualization infrastructure and physical infrastructure from a single console. (See Figure 5-72.)

***Figure 5-72 Using Firewall and IDS/IPS***


Discover VMware infrastructure
Define security policy
Over 100 VMware-specific controls added to Archer library, mapped to regulations/ standards such as PCE
Manage security incidents that affect compliance
Respond
Prevent
RSA Archer eGRC
Manual and automated configuration assessment
RSA enVision collects, analyzes and feeds security incidents from RSA, VMware and ecosystem products to inform Archer dashboards
Remediation of non-compliant controls
Solution component automatically assesses VMware configuration and updates Archer
290961

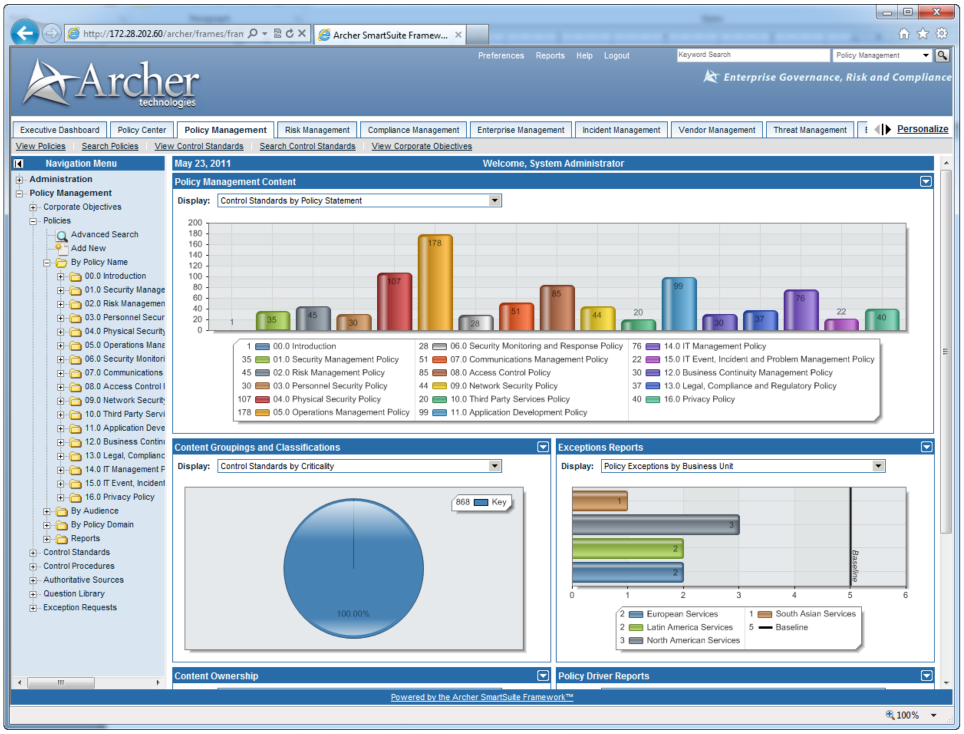
One of the major changes to PCI DSS 2.0 is its clarification on the use of virtualization technology in the cardholder data environment. If virtualization technology is used, the virtualization platform is always in scope for PCI. More than 130 control procedures in the Archer library have been written specifically for VMWare environments and have been mapped to PCI requirements. The RSA Cloud Security and Compliance solution includes software that substantially automates the assessment of whether VMware security controls have been implemented correctly. The results of these automated configuration checks are fed directly into the RSA Archer eGRC Platform, which also captures the results of configuration checks for physical assets via pre-built integration with commercially available scan technologies.

Although a significant number of the VMware control procedures are tested automatically, the remainder must be tested manually because their status cannot be directly inferred from the environment. For these control procedures, project managers can issue manual assessments from the RSA Archer eGRC Platform, using a pre-loaded bank of questions. Project managers can create new questionnaires within minutes and issue them to appropriate users based on asset ownership. Those users are automatically notified of their assessments via rules-driven workflow and My Tasks lists, and can complete their assessments online.

Results for both automated and manual assessments are consolidated in the RSA Archer eGRC Platform and mapped to PCI DSS and other regulations and standards. IT and security operations teams can then monitor compliance with regulations and internal policies across the physical and virtual infrastructure by device, policy, procedure, regulation, and other criteria. This information is presented through a graphical dashboard view, making the information easy to digest and understand.

Configuring the physical and virtual infrastructure according to best-practice security guidelines and regulatory requirements is critical. However, the security and compliance process does not stop there. Organizations also require the ability to monitor misconfigurations, policy violations, and control failures across their infrastructure; and to respond swiftly with appropriate remediation steps. Deficiencies identified through automated and manual configuration checks are captured within the RSA Archer eGRC Platform for management. Control failures are then assigned to appropriate personnel, who can respond by completing remediation tasks or logging exception requests that identify effective compensating controls and are tracked in a Policy Management dashboard, as shown in Figure 5-73.

***Figure 5-73 RSA Archer Policy Management***



# Encryption

A subtle, yet potentially significant change to key management has been introduced with the PCI 2.0 standard. With past versions of the DSS, annual key rotations were required for encryption keys. PCI DSS 2.0 now requires that keys are rotated at the end of their *cryptoperiod*, and references the NIST 800-57 Special Publication to determine what an appropriate cryptoperiod is. The NIST 800-57 Special Publication is a 324-page, three-part document. Merchants, and even QSAs, may not have the expertise to fully understand such a document that includes countless encryption scenarios, with cryptoperiods ranging from as short as a day and as long as three years.

In an ideal world, with all parties being expert cryptographers, this risk-based change to the standard would be very appropriate and most welcome. However, given the number of scenarios and criteria for determining an appropriate cryptoperiod, it could suggest that this change is too subjective and may become a point of contention between a merchant and QSA assessor, as to what is an appropriate cryptoperiod, whereas the former, more prescriptive control, did not allow for flexibility in this area.

## RSA Data Protection Manager

RSA Data Protection Manager (formerly RSA Key Manager) provides encryption, tokenization, and key management capabilities. It can be used to achieve PCI Requirement 3 compliance for protecting stored cardholder data, regardless of where the information resides.

RSA Data Protection Manager is an easy-to-use management tool for encrypting keys at the database, file server, and storage layers. It is designed to lower the total cost of ownership and simplify the deployment of encryption throughout the enterprise. It also helps ensure that information is properly secured and fully accessible when needed at any point in its lifecycle through a powerful management console and built-in high availability features. RSA Data Protection Manager provides a comprehensive platform for enforcing and managing the security of sensitive data.

*Table 5-28 PCI Assessment Summary—RSA Data Protection Manager*

| **Models Assessed** | |
|---|---|
| RSA Data Protection Manager | version KM-3.1 / AM-6.1.SP3 |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

### Primary PCI Function

The main function of RSA Data Protection Manager is to securely manage the keys that protect cardholder data. (3.5)

Table 5-28 lists the component assessment details for RSA Data Protection Manager.

*Table 5-29 Component Capability Assessment—RSA Data Protection Manager*

| RSA Data Protection Manager | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 3 (3.5)** |
| Securely manages the keys that protect cardholder data. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

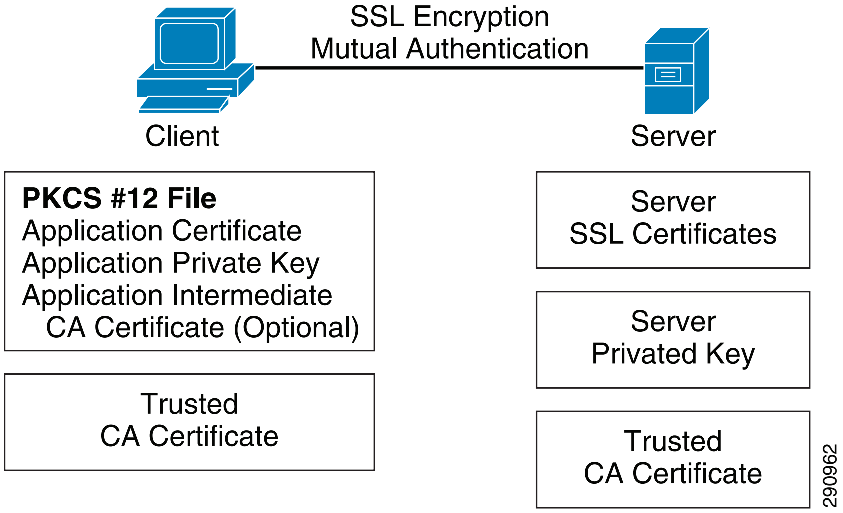
RSA Data Protection Manager's encryption and key management capabilities can be used to store the data in a compliant manner. RSA Data Protection Manager provides application development libraries that support a wide range of development languages and enables developers to easily integrate encryption into point-of-sale, payment, CRM, ERP, and other business applications that create or process sensitive information. RSA Data Protection Manager can also be used to encrypt data as it flows to both disk and tape by providing key management services to Cisco MDS or EMC storage systems.

Because there were no card handling applications in the simulated lab environment, RSA Data Protection Manager was integrated with Cisco MDS to encrypt all data in the environment regardless of whether it was cardholder data or not.

## Public Key Infrastructure (PKI) Requirements

In an RSA Data Protection Manager deployment, a PKI needs to be set up to enable secure communication between the RSA Data Protection server and its clients. (See Figure 5-74.)

*Figure 5-74 RSA Data Protection Manager Deployment*



The certificates and credentials that need to be prepared include:

- Client PKCS#12 certificate and key pair—Used to authenticate RSA Data Protection Manager clients to the RSA Data Protection Server
- Server SSL certificate and key pair—Used by RSA Data Protection Manager Clients to authenticate the server
- Trusted CA certificate—Installed on both clients and the server to verify the signature of certificates sent by a peer. For example, a RSA Key Manager Client has a trusted CA certificate to verify the signature of the Server certificate.
- Middle CA certificate (optional)—If a certificate is not signed directly by a trusted CA certificate, a middle CA certificate should be installed and sent during SSL connection to verify the certificate chain.

## Security Recommendation

Because of vulnerabilities with RSA signatures with a small public exponent, especially 3, RSA recommends that an exponent of F4 (216+1) be used.

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  The appliance version of RSA Data Protection Manager comes pre-hardened. The software version must be installed into a hardened operating system, application server, and database server.

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The appliance version of RSA Data Protection Manager comes pre-hardened. The software version must be installed into a hardened operating system, application server, and database server.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  RSA Data Protection Manager administrative interfaces are protected using SSL.

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  RSA Data Protection Manager publishes security patches at RSA Secure Care Online (https://knowledge.rsasecurity.com/) in accordance with industry best practices to manage and respond to security vulnerabilities to minimize customers' risk of exposure.

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using the included RSA Access Manager Internal Database. Within RSA Data Protection Manager (and the included Access Manager), individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

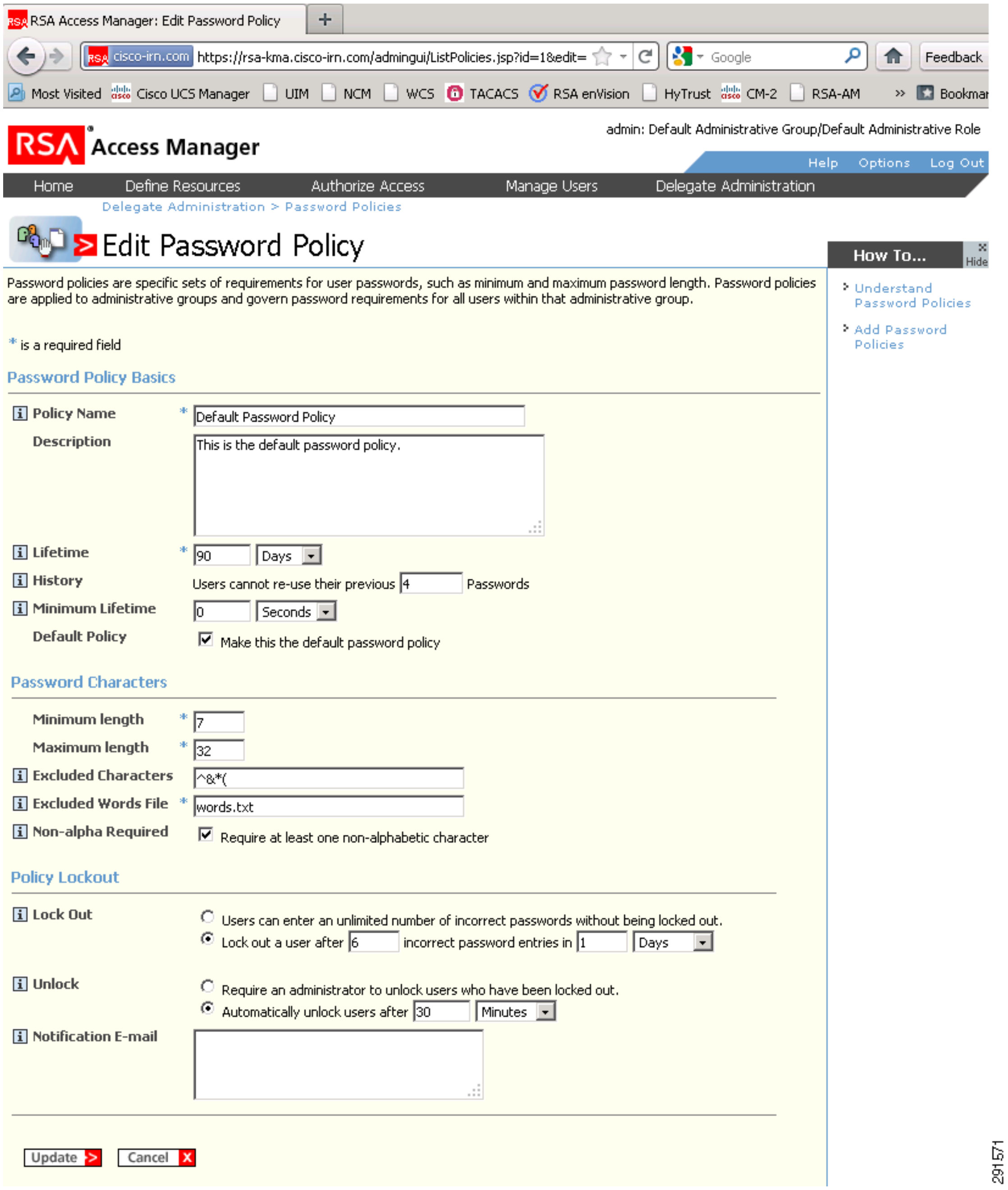
- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  RSA Data Protection Manager embeds and is protected by RSA Access Manager, which has very powerful and flexible capabilities to define password and account lockout policies that can meet all of the above criteria.

  Configuration of user policies is performed via the administration console that can be accessed at the following URL: https://<server address>/admingui/Login.jsp.

  Figure 5-75 shows an appropriate password policy for PCI compliance.

*Figure 5-75 Password Policy Settings*



admin: Default Administrative Group/Default Administrative Role

Edit Password Policy

Password policies are specific sets of requirements for user passwords, such as minimum and maximum password length. Password policies are applied to administrative groups and govern password requirements for all users within that administrative group.

* is a required field

**Password Policy Basics**

| | |
|---|---|
| Policy Name * | Default Password Policy |
| Description | This is the default password policy. |
| Lifetime * | 90 Days |
| History | Users cannot re-use their previous 4 Passwords |
| Minimum Lifetime | 0 Seconds |
| Default Policy | ☑ Make this the default password policy |

**Password Characters**

| | |
|---|---|
| Minimum length * | 7 |
| Maximum length * | 32 |
| Excluded Characters | ^&*( |
| Excluded Words File * | words.txt |
| Non-alpha Required | ☑ Require at least one non-alphabetic character |

**Policy Lockout**

| | |
|---|---|
| Lock Out | ○ Users can enter an unlimited number of incorrect passwords without being locked out.<br>● Lock out a user after 6 incorrect password entries in 1 Days |
| Unlock | ○ Require an administrator to unlock users who have been locked out.<br>● Automatically unlock users after 30 Minutes |
| Notification E-mail | |

Update Cancel

## Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution through configuration of local accounts in the database, as shown below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  RSA Data Protection Manager supports the creation of local users. Through company policy, each user must be assigned a unique ID.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts in RSA Data Protection Manager require the setting of a password according to the assigned password policy
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Through company policy, inactive users should be removed or disabled every 90 days. RSA Data Protection Manager also enables setting of an account expiration date for individual accounts.
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  The Default Password policy can be configured to force users to change their passwords every 90 days, as shown in Figure 5-75.
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  The Default Password policy can be configured to require a minimum of 7 characters, as shown in Figure 5-75.
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  The Default Password policy can be configured require at least one non-alphabetic character by checking the “Non-Alpha Required” box, as shown in Figure 5-75.
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  The Default Password policy can be configured to prevent the re-use of previous passwords by specifying the history number, as shown in Figure 5-75.
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  The Default Password policy can be configured to lock out accounts after a specified number of login failures, as shown in Figure 5-75.
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  The Default Password policy can be configured to lock out accounts for a specified duration or until the administrator re-enables the user ID, as shown in Figure 5-75.
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  RSA Data Protection Manager automatically closes sessions to the administrative consoles after 15 minutes of inactivity.

  RSA Data Protection Manager embeds and is protected by RSA Access Manager, which has very powerful and flexible capabilities to define password and account lockout policies that can meet all of the above criteria.

### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

RSA Data Protection Manager is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

RSA Data Protection Manager uses Network Time Protocol (NTP) to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. The appliance uses NTP to meet these requirements by specifying the appropriate NTP servers during the installation steps. If NTP servers need to be modified, use the following steps:

  1. Open the /etc/ntp.conf file.
  2. Under the List Servers section, provide the ntp server ip address or host name to the server parameter.
  3. Save the /etc/ntp.conf file.
  4. Execute the following commands (as root) to forcibly synchronize the clock of the appliance to the NTP server:

  a. Stop the NTPD daemon by typing the following:

```
service ntpd stop
```

  b. Execute the following command at least three times (to minimize the offset):

```
ntpdate -u <ntpserver>
```

  c. Start the NTPD daemon by typing the following:

```
service ntpd start
```

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*

  Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  RSA Data Protection Manager can be configured to send its log data to the RSA enVision log management platform to meet the above requirements. The configuration procedure is documented in the enVision Event Source Configuration Guide for RSA Data Protection Manager, which can be found at RSA Secure Care Online (https://knowledge.rsasecurity.com/)

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

# Storage

## EMC SAN Disk Array

The EMC SAN disk array is used to securely store sensitive compliance data within the data center. Using virtual storage technology, retailers are able to safely combine (in-scope) sensitive date with (out-of-scope) data while maintaining the compliance boundary.

EMC technology combines midrange networked storage with innovative technology and robust software capabilities to manage and consolidate your data.

*Table 5-30 PCI Assessment Summary—EMC SAN Disk Array*

| **Models Assessed** | |
|---|---|
| EMC CLARiiON CX-240<br>EMC Unified Infrastructure Manager version 2.0.1.1.160 | |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |

*Table 5-30 PCI Assessment Summary—EMC SAN Disk Array (continued)*

| | |
|---|---|
| **PCI 10** | 10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

## Primary PCI Function

The main function of the EMC SAN disk array is to store cardholder data. There is no direct PCI requirement for this storage function.

Table 5-30 lists the component assessment details for the EMC SAN disk array.

*Table 5-31 Component Capability Assessment—EMC SAN Disk Array*

| EMC SAN Disk Array | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement N/A** |
| Securely store sensitive compliance data within the data center. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***“Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

The EMC SAN disk array is a primary component of VCE Vblock architecture. Vblock 1 is designed for medium-to-high numbers of virtual machines, and is ideally suited to a broad range of usage scenarios, including shared services, e-mail, file and print, virtual desktops, and collaboration.

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  The storage management server provides 256-bit symmetric encryption of all data passed between it and the client components that communicate with it, as listed in the "Port Usage" section (Web browser, Secure CLI), as well as all data passed between storage management servers. The encryption is provided via SSL/TLS and uses the RSA encryption algorithm
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The EMC Storage system does not run any unnecessary services by default.
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  When you connect to Unisphere through http://<clariion_ip> (port 80), a Java applet is delivered to the browser on your computer. The applet establishes a secure connection over SSL/TLS (port 443) with the storage management server on the CLARiiON storage system. Therefore, even though "https://" is not displayed in the browser, the connection is secure.

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  EMC Powerlink services provide ongoing access to software updates and security patches.

  CLARiiON storage systems do not support installation of third-party utilities or patches. EMC will provide an officially released FLARE Operating Environment patch if needed to correct a security-related issue (or any other kind of issue).

  For information on product updates, see the following URL:
  https://support.emc.com/products/CLARiiONCX4

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by the EMC SAN disk array using LDAP services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*

- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

When you start a session, Unisphere prompts you for a username, password, and scope (local, global, or LDAP). These credentials are encrypted and sent to the storage management server. The storage management server then attempts to find a match within the user account information. If a match is found, you are identified as an authenticated user.

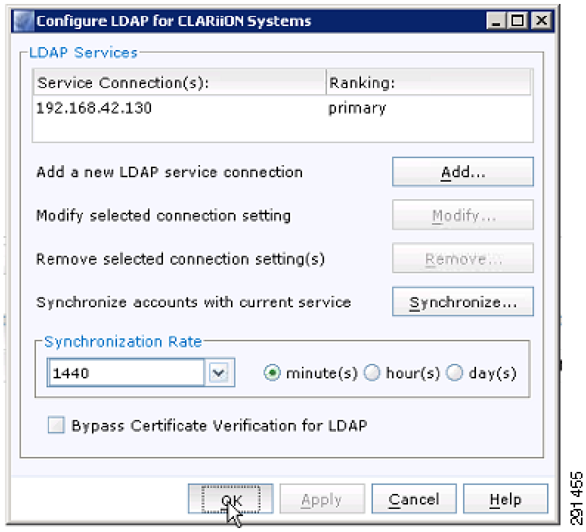
LDAP Authentication should be used for PCI compliance because the local authentication does not meet all PCI 8 requirements for secure user access and accounts.

---

**Step 1** To configure LDAP authentication, go to the Domains tab, then select **Configure LDAP for CLARiiON Systems** from the Users menu on the left.

**Step 2** Add a new LDAP service by clicking **Add** and then **OK**, as shown in Figure 5-76.

***Figure 5-76 Adding LDAP Service***



Configure LDAP for CLARiiON Systems

LDAP Services

| Service Connection(s): | Ranking: |
|---|---|
| 192.168.42.130 | primary |

Add a new LDAP service connection

Modify selected connection setting

Remove selected connection setting(s)

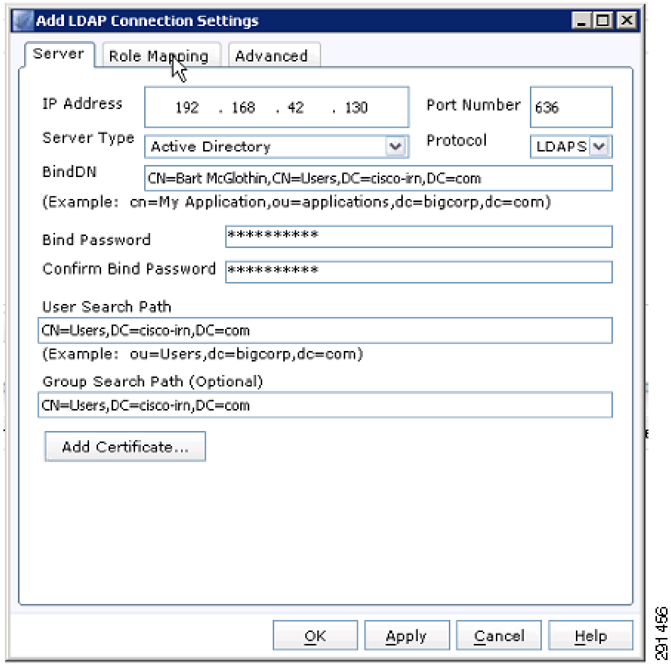
Synchronize accounts with current service

Synchronization Rate: 1440 ● minute(s) ○ hour(s) ○ day(s)

□ Bypass Certificate Verification for LDAP

**Step 3** Configure the LDAP server for Active Directory as shown in Figure 5-77.

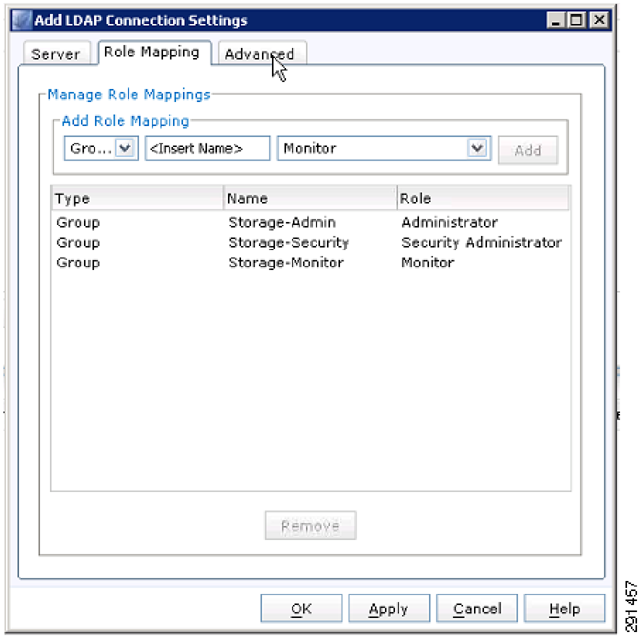
*Figure 5-77 Configuring the LDAP Server for Active Directory*



IP Address 192 . 168 . 42 . 130
Port Number 636
Server Type Active Directory
Protocol LDAPS
BindDN CN=Bart McGlothin,CN=Users,DC=cisco-irn,DC=com
(Example: cn=My Application,ou=applications,dc=bigcorp,dc=com)
Bind Password **********
Confirm Bind Password **********
User Search Path
CN=Users,DC=cisco-irn,DC=com
(Example: ou=Users,dc=bigcorp,dc=com)
Group Search Path (Optional)
CN=Users,DC=cisco-irn,DC=com

**Step 4** After communications are established with the LDAP service, specific LDAP users or groups must be given access to Unisphere by mapping them to Unisphere roles. The LDAP service merely performs the authentication. Once authenticated, user authorization is determined by the assigned Unisphere role. The most flexible configuration is to create LDAP groups that correspond to Unisphere roles. This allows you to control access to Unisphere by managing the members of the LDAP groups. Roles were configured as shown in Figure 5-78.

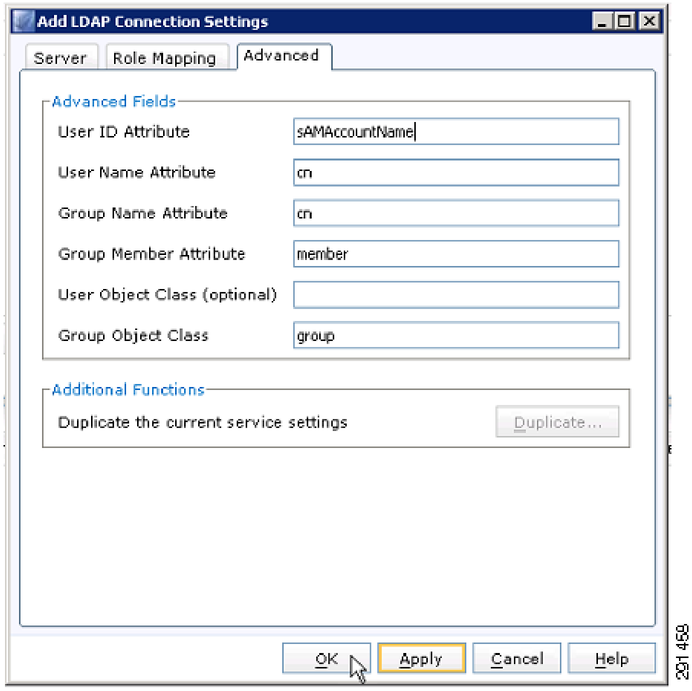
*Figure 5-78 Role Mapping*



| Type | Name | Role |
|---|---|---|
| Group | Storage-Admin | Administrator |
| Group | Storage-Security | Security Administrator |
| Group | Storage-Monitor | Monitor |

**Step 5** The Advanced features were left at their default settings, as shown in Figure 5-79.

*Figure 5-79 Advanced Settings*

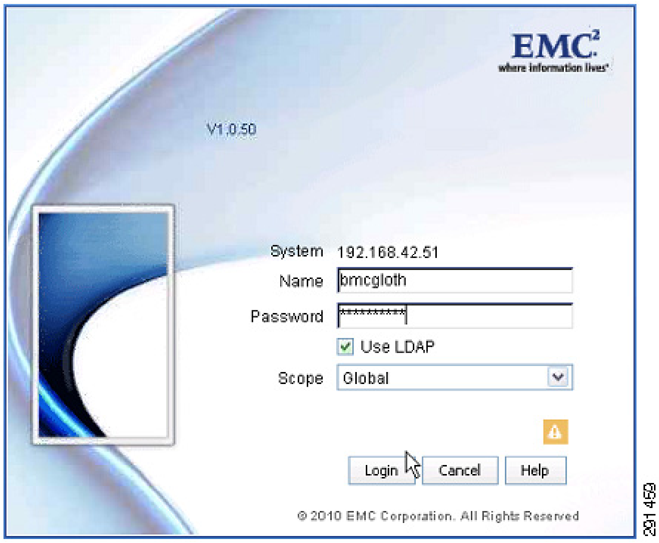


User ID Attribute: sAMAccountName
User Name Attribute: cn
Group Name Attribute: cn
Group Member Attribute: member
User Object Class (optional):
Group Object Class: group

Duplicate the current service settings

**Step 6** You can then log out, and log back in, selecting the **Use LDAP** option for centralized authentication, as shown in Figure 5-80.

*Figure 5-80 Selecting Use LDAP Function*



System 192.168.42.51
Name bmcgloth
Password **********
☑ Use LDAP
Scope Global

**Step 7** For further installation information, see the *FLARE 30 Security Configuration Guide* on EMC Powerlink for configuring LDAP/Active Directory authentication.

### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the LDAP authentication capabilities to the Windows Active Directory server for AAA services. Microsoft Active Directory contains the necessary user account services for all of the appropriate PCI 8 requirements. Configure AAA services as shown above in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.PCI Sub-Requirements with Compensating Controls*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

EMC CLARiiON is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*

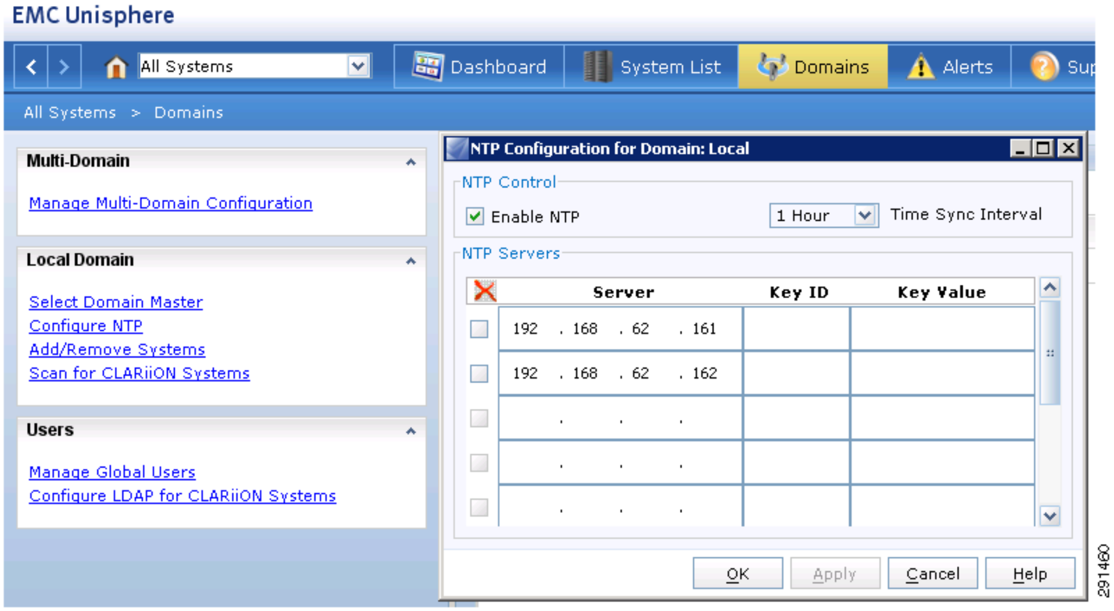
- **PCI 10.3.1**—*User identification*
- **PCI 10.3.2**—*Type of event*
- **PCI 10.3.3**—*Date and time*
- **PCI 10.3.4**—*Success or failure indication*
- **PCI 10.3.5**—*Origination of event*
- **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

EMC CLARiiON uses Network Time Protocol (NTP) to update and synchronize local clock facilities and meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. EMC CLARiion uses NTP to meet these requirements by implementing the configuration statements shown in Figure 5-81.

***Figure 5-81 NTP Configuration for Domain: Local***



NTP Configuration for Domain: Local

NTP Control

☑ Enable NTP

Time Sync Interval: 1 Hour

NTP Servers

| | Server | Key ID | Key Value |
|---|---|---|---|
| □ | 192 . 168 . 62 . 161 | | |
| □ | 192 . 168 . 62 . 162 | | |
| □ | . . . | | |
| □ | . . . | | |
| □ | . . . | | |

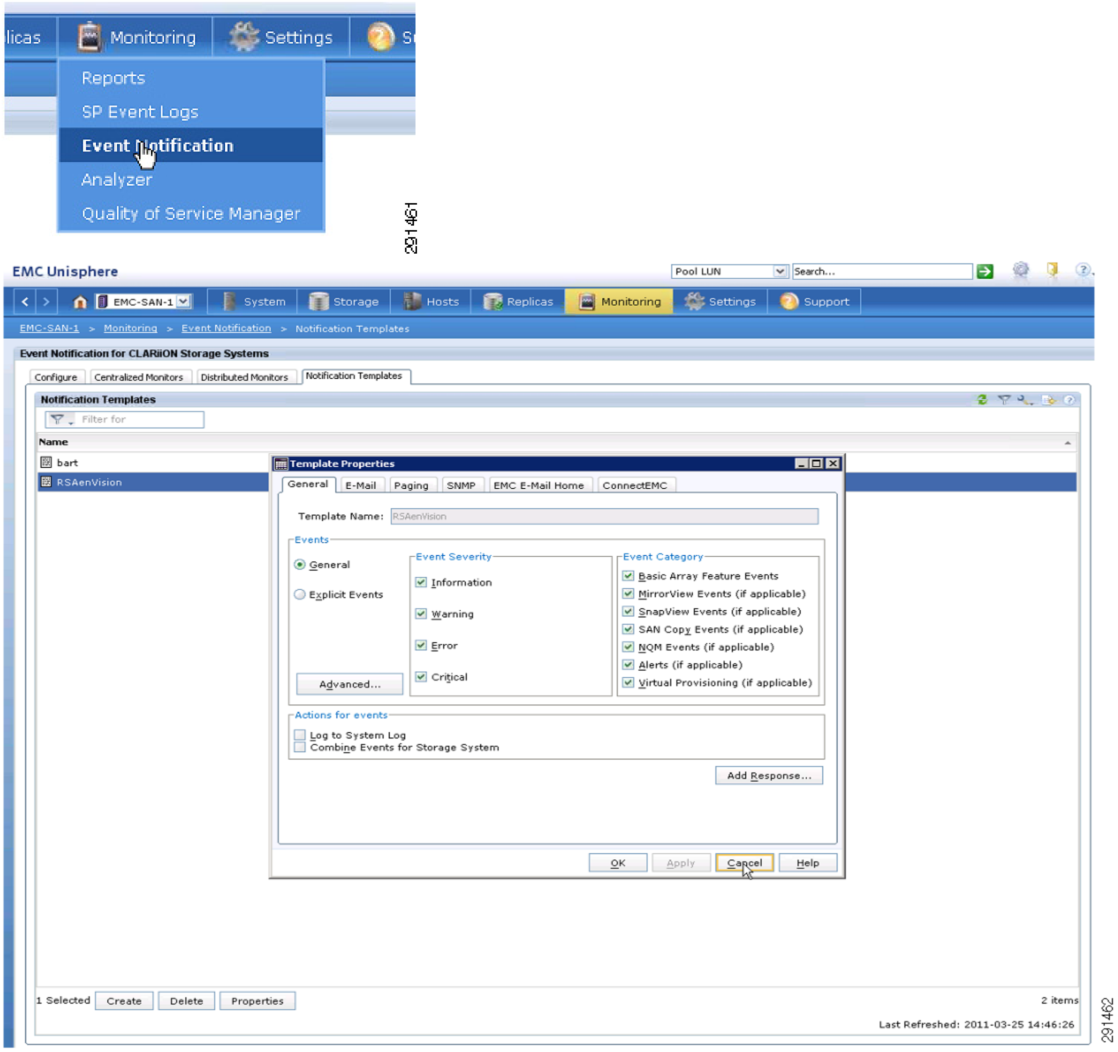
- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

  **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

SP event logs on CLARiiON storage systems can store only a fixed number of events and will wrap if that limit is exceeded. This may take days, weeks, months, or years depending on the logging activity. Therefore, because PCI requires keeping all logs for a set period of time, you need to archive the logs from the CLARiiON storage system on a regular basis. You can do this with the CLI **getlog** command, but a much more integrated method is to use the “log to system log” option of the Event Monitor template to log events to the Windows system log. You can then archive these logs as required.

Additional SNMP Traps are configured to send event notifications directly and immediately to RSA enVision. (See Figure 5-82.)

*Figure 5-82 Using Log to System Log Option*



Template Name: RSAenVision

Events

● General
○ Explicit Events

Event Severity

☑ Information
☑ Warning
☑ Error
☑ Critical

Event Category

☑ Basic Array Feature Events
☑ MirrorView Events (if applicable)
☑ SnapView Events (if applicable)
☑ SAN Copy Events (if applicable)
☑ NQM Events (if applicable)
☑ Alerts (if applicable)
☑ Virtual Provisioning (if applicable)

Actions for events

□ Log to System Log
□ Combine Events for Storage System

## PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls—EMC SAN

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

# Monitoring

## RSA enVision

RSA enVision is a security information and event management (SIEM) platform that provides the capability to implement PCI requirement 10 to track and monitor all access to network resources and cardholder data. RSA enVision does this by collecting, permanently archiving, and processing all the log and event data generated by devices and applications within your network, and generating alerts when it observes suspicious patterns of behavior. Administrators can interrogate the full volume of stored data through an intuitive dashboard, and can use advanced analytical software to gain visibility and understanding of how their network is used and the threats and risks to the infrastructure and applications.

The RSA enVision platform can draw logs from tens of thousands of devices at once, including Cisco network devices, the VCE Vblock infrastructure, the VMware virtual environment, Cisco ASA firewalls, Cisco IPS devices, Cisco IronPort E-mail Appliance, other RSA products, and the HyTrust appliance. Out of the box, RSA enVision can produce PCI 2.0 compliance reports and alerts based on the log and event data it collects. RSA enVision also offers powerful tools to create custom reports and alerts specific to your environment.

*Table 5-32 PCI Assessment Summary—RSA enVision*

| | |
|---|---|
| **Models Assessed** | |
| RSA enVision version 4.0, Revision 5 | |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

### Primary PCI Function

The main function of RSA enVision is to securely store and correlate the system logs that is receives. (10.5)

Table 5-32 lists the component assessment details for RSA enVision.

*Table 5-33 Component Capability Assessment—RSA enVision*

| RSA enVision | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 10 (10.5)** |
| Securely store and correlate the system logs that it receives. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

Depending on the size of your network, RSA enVision may be deployed as a standalone, self-contained, security-hardened appliance or in a distributed deployment to cope with the demands of the largest enterprise networks. When deployed in a distributed architecture, multiple dedicated appliances are deployed where required to perform key roles. Local and remote collectors perform data collection. Data servers manage the data. Application servers perform analysis and reporting. Data itself can be stored using direct attached, online, near-line or offline storage from the full EMC storage portfolio.

RSA enVision does not require any client-side agents to pull log or event data from your infrastructure or applications. RSA enVision can integrate with event sources through standard protocols such as syslog or SNMP by configuring the event source to send data to enVision. For richer event data, enVision integrates with some event sources through their APIs or directly with their database backends. Specific event source device configuration procedures can be found at RSA Secure Care Online (https://knowledge.rsasecurity.com/)

RSA enVision is sold as a standalone appliance. It is available in a variety of hardware options based on the requirements of the enterprise design. The system comes pre-installed on an already hardened operation system.

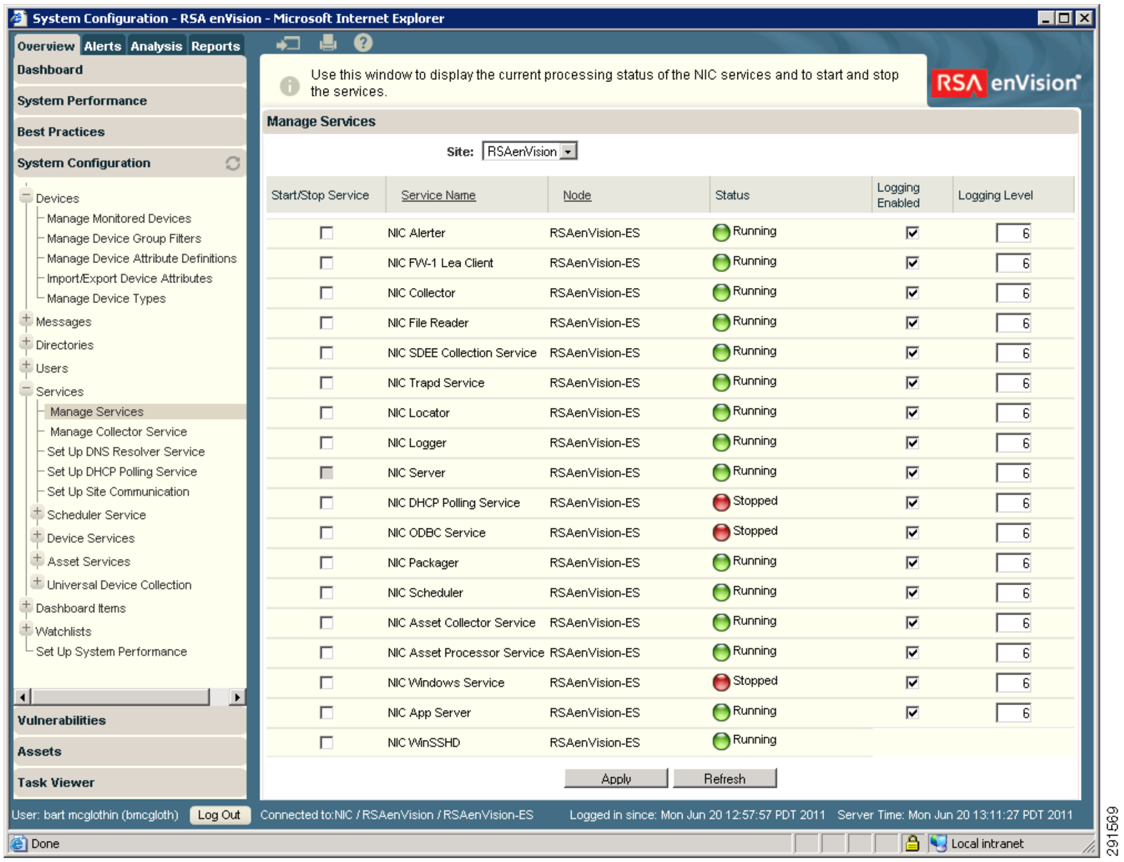
## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  RSA enVision services can be independently enabled or disabled, depending on what protocols are required to collect log and event data, as shown in Figure 5-83.

***Figure 5-83 RSA enVision Managed Services***



Use this window to display the current processing status of the NIC services and to start and stop the services.

Manage Services

Site: RSAenVision

| Start/Stop Service | Service Name | Node | Status | Logging Enabled | Logging Level |
|---|---|---|---|---|---|
| □ | NIC Alerter | RSAenVision-ES | Running | ☑ | 6 |
| □ | NIC FW-1 Lea Client | RSAenVision-ES | Running | ☑ | 6 |
| □ | NIC Collector | RSAenVision-ES | Running | ☑ | 6 |
| □ | NIC File Reader | RSAenVision-ES | Running | ☑ | 6 |
| □ | NIC SDEE Collection Service | RSAenVision-ES | Running | ☑ | 6 |
| □ | NIC Trapd Service | RSAenVision-ES | Running | ☑ | 6 |
| □ | NIC Locator | RSAenVision-ES | Running | ☑ | 6 |
| □ | NIC Logger | RSAenVision-ES | Running | ☑ | 6 |
| ▨ | NIC Server | RSAenVision-ES | Running | ☑ | 6 |
| □ | NIC DHCP Polling Service | RSAenVision-ES | Stopped | ☑ | 6 |
| □ | NIC ODBC Service | RSAenVision-ES | Stopped | ☑ | 6 |
| □ | NIC Packager | RSAenVision-ES | Running | ☑ | 6 |
| □ | NIC Scheduler | RSAenVision-ES | Running | ☑ | 6 |
| □ | NIC Asset Collector Service | RSAenVision-ES | Running | ☑ | 6 |
| □ | NIC Asset Processor Service | RSAenVision-ES | Running | ☑ | 6 |
| □ | NIC Windows Service | RSAenVision-ES | Stopped | ☑ | 6 |
| □ | NIC App Server | RSAenVision-ES | Running | ☑ | 6 |
| □ | NIC WinSSHD | RSAenVision-ES | Running | | |

User: bart mcglothin (bmcgloth) Connected to:NIC / RSAenVision / RSAenVision-ES Logged in since: Mon Jun 20 12:57:57 PDT 2011 Server Time: Mon Jun 20 13:11:27 PDT 2011

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The RSA enVision appliance ships security-hardened. The embedded Windows 2003 server is hardened to remove all unnecessary functionality.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  The RSA enVision web interface is protected using SSL.

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  RSA enVision publishes security patches on RSA Secure Care Online (https://knowledge.rsasecurity.com/) in accordance with industry best practices to manage and respond to security vulnerabilities to minimize customers' risk of exposure.

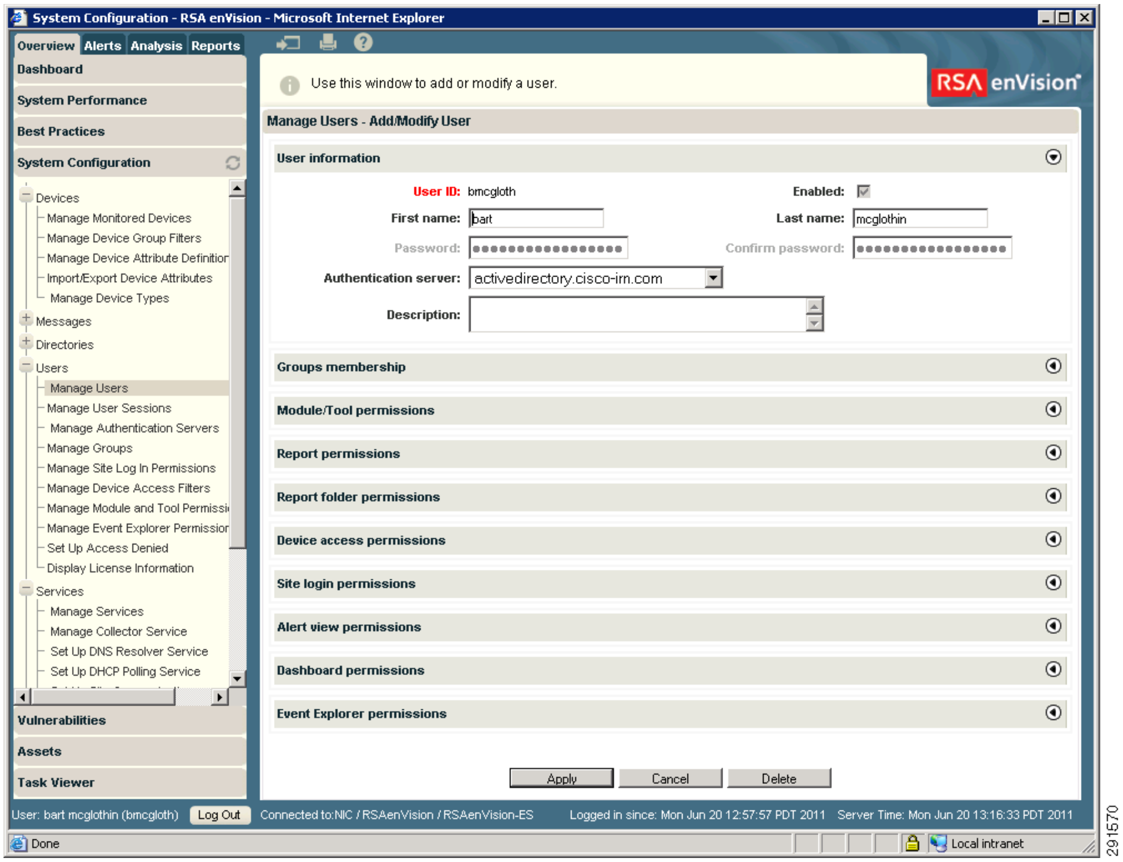
### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 can be met using the RSA enVision Internal Database (as part of its local Windows Active Directory). For validation, RSA enVision was linked to the centralized user database (Active Directory) using LDAP. Within RSA enVision, individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

RSA enVision management interfaces implement role-based access control that can be used to restrict access to privileged user IDs, as shown in Figure 5-84.

Figure 5-84 RSA enVision User Profile



Use this window to add or modify a user.

User ID: bmcgloth
Enabled: ☑
First name: bart
Last name: mcglothin
Password: ●●●●●●●●●●●●●●●●
Confirm password: ●●●●●●●●●●●●●●●●
Authentication server: activedirectory.cisco-irn.com
Description:

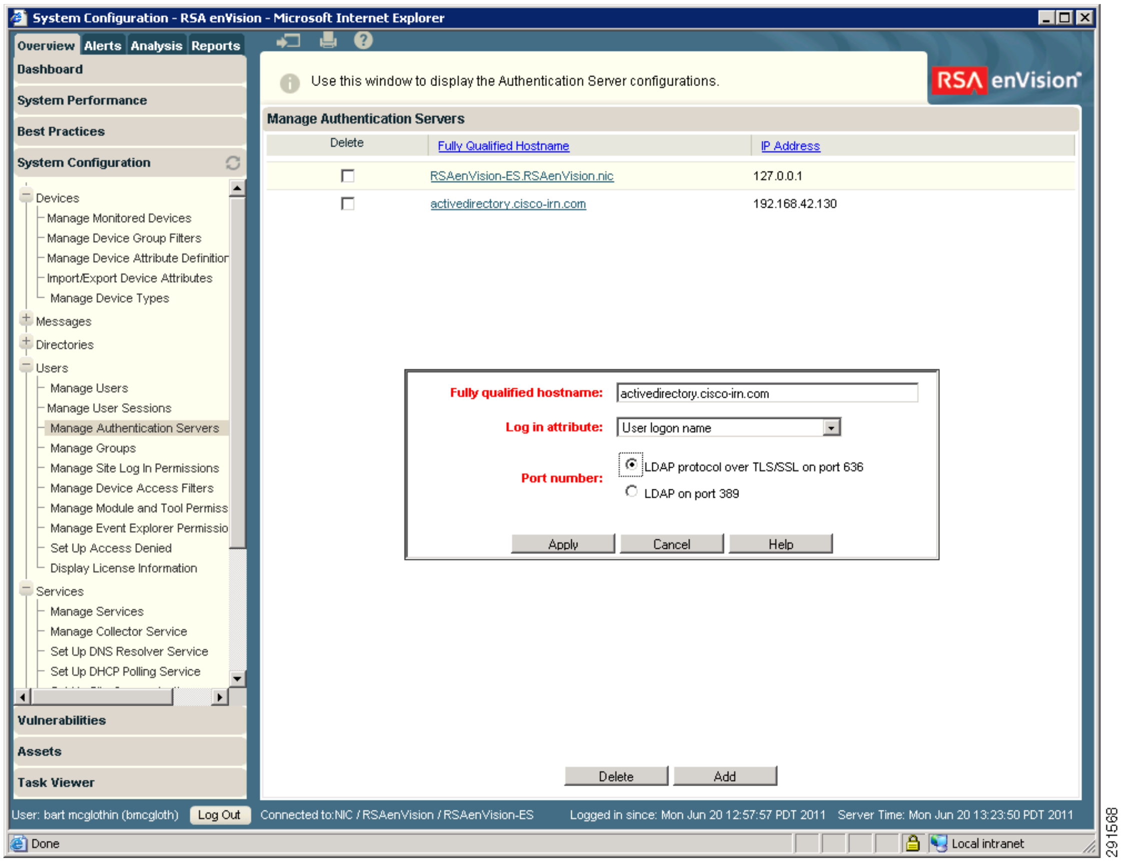
User: bart mcglothin (bmcgloth)
Connected to:NIC / RSAenVision / RSAenVision-ES
Logged in since: Mon Jun 20 12:57:57 PDT 2011
Server Time: Mon Jun 20 13:16:33 PDT 2011

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

RSA enVision's access control system defaults to deny access.

RSA enVision is configurable to use its local Active Directory database, or an external database via LDAP, as shown in Figure 5-85.

*Figure 5-85 RSA enVision Authentication Servers*


System Configuration - RSA enVision - Microsoft Internet Explorer
Overview
Alerts
Analysis
Reports
Dashboard
System Performance
Best Practices
System Configuration
Devices
Manage Monitored Devices
Manage Device Group Filters
Manage Device Attribute Definitior
Import/Export Device Attributes
Manage Device Types
Messages
Directories
Users
Manage Users
Manage User Sessions
Manage Authentication Servers
Manage Groups
Manage Site Log In Permissions
Manage Device Access Filters
Manage Module and Tool Permiss
Manage Event Explorer Permissio
Set Up Access Denied
Display License Information
Services
Manage Services
Manage Collector Service
Set Up DNS Resolver Service
Set Up DHCP Polling Service
Vulnerabilities
Assets
Task Viewer
RSA enVision
Apply
Cancel
Help
Delete
Add
Log Out
Done
Local intranet
291568

Use this window to display the Authentication Server configurations.

Manage Authentication Servers

| Delete | Fully Qualified Hostname | IP Address |
|---|---|---|
| □ | RSAenVision-ES.RSAenVision.nic | 127.0.0.1 |
| □ | activedirectory.cisco-irn.com | 192.168.42.130 |

Fully qualified hostname: activedirectory.cisco-irn.com

Log in attribute: User logon name

Port number: ● LDAP protocol over TLS/SSL on port 636
○ LDAP on port 389

User: bart mcglothin (bmcgloth)   Connected to:NIC / RSAenVision / RSAenVision-ES   Logged in since: Mon Jun 20 12:57:57 PDT 2011   Server Time: Mon Jun 20 13:23:50 PDT 2011

### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the LDAP authentication capabilities to the Windows Active Directory server for AAA services. Microsoft Active Directory contains the necessary user account services for all of the appropriate PCI 8 requirements. Configure AAA services as shown above in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  RSA enVision can authenticate users against external authentication services such as Windows Active Directory using the LDAP protocol. The above policies can be implemented within Windows Active Directory as was validated in this solution.

#### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

RSA enVision is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

RSA enVision uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.4**—*Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  Time synchronization for this windows server is specified through the Domain Policy because the RSA enVision appliance is itself a Domain Controller. The server synchronizes its clock to know time sources using NTP as specified in the initial appliance setup. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*

  Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

  RSA enVision delivers mirrored, unfiltered data to its Internet Protocol Database, which provides the ability to retain data in its original format. Further, "write once, read many" capabilities help ensure that the mirrored copy remains intact, even if the original data is compromised. RSA enVision-captured event logs are stored on a hardened operating system and protected using an integrity check mechanism.

- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*

  RSA enVision's management interfaces implement a role-based access control system to limit who has access to log data.

- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*

  RSA enVision-captured event logs are stored on a hardened operating system in a compressed form and protected via an integrity check mechanism. Access to the operating system and enVision management interfaces can be restricted through operating system and enVision access control systems.

- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

  RSA enVision's primary function is to provide a centralized point for tracking and monitoring access to cardholder data throughout a PCI environment.

- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  RSA enVision stores event data in a tamper evident manner using an internal integrity checking mechanism.

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

## HyTrust Appliance

Vblock Infrastructure Platforms from VCE allow retailers to take advantage of the architectural, operational, and financial benefits of virtualization in their PCI infrastructure. HyTrust Appliance (HTA) complements Vblock capabilities by providing:

- Access control for virtual infrastructure including least privilege, separation of duties, and two-factor authentication
- Granular and exhaustive logging and auditing
- Segmentation of infrastructure to support virtualized applications

PCI DSS 2.0 clarifies the use of virtualization technology with the cardholder data environment (CDE) and specifies that the platform is always in scope. This requirement is consistent with additional risks introduced by mobility and the fast-paced change rate of virtualized assets that can now be reconfigured, relocated, and duplicated by remote administrators. These capabilities combined with poor access control create a significant risk. Hypervisor logs geared toward software maintenance and troubleshooting are obviously useful, but not in the context of a compliance audit.

HyTrust Appliance systematically addresses the three broad areas of IT control objectives (access and user administration, change and configuration, and operations), by proactively enforcing policies for all administrative access, regardless of access method: Secure Shell (SSH) to host, VMware vSphere client to host, or VMware vCenter or any of the programmatic access. HyTrust Appliance provides two-factor authentication and role-based access control, logical segmentation of shared infrastructure, root password vaulting, and audit-quality logs of every attempted access.

*Table 5-34 PCI Assessment Summary—HyTrust Appliance*

| **Models Assessed** | |
|---|---|
| HyTrust version 2.2.1.14064 | |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

## Primary PCI Function

The primary function of HyTrust Appliance is to provide an automated control and audit facility for the virtual infrastructure and cloud stack. (2, 7, and 10).

Table 5-34 lists the component assessment details for the HyTrust Appliance.

*Table 5-35 Component Capability Assessment—HyTrust Appliance*

| HyTrust Appliance | |
|---|---|
| PRIMARY FUNCTION | **Requirement 2.3, 7.1, 10.5** |
| Monitor and secure access to the virtual infrastructure by proxying administrative sessions to VMware vCenter. | |
| CAPABILITY | ASSESSMENT |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

Define rules and deploy policy to activate protection for the virtual infrastructure.

Administrators can define custom rules that restrict entitlement based on specific virtual infrastructure objects that users need to access and manage. Rules that define entitlement can be based on pre-defined roles or administrators can use custom user-defined roles.

The Hytrust appliance provides complete logging of administrator actions by proxying VMware vCenter client connections to the vSphere management server, and clients that try to connect directly to ESX/ESXi hosts. This logging includes the source IP address of the clients, permitted actions and actions that are blocked because the client may not have sufficient privileges (all requirements of PCI that VMware cannot perform natively).

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  HyTrust Appliance configures the virtualization platform (VMware ESX server) to disable unsecure protocols. In addition, HyTrust Appliance proxies non-console management access and redirects attempts to connect via the HTTP management protocol to HTTPS-based connections. In the reference implementation, the configuration of VMware ESX 4.0 servers was performed in accordance with the HyTrust default PCI configuration template. Specifically, the following controls are set:

  ```
  ssh_config: Protocol = 2
  sshd_config:
  Protocol = 2
  X11Forwarding = yes
  IgnoreRhosts = yes
  RhostsAuthentication = no
  RhostsRSAAuthentication = no
  HostbasedAuthentication =no
  PermitRootLogin = no
  PermitEmptyPasswords = no
  Banner = /etc/issue.net if not set
  ```

  Check that a BIOS password is set and that it is not the manufacturer default. For more information, see the following URL: http://www.pwcrack.com/bios.shtml

  Set file permissions on */etc/snmp.conf* and */etc/snmp.conf/preesx* to 700, and set *root* as owner and group.

  Replace the default "COMMUNITY" phrase with a stronger passphrase.

  Restrict SNMP access to authorized IP addresses on a separate admin-network.

  Use read-only mode.

  ```
  - chown root:root & chmod 0600 /etc/security/console.perms or
  /etc/security/console.perms.d/50-default.perms
  - comment out the lines as needed
  - chmod 644 /etc/{profile, pam.d/system_auth, ntp.conf, passwd, group}
  - chmod 600 /etc/ssh/sshd_config
  - chmod 755 /etc/{ntp, vmware}
  - chmod 440 /etc/sudoers
  - chmod 400 /etc/shadow
  ```

  Establish the following local firewall settings:

  ```
  Ports: 22/sshd/inTCP, 53/dns/outUDP, 67-68/dhcp/UDP, 80/http/inTCP, 427/cim slp/TCP,
  443/https/inTCP, 902/vmwareauthd/ inTCP-outTCPUDP, 2050-5000/vmware/TCPUDP,
  5988-89/cim server/inTCP, 27000/license server/outTCP
  ```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  HyTrust Appliance configures the virtualization platform (VMware ESX server) to disable unnecessary boot services. In addition, HyTrust Appliance restricts the use of **sudo** and **su** services and ensures tighter configuration of copy and paste sharing between the host hypervisor and CDE implemented as a virtual system component.

  In addition, HyTrust Appliance periodically monitors the virtualization platform configuration to ensure ongoing compliance with the above sub-requirements.

In the reference implementation, the configuration of VMware ESX 4.0 servers was performed in accordance with the HyTrust default PCI configuration template. Specifically, the following controls were configured and monitored:

All the boot services were disabled on the VMware ESX server except as follows:

```
S00microcode_ctl S00vmkstart S01vmware S02mptctlnode
S08iptables S09firewall S10network S12syslog S13irqbalance
S20random S55sshd S56rawdevices S56xinetd S58ntpd
S85gpm S85vmware-webAccess S90crond S91httpd.vmware
S99local S99pegasus S99vmware-autostart
```

Add following to each VM dot-vmx file:

```
isolation.tools.copy.enable=false
isolation.tools.paste.enable=false
isolation.tools.setGUIOptions.enable=false
```

Required set-uid programs:

```
pam_timestamp_check, passwd, pwdb_chkpwd, su, unix_chkpwd, vmkload_app, vmware-authd,
vmware-vmx
```

Optional:

```
crontab, ping, sudo, vmkping
```

Special case:

```
ssh-keysign
```

Make sure there is at least one user in the wheel group, then uncomment:

```
"auth required /lib/security/$ISA/pam_wheel.so
use_uid" in /etc/pam.d/su
```

Additionally, HyTrust establishes a system for rotating root passwords for the VMware ESX servers under HyTrust protection and allowing authorized users to check out one-time use time-limited auto-generated root passwords.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  HyTrust Appliance is a closed system based on the CentOS operating system, which implements a limited number of necessary services. Additional security features include the following:

  - Production services run unprivileged
  - No root login is allowed
  - The HTA administrator account is unprivileged
  - Sudoers-based privilege escalation
  - All unencrypted services disabled by default

#### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for* *example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

HyTrust Appliance has the capability to download security updates and fixes directly from the HyTrust web site. When this is enabled, updates are downloaded and installed automatically. Updates can also be distributed as ISO packages and installed manually. To prevent Trojan attacks, HyTrust updates and HTA licenses are signed and validated using public keys.

Updates provided via this facility include security updates to the CentOS, application stack, and software developed by HyTrust.

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

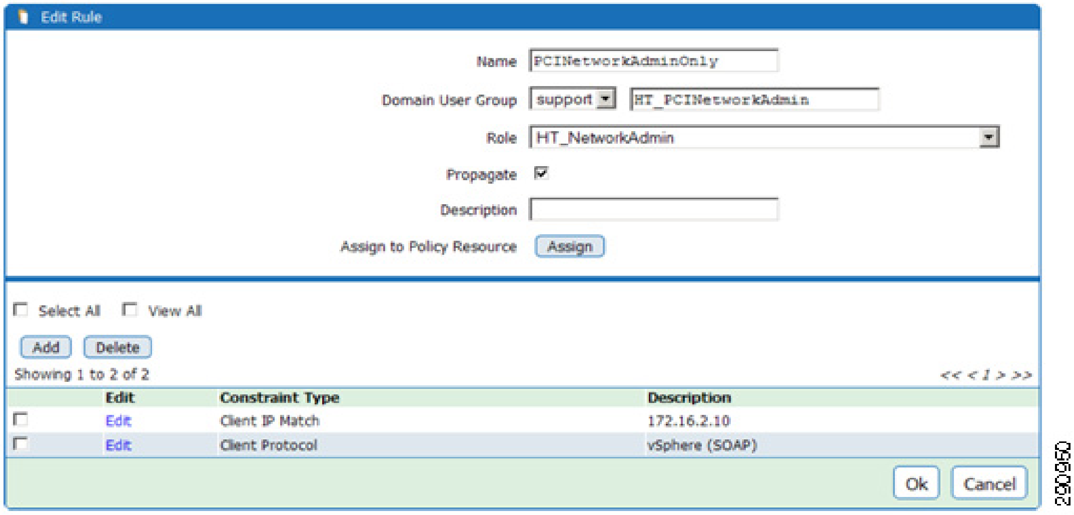
The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory, which is linked via LDAP, RADIUS, and TACACS+ services). Individual user IDs are assigned. Roles are defined and based on group membership. HyTrust Appliance connects to this resource via LDAP to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

HyTrust Appliance implements a sophisticated policy-driven access control system that makes an authorization decision for every attempted operation in the Vblock environment. The authorization decision is based on the user ID as obtained from the vSphere session, the user function as derived from the user's assigned role in Active Directory, logical infrastructure segmentation, least privilege role defined for this activity, and object-level policy active for that user.

In the reference implementation, a policy was created that restricted CDE virtual systems to operating only on the PCI portion of the infrastructure and enforced separation of duties between the network administrators and CDE application owners.

*Figure 5-86 Edit Rule Screen*



Edit Rule

Name PCINetworkAdminOnly

Domain User Group support HT_PCINetworkAdmin

Role HT_NetworkAdmin

Propagate ☑

Description

Assign to Policy Resource

□ Select All □ View All

Showing 1 to 2 of 2

| | Edit | Constraint Type | Description |
|---|---|---|---|
| □ | Edit | Client IP Match | 172.16.2.10 |
| □ | Edit | Client Protocol | vSphere (SOAP) |

Policy and privilege definition was performed by a separate group of authorized users, typically security professionals.

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  HyTrust Appliance implements default "deny all" access policy. Many of the users that gain access to Vblock infrastructure by the means of HyTrust Appliance proxying their operations do not have privileges to log into the HyTrust Appliance management console.

#### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing LDAP to the domain controller for AAA services and Microsoft Active Directory policy for user account services. Configure AAA services as shown in Requirement 7.

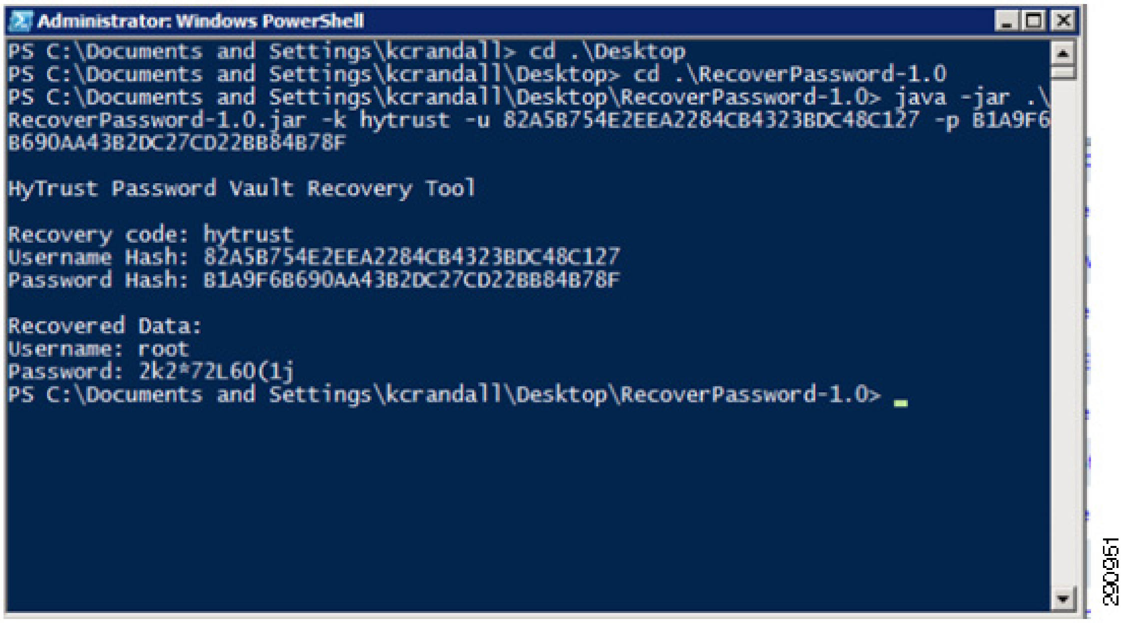
- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Sub-requirement 8.2 is met by supporting RSA two-factor authentication where the user enters the AD password (something they know) in conjunction with an RSA physical token (something they have).

  HyTrust Appliance acts as a compensating control for the Vblock infrastructure and enables RSA two-factor authentication to work with any methods of access to VMware vSphere or Cisco Nexus 1000V.
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.8**—
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  HyTrust Appliance enforces the use of one-time root passwords for all VMware ESX hosts in the environment. Unique random machine-generated passwords of 12 characters in length are set up for each host and rotated every five days (see Figure 5-87). If requested by a privileged user, a different one-time use password was generated and remained valid for a fixed time duration not to exceed 24 hours. Sub-requirement 8.5.8 was met by allowing only one temporary use password to be issued at the time, thus associating the password with a specific user who was issued the password.

*Figure 5-87 Using Root Passwords*



```
PS C:\Documents and Settings\kcrandall> cd .\Desktop
PS C:\Documents and Settings\kcrandall\Desktop> cd .\RecoverPassword-1.0
PS C:\Documents and Settings\kcrandall\Desktop\RecoverPassword-1.0> java -jar .\
RecoverPassword-1.0.jar -k hytrust -u 82A5B754E2EEA2284CB4323BDC48C127 -p B1A9F6
B690AA43B2DC27CD22BB84B78F

HyTrust Password Vault Recovery Tool

Recovery code: hytrust
Username Hash: 82A5B754E2EEA2284CB4323BDC48C127
Password Hash: B1A9F6B690AA43B2DC27CD22BB84B78F

Recovered Data:
Username: root
Password: 2k2*72L60(1j
PS C:\Documents and Settings\kcrandall\Desktop\RecoverPassword-1.0> _
```

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Sub-requirements 8.1, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, and 8.5.15 were met by integrating HyTrust Appliance authentication with Microsoft Active Directory. User accounts and passwords are not managed on HyTrust Appliance; instead, when authentication is requested by the user, HyTrust Appliance performs the actual authentication request against Active Directory. Complex AD environments with multiple domains are supported for authentication.

### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

HyTrust Appliance is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*

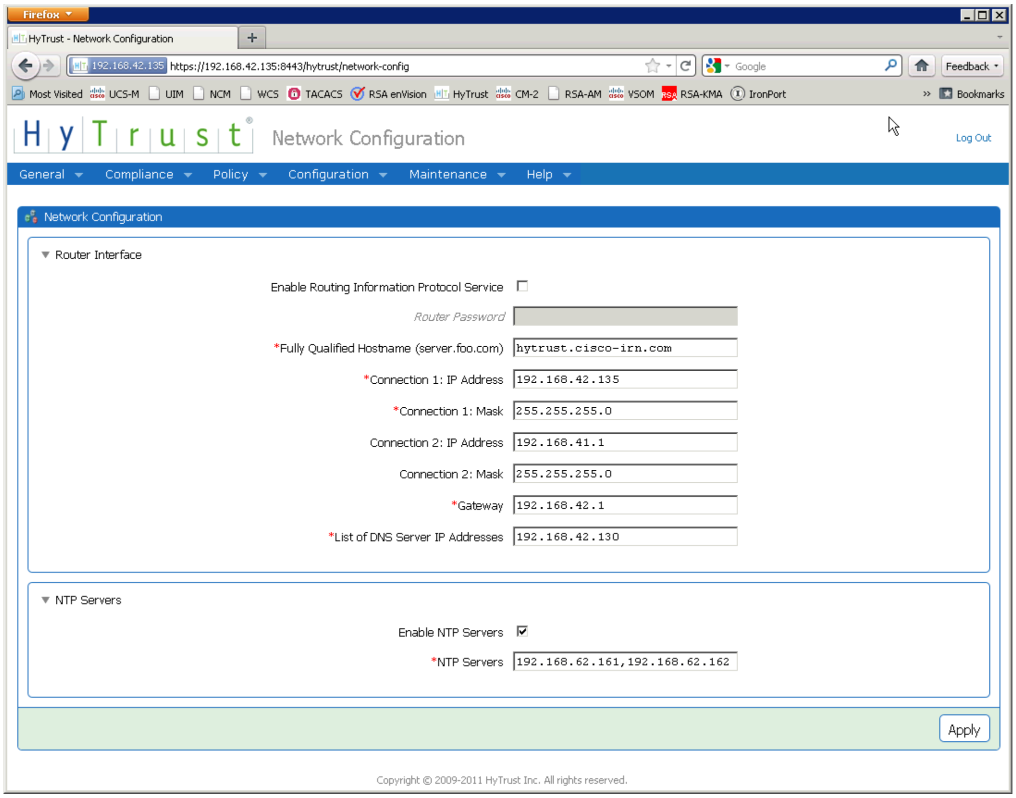
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

HyTrust Appliance uses NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. The HyTrust Appliance uses NTP to meet these requirements by specifying the NTP server in the IP settings. (See Figure 5-88.)

***Figure 5-88 Specifying the NTP Server***



| | |
|---|---|
| Enable Routing Information Protocol Service | □ |
| Router Password | |
| *Fully Qualified Hostname (server.foo.com) | hytrust.cisco-irn.com |
| *Connection 1: IP Address | 192.168.42.135 |
| *Connection 1: Mask | 255.255.255.0 |
| Connection 2: IP Address | 192.168.41.1 |
| Connection 2: Mask | 255.255.255.0 |
| *Gateway | 192.168.42.1 |
| *List of DNS Server IP Addresses | 192.168.42.130 |
| Enable NTP Servers | ☑ |
| *NTP Servers | 192.168.62.161,192.168.62.162 |

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

#### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

#### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

## Additional In Scope Devices

Any system that stores, processes, or transmits cardholder data is considered in scope for PCI compliance. Infrastructure components that provide network services such as load balancing or WAN optimization are often not considered when contemplating compliance. However, if these technologies pass sensitive data, they are subject to the same controls of traditional security products.

The capabilities that these components need to meet are highlighted in Table 5-1.

# Infrastructure

## Routing

### Router—Store

The Cisco Integrated Services Router (ISR) is the component that is used as the primary routing and security platform of the stores. It can securely scale to the requirements of the business because it has integrated firewall, VPN, and IPS/IDS capabilities. WAN options include traditional terrestrial paths using T1, T3, Ethernet, and so on; wireless options include 3G/4G/Wi-Fi modules connecting stores over public paths for higher availability.

The Cisco ISR consolidates voice, data, and security into a single platform with local and centralized management services. It delivers scalable rich media, service virtualization, and energy efficiency ideal for deployments requiring business continuity, WAN flexibility, and superior collaboration capabilities. The Cisco ISR uses field-upgradeable motherboards, with services such as security, mobility, WAN optimization, unified communications, video, and customized applications.

Table 5-36 lists the performance of the Cisco ISR in satisfying PCI sub-requirements.

*Table 5-36 PCI Assessment Summary—Cisco ISR*

| **Models Assessed** | |
|---|---|
| CISCO891W version c890-universalk9-mz.151-3.T.bin | |
| CISCO1941W-A/K9 version c1900-universalk9-mz.SPA.151-3.T.bin | |
| CISCO2921/K9 version c2900-universalk9-mz.SPA.151-3.T.bin | |
| CISCO2951/K9 version c2951-universalk9-mz.SPA.151-3.T.bin | |
| CISCO3945-SPE150/K9 version c3900-universalk9-mz.SPA.151-3.T.bin | |
| **PCI Sub-Requirements Passed** | |
| **PCI 1** | 1.2.1, 1.2.2, 1.2.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8 |
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 4** | 4.1 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.7.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10. 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1,10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3 |
| **PCI 11** | 11.4 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

## Primary PCI Function

The main function of the Cisco ISR is the segmentation of PCI scope and enforcement of that new scope boundary.

It has five primary functions/capabilities in relation to PCI.

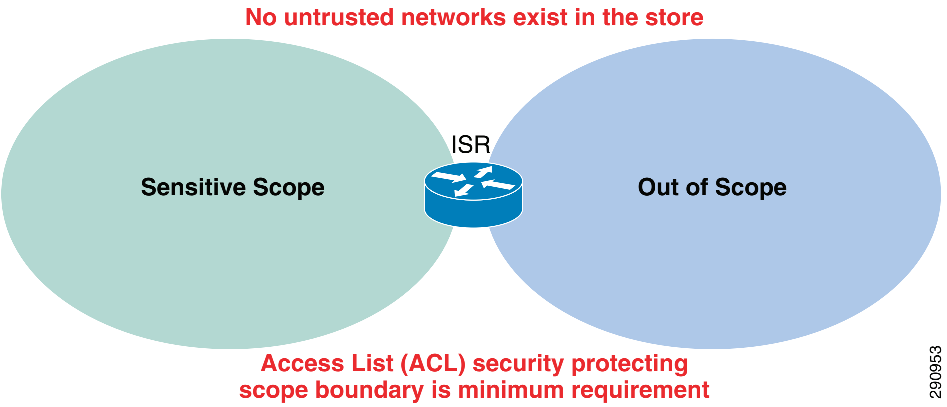
1. As a router, directing traffic between networks

   A router in its simplest form routes between networks. By segmenting a network into sub-networks, a retailer can isolate sensitive information from non-sensitive information. The Cisco ISR can segment and route sensitive traffic separately from non-sensitive traffic to reduce the overall scope of a company's cardholder data environment. Depending on risk vectors within the store, different levels of enforcement might be required at the segmented scope boundary level. (See items 2, 3 and 4 following.)

2. As a router with ACLs, restricting traffic between the cardholder data environment and other areas of the network

   A router with ACLs can be used to enforce segmented traffic only if the ACLs are used to filter and segment private networks of the retailer. They may not be used to filter untrusted networks. For example, many retailers have a central chokepoint in their data center that is the connection to the Internet (an untrusted network). As long as the retailer has only untrusted network connections outside of the store, (the data center, in this case), then a retailer may use router access lists to protect its scope from its own private internal networks. As soon as the store connects to untrusted networks directly, items 3 and 4 below become relevant. (See Figure 5-89.)

*Figure 5-89 ACLs Segment Traffic*


No untrusted networks exist in the store
ISR
Sensitive Scope
Out of Scope
Access List (ACL) security protecting scope boundary is minimum requirement
290953

3. As a stateful firewall, restricting traffic between the cardholder data environment and other areas of the network

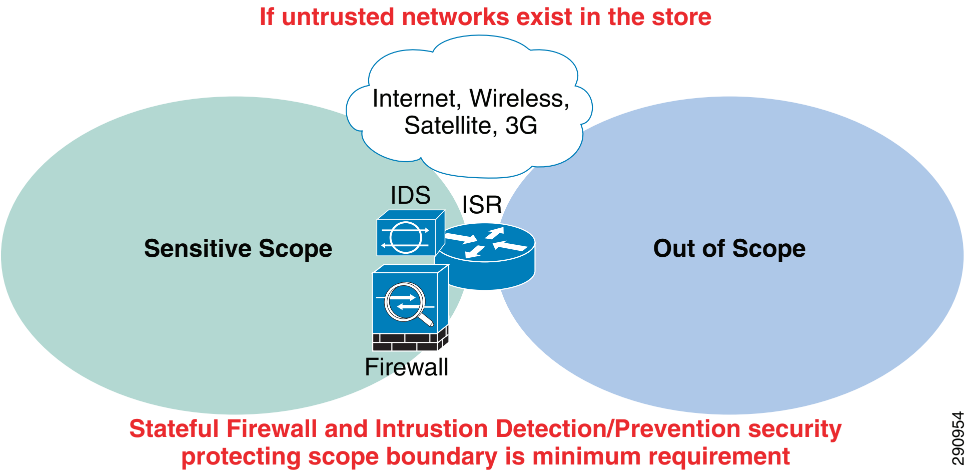
   As soon as any untrusted network is introduced at the store level, firewalling and IDS/IPS must be deployed. The following are examples of untrusted networks:

   - The Internet
   - Wireless
   - Satellite
   - 3G/4G cellular backup

4. As an intrusion prevention system, inspecting all traffic going to and from the cardholder data environment

   As soon as any untrusted network is introduced at the store level, firewalling and IDS/IPS must be deployed. (See Figure 5-90.)

*Figure 5-90 Using Firewall and IDS/IPS*


If untrusted networks exist in the store
Internet, Wireless, Satellite, 3G
IDS
ISR
Sensitive Scope
Out of Scope
Firewall
Stateful Firewall and Intrustion Detection/Prevention security protecting scope boundary is minimum requirement
290954

The Cisco ISR can be used to address segmentation challenges and enforce scope boundaries depending on the levels required by the retailer. Each of these features can be enabled by using a license key. This feature is particularly useful for retailers because it does not require a visit to every store to enable the firewall/IPS/IDS capability. If these capabilities are not used within the Cisco ISR, an external component(s) can be used to address this level of scope enforcement.

5. As a VPN system, encrypting all traffic going to and from the store across open and public networks.

   The Cisco ISR can be used to address the need to encrypt the transmission of cardholder data across open, public networks such as 3G/4G/Wi-fi, and satellite technologies using SSL and IPSec technologies.

Table 5-36 lists the component assessment details for the Cisco ISR.

*Table 5-37 Component Capability Assessment—Cisco ISR*

| Cisco ISR | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 1, 11 (1.2, 1.3, 11.4)** |
| Protect trusted networks from untrusted networks with ACLs or firewall/IDS/IPS. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

- The security features of the Cisco ISR routers in the store designs are configured using Cisco Security Manager. When adopting this as the primary method of router configuration, Cisco does not recommend making changes directly to the command-line interface (CLI) of the router. Unpredictable results can occur when central and local management are used concurrently.
- The general configuration of the Cisco ISR routers in the store architectures are maintained with EMC Ionix Network Configuration Manager.

- Firewall rule sets must adhere to a "least amount of access necessary" policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports required for the cardholder data environment (for example, point-of-sale) networks.
- Ensure that inspection rules and/or zones are enabled on the Cisco ISR router so that the firewall maintains state (none are enabled by default).
- Redundant Cisco IOS firewalls do not have the capability to maintain state between the routers. During a failure, client communication sessions need to be re-established through the alternate router. If high availability with statefulness is a requirement, Cisco ASA firewalls should be used.
- Access into a store router from the WAN needs to be protected by a store-located firewall filter if the WAN technology is considered untrusted/public (for example, Internet DSL or cable network, public 3G or 4G, satellite). In the Cisco Retail PCI Solution lab, a private MPLS WAN is simulated, and filtering of the store traffic occurs on the WAN link of all in-scope locations.
- Disable the HTTP server service on the router and enable the HTTP secure server.
- Disable use of Telnet and enable use of only SSH version 2.
- Configure the **session-timeout** and **exec-timeout** commands to 15 minutes or less on the console, VTY, and line interfaces on the router. Disable the AUX interface.
- Configure appropriate banner messages on login, incoming, and exec modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the router to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the router itself in the event of a WAN or Cisco Secure ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the router.
- Change default passwords and community strings to appropriate complexity.
- Configure logs to be sent to a centralized syslog server, such as RSA enVision.
- Configure NTP to ensure all logging is coordinated.
- Disable un-necessary services (for example, Bootp, Pad, ipv6).
- Shutdown unused interfaces.

Each of the store designs was implemented using guidance from the following:

- Cisco Enterprise Branch Security Design Guide—
http://www.cisco.com/en/US/docs/solutions/Enterprise/Branch/E_B_SDC1.html
- Branch/WAN Design Zone—
http://www.cisco.com/en/US/netsol/ns816/networking_solutions_design_guidances_list.html

Additional information for router hardening can be found at the following URLs:

- Cisco Guide to Harden Cisco IOS Devices—
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml
- Cisco IOS Security Configuration Guide, Release 12.4—
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html

### PCI Assessment Detail—PCI Sub-Requirements Satisfied

#### Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.1**—*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*

  Cisco zone-based firewalls are configurable to restrict traffic through the use of class map, policy map, and zone pair service policy statements and access lists.

- **PCI 1.2.2**—*Secure and synchronize router configuration files*

  Router configuration files are backed up centrally using EMC Ionix Network Configuration Manager (NCM). This tool also verifies that running and startup configurations of routers and switches are synchronized.

- **PCI 1.2.3**—*Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.*

  Cisco zone-based firewalls are configured with source and destination zones to control traffic passing from one zone to another. Each of these zone pairs receives a service policy, which is the mechanism that identifies permitted traffic, while all other traffic is dropped and logged.

```
zone-pair security CSM_S_POS-W-S_POS_1 source S_POS-W destination S_POS
 service-policy type inspect CSM_ZBF_POLICY_MAP_18
```

- **PCI 1.3.1**—*Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.*
- **PCI 1.3.2**—*Limit inbound Internet traffic to IP addresses within the DMZ.*
- **PCI 1.3.3**—*Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.*
- **PCI 1.3.4**—*Do not allow internal addresses to pass from the Internet into the DMZ.*

  Router WAN interfaces connected to public network connections such as the Internet should have filtering applied to prevent spoofing of both public and private IP address. Typical filters for private IP address blocks are as follows:

```
ip access-list extended COARSE-FILTER-INTERNET-IN
 remark -------------------------------------------------------
 remark ---Block Private Networks---
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark -
 remark ---Block Autoconfiguration Networks---
 deny   ip 169.254.0.0 0.0.255.255 any log
 remark -
 remark ---Block Loopback Networks---
 deny   ip 127.0.0.0 0.0.255.255 any log
 remark -
 remark ---Block Multicast Networks---
 deny   ip 224.0.0.0 15.255.255.255 any log
 remark -
 remark ---Block Your assigned IP's at edge---
 deny   ip <YOUR_CIDR_BLOCK> any log
 remark -
 remark ---Allow remaining public internet traffic---
 permit ip any any
```

- **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*

  Cisco zone-based firewalls are configured with source and destination zones to control traffic passing from one zone to another. Each of these zone pairs receives a service policy, which is the mechanism that identifies permitted traffic, while all other traffic is dropped and logged.

  ```
  zone-pair security CSM_S_POS-S_WAN_1 source S_POS destination S_WAN
   service-policy type inspect CSM_ZBF_POLICY_MAP_16
  ```

- **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*

  Cisco zone-based firewalls are configurable to perform stateful inspection by use of the *inspect* statement in the associated class map, policy map, and zone pair service policy statements.

  ```
  class-map type inspect match-all CSM_ZBF_CLASS_MAP_9
   match access-group name CSM_ZBF_CMAP_ACL_9
   match protocol tcp

  policy-map type inspect CSM_ZBF_POLICY_MAP_7
   class type inspect CSM_ZBF_CLASS_MAP_9
    inspect Inspect-1
   class type inspect CSM_ZBF_CLASS_MAP_10
    inspect Inspect-1
   class type inspect CSM_ZBF_CLASS_MAP_11
    inspect Inspect-1
   class class-default
    drop log

  zone-pair security CSM_S_WAN-S_POS_1 source S_WAN destination S_POS
   service-policy type inspect CSM_ZBF_POLICY_MAP_7
  ```

- **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*

  In the store design, VLANs are used to segment traffic based on function and security requirements. Each of these VLANs are assigned to an appropriate security zone using the zone-based firewall feature of the router.

  ```
  interface GigabitEthernet0/0.11
   description POS
   zone-member security S_POS
  interface GigabitEthernet0/0.13
   description VOICE
   zone-member security S_Voice
  ```

- **PCI 1.3.8**—*Do not disclose private IP addresses and routing information to unauthorized parties.*

#### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco routers can be configured to use secure protocols for all system functions. This includes SSH and HTTPS for remote management, IPsec VPN for remote connectivity, and SCP for file transfers. Insecure services can be disabled or blocked using configuration statements and access lists.

```
no ip http server
ip http secure-server
snmp-server user remoteuser remoteuser v3
line vty 0 4
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 transport preferred none
 transport input ssh
 transport output none
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco routers have several services that are enabled by default that need to be disabled:

```
no service pad
no service udp-small-servers
no service tcp-small-servers
no ip bootp server
no mop enable
no service finger
no ip forward-protocol nd
no ip http server
```

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco routers support administrative protocols with strong cryptography such as SSH version 2 and HTTPS with 3DES.

**Note** Strong cryptography—Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible). Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher). See NIST Special Publication 800-57 (www.csrc.nist.gov/publications/) for more information.

```
! Before Crypto keys can be generated hostname and domain name must be entered

hostname R-A2-Small-1
ip domain name cisco-irn.com

! Generate keys with 1024 or larger bit key generation NOT the default 512

Crypto key generate rsa

ip ssh version 2

ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
```

### Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

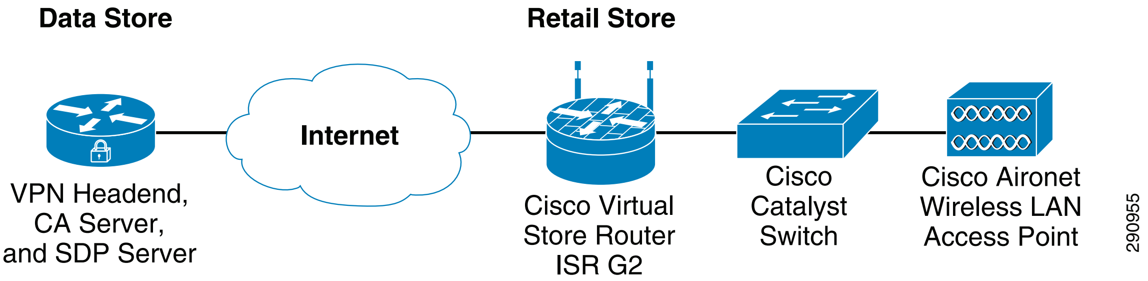
- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*
  - *The Internet*
  - *Wireless technologies,*
  - *Global System for Mobile communications (GSM)*
  - *General Packet Radio Service (GPRS)*

  Public WAN link connections include technologies such as DSL, cable, satellite, Wi-Fi, and 3G/4G networks. These are considered untrusted public networks within PCI. A VPN is required to securely tunnel traffic between the store and the enterprise network.

  Cisco Virtual Office provides reference designs for building a VPN solution to connect stores to data centers using these technologies. For more information about Cisco VPN solutions, see: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6808/prod_white_paper0900aecd8051bf3b_ns855_Networking_Solutions_White_Paper.html

  The following example describes equipment located at the store and the data center headend router. The store router is referred to as the spoke router, and the data center router as the hub. Figure 5-91 shows a simplified Cisco VPN topology.

*Figure 5-91 Cisco VPN Topology*



Cisco VPN technology connects the stores to the data center over the Internet. As a result, a secure, encrypted tunnel is used to secure sensitive information such as cardholder data. Cisco VPN technologies offer a choice to protect the data in transit and provide a secure access to the stores' networks, including Easy VPN and Dynamic Multipoint VPN (DMVPN).

This example shows DMVPN as the VPN technology. DMVPN uses IPSec-encrypted GRE tunnels, with dynamic routing. Two simultaneously active DMVPN tunnels are built from each store to different hub routers, providing instant failover. If the primary tunnel fails, routing converges to use the secondary tunnel, and all sessions are kept alive. In addition, with DMVPN, store routers can dynamically build spoke-to-spoke tunnels between each other to exchange data, without having to tunnel the traffic back to the hub, thus alleviating the load on the headend.

Following are sample DMVPN spoke and hub configurations. Enhanced Interior Gateway Routing Protocol (EIGRP) is used as the routing protocol inside the DMVPN network. Split-tunneling is used and only traffic on the POS and employee VLANs going to the servers on the 10.0.0.0 network at the headquarters is sent through the DMVPN tunnel, while any other traffic is sent straight to the Internet. Note that, if split-tunneling is not required, a default route (to 0.0.0.0) can be advertised from the hubs to the spokes, instead of specific subnets.

### 891 Store Router

```
!! Configure the IP addresses on the VLAN interfaces
interface vlan 10
  description POS VLAN
  ip address 172.16.10.1 255.255.255.0
  no autostate
interface vlan 20
  description employee VLAN
  ip address 172.16.20.1 255.255.255.0
  no autostate
interface vlan 30
  description guest VLAN
  ip address 172.16.30.1 255.255.255.0
  no autostate
!! Configure the ISAKMP and IPSec policies
crypto isakmp policy 1
  encryption aes 256

crypto isakmp keepalive 35 5
crypto isakmp nat keepalive 10
crypto ipsec transform-set t1 esp-aes 256 esp-sha-hmac
 mode transport

crypto ipsec profile cvs
 set transform-set t1
ip multicast-routing
!! Configure the DMVPN tunnel
interface Tunnel0
  bandwidth 1000
  ip address 192.168.1.3 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip hello-interval eigrp 99 30
  ip hold-time eigrp 99 90
  ip pim sparse-dense-mode
  ip nhrp map multicast <Primary-hub-public-IP>
  ip nhrp map 192.168.1.1 <Primary-hub-public-IP>
  ip nhrp nhs 192.168.1.1
  ip nhrp map multicast <Secondary-hub-public-IP>
  ip nhrp map 192.168.1.2 <Secondary-hub-public-IP>
  ip nhrp nhs 192.168.1.2
  ip nhrp authentication <password>
  ip nhrp network-id 12345
  ip nhrp holdtime 300
  ip nhrp registration no-unique
  ip nhrp shortcut
  ip nhrp redirect
  ip tcp adjust-mss 1360
  load-interval 30
  delay 1000
  qos pre-classify
  tunnel source GigabitEthernet0
  tunnel mode gre multipoint
  tunnel key 12345
  tunnel protection ipsec profile cvs


!! Configure the DMVPN routing protocol. Only permit the POS and employee LAN !!
subnets to be advertised to the hubs
ip access-list standard dmvpn_acl
  permit 172.16.10.0 0.0.0.255
  permit 172.16.20.0 0.0.0.255
```

```
router eigrp 99
  no auto-summary
  network 192.168.1.3 0.0.0.0
  network 172.16.10.1 0.0.0.0
  network 172.16.20.1 0.0.0.0
  distribute-list dmvpn_acl out
```

### 3945E Hub Router:

```
!! Configure the ISAKMP and IPSec policies

crypto isakmp policy 1
  encryption aes 256

crypto isakmp keepalive 35 5
crypto isakmp nat keepalive 10

crypto ipsec transform-set t1 esp-aes 256 esp-sha-hmac
  mode transport require

crypto ipsec profile cvs
  set transform-set t1

!! Enable multicast routing

ip multicast-routing

!! Configure the DMVPN tunnel. Use the same bandwidth metric for both primary !! and
secondary hubs, but a lower delay metric on the primary hub

interface Tunnel0

  bandwidth 2000
  ip address 192.168.1.1 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip pim sparse-dense-mode
  ip nhrp authentication <password>
  ip nhrp map multicast dynamic
  ip nhrp network-id 12345
  ip nhrp redirect
  ip tcp adjust-mss 1360
  no ip split-horizon eigrp 99
  delay 1000
  qos pre-classify
  tunnel source <Outside_Interface >
  tunnel mode gre multipoint
  tunnel key 12345
  tunnel protection ipsec profile cvs

!! Configure the DMVPN routing protocol. Only the 10.0.0.0 network is        !!
advertised to the spokes in this example (split-tunneling)

router eigrp 99
  no auto-summary
  network 192.168.1.1 0.0.0.0
  redistribute static route-map split_in
ip access-list standard split_in
  permit 10.0.0.0

route-map split_in permit 10
  match ip address split_in
```

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Integrated Services Routers. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco routers are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default in Cisco routers, no users are allowed access unless specifically configured and assigned appropriate passwords.

```
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa session-id common
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
```

Local user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration, as specified in PCI requirement 8.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

These AAA authentication groups are assigned to the administrative interfaces where users connect:

```
ip http authentication aaa login-authentication RETAIL

line con 0
 login authentication RETAIL

line vty 0 4
 login authentication RETAIL

line vty 5 15
 login authentication RETAIL
```

Services provide on-going access to software updates and security patches for a variety of Cisco products.

#### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

The router is able to meet some of the requirements locally, as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco routers support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco routers require setting of a password.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  In addition to the use of service password encryption to encrypt line interface passwords, the routers also support the use of AES encryption of pre-shared keys.

```
service password-encryption
password encryption aes
```

Use the **username secret** command to configure a username and MD5-encrypted user password when creating local fall back user accounts.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco routers do not support an automated capability to perform this function at this time; the user account would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco routers do not support an automated capability to perform this function at this time, user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco routers support the ability to specify a minimum password length for local accounts.

  ```
  security passwords min-length 7
  ```
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco routers do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco routers do not support an automated capability to perform this function at this time: user account creation would have to follow this policy manually.
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco routers support the local ability to block logins after a specified number of failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco routers support the local ability to block logins after a specified time after failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco router management interfaces are configured as follows to meet this requirement:

  ```
  ip http timeout-policy idle 900

  line con 0
  ```

```
 session-timeout 15 output
 exec-timeout 15 0
line vty 0 4
 session-timeout 15  output
 exec-timeout 15 0
line vty 5 15
 session-timeout 15  output
 exec-timeout 15 0
```

**Note** If only the **session timeout** command is specified, the session timeout interval is based solely on detected input from the user. If the **session timeout** command is specified with the **output** keyword, the interval is based on both input and output traffic. You can specify a session timeout on each port. The **session-timeout** command behaves slightly differently on virtual (vty) terminals than on physical console, auxiliary (aux), and terminal (tty) lines. When a timeout occurs on a vty, the user session returns to the EXEC prompt. When a timeout occurs on physical lines, the user session is logged out and the line returned to the idle state. You can use a combination of the **exec-timeout** and **session-timeout** line configuration commands, set to approximately the same values, to get the same behavior from virtual lines that the **session-timeout** command causes on physical lines.

#### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

The Cisco ISRs are able to track and monitor all administrative user access and events such as port up/down, as well as device authentication events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco routers track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging trap debugging
logging 192.168.42.124
logging buffered 50000

login on-failure log
login on-success log


archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
```

The Cisco ISR uses Network Time Protocol (NTP) to update and synchronize their local clock facilities and meet sub-requirements 10.4.1 through 10.4.3:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco routers use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162

clock timezone PST -8 0
clock summer-time PDT recurring

service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

  To learn more about NTP, visit the following URL:
  http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Requirement 10.5 was met using RSA enVision, a central logging repository that collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

### Requirement 11: Regularly Test Security Systems and Processes

- **PCI 11.4**—*Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.*

Cisco routers are capable of performing intrusion detection. Each of the store reference designs includes untrusted networks (either a public Internet connection or wireless networks); therefore, intrusion detection capabilities are required. IPS signature updates and configurations are managed centrally through Cisco Security Manager, which implements the following configuration statements to enable the IPS inspection capability in the routers:

```
ip ips config location flash0: retries 1 timeout 1
ip ips notify SDEE
ip ips name Store-IPS
!
ip ips signature-category
  category all
   retired true
  category ios_ips default
   retired false
!
interface GigabitEthernet0/0
 description WAN
 ip ips Store-IPS in
 ip ips Store-IPS out
interface GigabitEthernet0/1.11
 description POS
 ip ips Store-IPS in
 ip ips Store-IPS out
interface GigabitEthernet0/1.15
 description WIRELESS-POS
 ip ips Store-IPS in
 ip ips Store-IPS out
```

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

## Routers—Data Center

The primary function of data center routers from a PCI perspective is routing between sensitive networks and out-of scope networks. Data center routers function as WAN aggregation routers or connecting to larger networks such as the Internet. Therefore, performance and scalability are equally important as securely passing data. For this reason, and unlike the routers in the store, security functions are typically separated physically into distinct appliances. The Cisco 7206VXR and the the Cisco ASR1002 routers were used for the Internet edge and store WAN edge portions of the network within the solution testing.

### Primary PCI Function

The main function of the data center routers is the segmentation of PCI scope and enforcement of that new scope boundary. The data center router has four primary functions/capabilities in relation to PCI:

1. As a router, directing traffic between networks

   A router in its simplest form routes between networks. By segmenting a network into sub-networks, a retailer can isolate sensitive information from non-sensitive information. Data center routers can segment and route sensitive traffic separately from non-sensitive traffic to reduce the overall scope of a company's cardholder data environment. Depending on risk vectors, different levels of enforcement might be required at the segmented scope boundary level. (See items 2, 3, and 4 following.)

2. As a router with ACLs, restricting traffic between the cardholder data environment and other areas of the network

   A router with ACLs can be used to enforce segmented traffic only if the ACLs are used to filter and segment private networks of the retailer. They may not be used to filter untrusted networks. For example, if a data center router is used to segment sensitive PCI networks from internal inventory networks, a retailer may use router access lists to protect its scope. As soon as the store connects to untrusted networks directly, items 3 and 4 below become relevant.

3. As a stateful firewall, restricting traffic between the cardholder data environment and other areas of the network

   As soon as any untrusted network is introduced to the connections of the data center router, firewalling and IDS/IPS must be deployed. The following are examples of untrusted networks:

   - Internet
   - Wireless
   - Satellite
   - Cellular backup

4. As an intrusion prevention system, inspecting all traffic going to and from the cardholder data environment

   As soon as any untrusted network is introduced to the connections of the data center router, firewalling and IDS/IPS must be deployed at that location.

*Table 5-38 PCI Assessment Summary—Data Center Routers*

| Models Assessed | |
|---|---|
| CISCO7206VXR-NPE-G1 version c7200-advipservicesk9-mz.124-24.T4.bin,<br>ASR-1002 (RP1) version asr1000rp1-adventerprisek9.03.02.01.S.151-1.S1.bin | |
| **PCI Sub-Requirements Passed** | |
| **PCI 1** | 1.2.2, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8 |
| **PCI 2** | 2.2, 2.2.2, 2.2.3, 2.2.4, 2.3 |
| **PCI 4** | 4.1 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

## Primary PCI Function

The data center routers protect trusted networks from untrusted networks with ACLs or firewall/IDS/IOS. (1.2, 1.3, 11.4)

Table 5-38 lists the component assessment details for the Cisco data center routers.

***Table 5-39 Component Capability Assessment—Data Center Routers***

| Data Center Routers | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 1, 11 (1.2, 1.3, 11.4)** |
| Protect trusted networks from untrusted networks with ACLs or firewall/IDS IOS. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

- Configuration was done manually on the router CLI, and backup of configuration and monitoring of configuration for changes and non-compliance were done through the EMC Ionix Network Configuration Manager (alternatively, CiscoWorks Resource Manager Essentials, a component of Cisco LMS, can be used as well).
- The perimeter firewalling of the data center was provided by the Cisco ASA. As a result, the Cisco 7206VXR and the Cisco ASR1002 were not evaluated according to the set of 1.x requirements for firewalls.
- Disable the HTTP server service on the router and enable the HTTP secure server.
- Configure the **session-timeout** and **exec-timeout** commands to 15 minutes or less on the console, VTY, and line interfaces on the router. Disable the AUX interface.

- Configure appropriate banner messages on login, incoming, and exec modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the router to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the router itself in the event of a WAN or Cisco Secure ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the router.
- Enable anti-spoofing on all interfaces.
- Routers in the data center were implemented using guidance from the following:
  - Enterprise Data Center Design guide based on a Data Center 3.0 Architecture—
http://www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html
  - Enterprise Internet Edge Design Guide—
http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/IE_DG.html
- For the Internet edge routers, use the access list below on the interface that is facing the Internet. This access list explicitly filters traffic destined for the infrastructure address space. Deployment of edge infrastructure access lists requires that you clearly define your infrastructure space and the required/authorized protocols that access this space. The access list is applied at the ingress to your network on all externally facing connections, such as peering connections, customer connections, and so forth.

```
!
ip access-list extended COARSE-FILTER-INTERNET-IN
 remark --------------------------------------
 remark ---Block Private Networks---
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark -
 remark ---Block Autoconfiguration Networks---
 deny   ip 169.254.0.0 0.0.255.255 any log
 remark -
 remark ---Block Loopback Networks---
 deny   ip 127.0.0.0 0.0.255.255 any log
 remark -
 remark ---Block Multicast Networks---
 deny   ip 224.0.0.0 15.255.255.255 any log
 remark -
 remark ---Block Your assigned IP's at edge---
 deny   ip <YOUR_CIDR_BLOCK> any log
 remark -
 remark ---Allow remaining public internet traffic---
 permit ip any any
!
```

**Note** The **log** keyword can be used to provide additional details about source and destinations for a given protocol. Although this keyword provides valuable insight into the details of access list hits, excessive hits to an access list entry that uses the **log** keyword increase CPU utilization. The performance impact associated with logging varies by platform.

The service provider network in the solution represented an Multiprotocol Label Switching (MPLS) network. At the writing of this document, MPLS is considered a private network, and secure tunneling across the WAN is not required. MPLS implementations may be public or private with regards to PCI, depending on how the service provider implements the MPLS network and whether the provider has satisfactorily completed their annual PCI audit. For best practices when in doubt, Cisco recommends VPN tunneling be implemented. For further information on implementing an IPSec VPN, see the *IPSec VPN Direct Encapsulation Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/Dir_Encap.html

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

  Router configuration files are backed up centrally using EMC Ionix Network Configuration Manager (NCM). This tool also verifies that running and startup configurations of routers and switches are synchronized.

- **PCI 1.3.2**—*Limit inbound Internet traffic to IP addresses within the DMZ.*
- **PCI 1.3.3**—*Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.*
- **PCI 1.3.4**—*Do not allow internal addresses to pass from the Internet into the DMZ.*
- **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*
- **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*
- **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*

  **PCI 1.3.8**—*Do not disclose private IP addresses and routing information to unauthorized parties.*

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco routers can be configured to use secure protocols for all system functions. This includes SSH and HTTPS for remote management, IPsec VPN for remote connectivity, and SCP for file transfers. Insecure services can be disabled or blocked using configuration statements and access lists:

```
no ip http server
ip http secure-server
ip scp server enable
snmp-server user remoteuser remoteuser v3
line vty 0 4
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 transport preferred none
 transport input ssh
 transport output none
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco routers have several services that are enabled by default that can be disabled:

  ```
  no service pad
  no service udp-small-servers
  no service tcp-small-servers
  no ip bootp server
  no mop enable
  no service finger
  no ip forward-protocol nd
  no ip http server
  ```

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco routers support administrative protocols with strong cryptography such as SSH version 2 and HTTPS with 3DES.

**Note** Strong cryptography is based on industry-tested and accepted algorithms, along with strong key lengths and proper key management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible). Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher). See NIST Special Publication 800-57 (www.csrc.nist.gov/publications/) for more information.

```
! Before Crypto keys can be generated hostname and domain name must be entered

hostname RWAN-1
ip domain name cisco-irn.com

! Generate keys with 1024 or larger bit key generation NOT the default 512

Crypto key generate rsa

ip ssh version 2

ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
```

### Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*
  - *The Internet*
  - *Wireless technologies,*
  - *Global System for Mobile communications (GSM)*
  - *General Packet Radio Service (GPRS)*

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco routers. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco routers are configured to use a AAA model for user-based access. Users can be assigned to groups, and based on privilege levels, have access to only the information they require for their job function. By default in Cisco routers, no users are allowed access unless specifically configured and assigned appropriate passwords.

```
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa session-id common
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
```

Local user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI requirement 8.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

The following AAA authentication groups are assigned to the administrative interfaces where users connect:

```
ip http authentication aaa login-authentication RETAIL

line con 0
 login authentication RETAIL

line vty 0 4
 login authentication RETAIL

line vty 5 15
 login authentication RETAIL
```

### Requirement 8: Assign a Unique ID to Each Person with Computer Access

For Cisco routers to meet all of the user access restrictions specified in Requirement 8, an external authentication service such as Cisco Secure ACS must be implemented. Configure AAA services as shown above in Requirement 7.

The router is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco routers support the creation of local user accounts with unique ID's through the use of the **username** command. These can be used for local fallback user accounts.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco routers require the setting of a password.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  In addition to the use of service password encryption to encrypt line interface passwords, the routers also support the use of AES encryption of pre-shared keys.

  ```
  service password-encryption
  ```

```
password encryption aes
```

Use the **username secret** command to configure a username and MD5-encrypted user password when creating local fallback user accounts.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco routers do not support an automated capability to perform this function at this time; the user account would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco routers do not support an automated capability to perform this function at this time, user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco routers support the ability to specify a minimum password length for local accounts.

  ```
  security passwords min-length 7
  ```

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco routers do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco routers do not support an automated capability to perform this function at this time: user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco routers support the local ability to block logins after a specified number of failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco routers support the local ability to block logins after a specified time after failed login attempts with the following command:

```
login block-for 1800 attempts 6 within 65535
```

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco router management interfaces are configured as follows to meet this requirement:

```
ip http timeout-policy idle 900

line con 0
 session-timeout 15 output
```

```
 exec-timeout 15 0
line vty 0 4
 session-timeout 15  output
 exec-timeout 15 0
line vty 5 15
 session-timeout 15  output
 exec-timeout 15 0
```

**Note** If only the **session timeout** command is specified, the session timeout interval is based solely on detected input from the user.

If the **session timeout** command is specified with the **output** keyword, the interval is based on both input and output traffic.You can specify a session timeout on each port.

The **session-timeout** command behaves slightly differently on virtual (vty) terminals than on physical console, auxiliary (aux), and terminal (tty) lines. When a timeout occurs on a vty, the user session returns to the EXEC prompt. When a timeout occurs on physical lines, the user session is logged out and the line returned to the idle state.

You can use a combination of the **exec-timeout** and **session-timeout** line configuration commands, set to approximately the same values, to get the same behavior from virtual lines that the **session-timeout** command causes on physical lines.

#### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco routers are able to track and monitor all administrative user access and events such as port up/down, as well as device authentication events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco routers track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging trap debugging
logging 192.168.42.124
logging buffered 50000

login on-failure log
login on-success log


archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
```

Cisco routers use NTP to update and synchronize their local clock facilities and meet sub-requirements 10.4 through 10.4.3.

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP server was hosted at the data center site. Cisco routers use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162

clock timezone PST -8 0
clock summer-time PDT recurring

service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

To learn more about NTP, visit:
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

**Note** The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

# Switching

## Switches—Store

Cisco store switches provide connectivity for wired endpoints and the ability to segment them onto their own sensitive scope networks. Virtual local area networks (VLANs) are used to put sensitive PCI applications and devices onto their own network and segregate them from devices that are on non-sensitive networks.

Store switches are broken into three categories to provide scale and feature relevance;

- Compact switches—Quiet, small form factor switches that can be used on store floors to extend the capability of the network to the register. These switches use power over Ethernet (PoE) pass-through, reducing expensive power and network cabling costs to new devices at the area of sale.
- Access switches—Stackable, expandable switches that can be used for wired device port density in the store wiring closets. Access switches offer a variety of modular and fixed configuration options, and feature operational efficiency with StackPower, FlexStack, and NetFlow to increase visibility and control.
- Core/distribution—Highly redundant, powerful core switches allow for the most demanding business requirements of the store. Modular functionality provides the ability to insert security technology as the needs of the business expand into new areas.

*Table 5-40 PCI Assessment Summary—Store Switches*

| **Models Assessed** | |
|---|---|
| WS-C3560E-PS-24c3560e-universalk9-mz.122-35.SE5.bin<br>WS-C2960PD-8TT-Lc2960-lanbasek9-mz.122-55.SE1.bin<br>WS-C2960G-8TC-Lc2960-lanbasek9-mz.122-50.SE4.bin<br>WS-C2960-8TC-Lc2960-lanbasek9-mz.122-50.SE4.bin<br>WS-C2960S-48FPS-Lc2960s-universalk9-mz.122-53.SE1.bin<br>WS-C3750X-48PF-Sc3750e-universalk9-mz.122-53.SE2.bin<br>WS-C2960CPD-8PT-Lc2960c405-universalk9-mz.122-55.0.43.SK.bin<br>WS-4507+R SUP-7cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin<br>WS-C3560X-48PF-Sc3560e-universalk9-mz.122-53.SE2.bin<br>WS-C3560CPD-8PT-Lc3560c405ex-universalk9-mz.122-55.0.44.SK.bin | |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |

*Table 5-40 PCI Assessment Summary—Store Switches (continued)*

| | |
|---|---|
| **PCI 10** | 10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3 |
| **PCI 11** | 11.1.b, 11.1.d |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

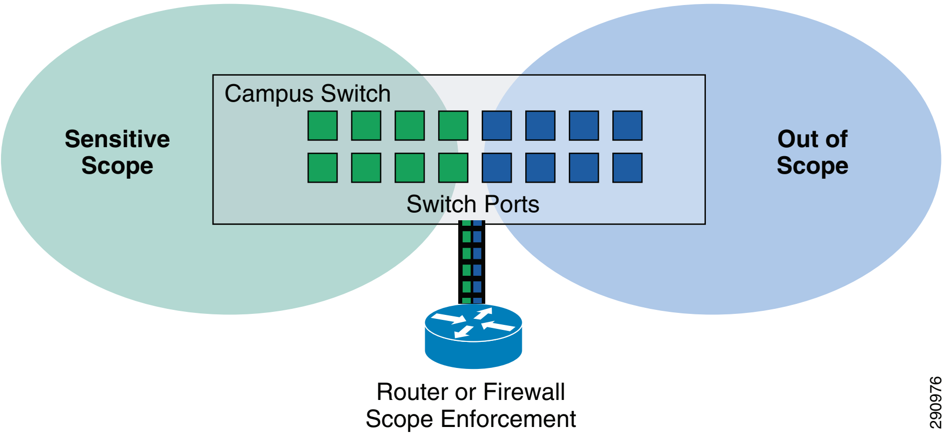
## Primary PCI Function

The primary PCI compliance feature of store switches is to provide secure wired port access. (9.1.2, 11.1)

Store switches also provide PCI compliance via segmentation of sensitive networks from out-of-scope networks. Although technically a firewall or ACL is used to enforce PCI Requirement 1, switches extend that Layer 3 boundary to Layer 2. Using VLANs, Cisco store switches allow retailers to put their payment networks into separate VLANs (scopes) from other non-sensitive data (out-of-scope).

Figure 5-92 shows an example of switch segmentation.

*Figure 5-92 Cisco Store Switch Segmentation*



Although the enforcement of these boundaries would be handled by either a router or firewall, the switch provides the port density and access required to connect the payment devices from the store floor.

Table 5-40 lists the component assessment details for the Cisco store switches.

*Table 5-41 Component Capability Assessment—Store Switches*

| Store Switches | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 9, 11 (9.1.2, 11.1.b)** |
| Provide secure access to payment devices in the stores. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

- The configurations of the Cisco Catalyst switches in the store architectures are maintained within EMC Ionix Network Configuration Manager (alternatively CiscoWorks Resource Manager Essentials, a component of C-LMS, can be used as well).
- The use of VLANs on the Cisco Catalyst switch enables the retailer to provide same-box wired access to its devices while maintaining segregated addressing schemes.
- Disable the HTTP server on the switch and enable the HTTP secure server.
- Using the stacking capability of Cisco Catalyst switches improves high availability designs while simplifying configuration and support.
- Cisco SmartPorts simplifies connecting the right device to the right VLAN.
- Network Admission Control (NAC) protects the network from rogue devices being connected.
- Cisco compact switches can easily add more securely managed ports where needed (for example, Cash Wrap and customer service desk), and some models can use PoE.
- Set the **session** and **exec timeout** commands to 15 minutes or less.

- Configure appropriate banner messages on login, incoming, and exec modes of the switch. The login banner warning should not reveal the identity of the company that owns or manages the switch. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the switch to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the switch itself in the event of a WAN or Cisco Secure ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the switch.

### PCI Assessment Detail—PCI Sub-Requirements Satisfied

#### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco switches can be configured to use secure protocols for all system functions. This includes SSH and HTTPS for remote management and SCP for file transfers. Insecure services can be disabled or blocked using configuration statements and access lists.

```
no ip http server
ip http secure-server
ip scp server enable
snmp-server user remoteuser remoteuser v3
line vty 0 4
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 transport preferred none
 transport input ssh
 transport output none
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco switches may have several services that are enabled by default that can be disabled.

```
no service pad
no service udp-small-servers
no service tcp-small-servers
no service finger
no ip http server
```

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco switches support administrative protocols with strong cryptography such as SSH version 2 and HTTPS with 3DES.

**Note** Strong cryptography—Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible). Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher). See NIST Special Publication 800-57 (www.csrc.nist.gov/publications/) for more information.

```
! Before Crypto keys can be generated hostname and domain name must be entered

hostname S-A2-Small-1
ip domain name cisco-irn.com

! Generate keys with 1024 or larger bit key generation NOT the default 512

Crypto key generate rsa

ip ssh version 2

ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
```

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco switches. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

To meet all of the requirements listed below, the PCI solution for retail uses the centralized user database in Active Directory, which is linked to via LDAP, RADIUS, and TACACS+ services. This server is located in the data center. Individual user IDs are assigned, and roles are based on group membership. This resource is used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco switches are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default in Cisco switches, no users are allowed access unless specifically configured and assigned appropriate passwords. The following configuration statements create an authentication group called *RETAIL*, which is assigned to various interfaces. This group uses the TACACS+ protocol to communicate with the Cisco ACS server where individual user groups and roles are configured, limiting and logging access as appropriate.

```
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa session-id common
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
```

  Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

  These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
ip http authentication aaa login-authentication RETAIL

line con 0
 login authentication RETAIL

line vty 0 4
 login authentication RETAIL

line vty 5 15
 login authentication RETAIL
```

#### Requirement 8: Assign a Unique ID to Each Person with Computer Access

For Cisco switches to meet all of the user access restrictions specified in Requirement 8, an external authentication service such as Cisco Secure ACS must be implemented. Configure AAA services as shown above in Requirement 7.

The switch is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

Cisco switches support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco switches require the setting of a password.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  In addition to the use of service password encryption to encrypt line interface passwords, the switches also support the use of AES encryption of pre-shared keys.

```
service password-encryption
password encryption aes
```

  Use the **username secret** command to configure a username and MD5-encrypted user password when creating local fallback user accounts.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco switches do not support an automated capability to perform this function at this time; the user account would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco switches do not support an automated capability to perform this function at this time; user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco switches do not support the ability to specify a minimum password length for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco switches do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco switches do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco switches support the local ability to block logins after a specified number of failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco switches support the local ability to block logins after a specified time after failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco switch management interfaces are configured as follows to meet this requirement:

  ```
  ip http timeout-policy idle 900

  line con 0
   session-timeout 15 output
   exec-timeout 15 0
  line vty 0 4
   session-timeout 15  output
   exec-timeout 15 0
  line vty 5 15
   session-timeout 15  output
   exec-timeout 15 0
  ```

**Note** If only the **session timeout** command is specified, the session timeout interval is based solely on detected input from the user. If the **session timeout** command is specified with the **output** keyword, the interval is based on both input and output traffic. You can specify a session timeout on each port. The **session-timeout** command behaves slightly differently on virtual (vty) terminals than on physical console, auxiliary (aux), and terminal (tty) lines. When a timeout occurs on a vty, the user session returns to the EXEC prompt. When a timeout occurs on physical lines, the user session is logged out and the line returned to the idle state. You can use a combination of the **exec-timeout** and **session-timeout** line configuration commands, set to approximately the same values, to get the same behavior from virtual lines that the **session-timeout** command causes on physical lines.

### Requirement 9: Restrict Physical Access to Cardholder Data

- **PCI 9.1.2**—*Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.*

  In addition to disabling switch port interfaces for ports that are not in use, or in public areas, ports can also be placed in the guest network VLAN. This VLAN is treated as a public network and requires the appropriate PCI requirements for public networks to be met as well (for example, IPS/IDS and stateful firewall). Cisco switches support a feature called SmartPorts, whereby devices connected to these ports can be dynamically moved to an appropriate network VLAN from a blackhole VLAN or guest VLAN based on automatic identification macros. This allows ports to be active for periodic use when devices are attached (for example, media players for in-aisle promotions, and IP phones for customer service) when these network ports are in publicly accessible areas. The following configurations show how to enable SmartPorts for a variety of default or custom devices based on MAC addresses as opposed to 802.1x authentication methods.

```
!
macro global description cisco-desktop
!
macro auto execute CISCO_LAST_RESORT_EVENT builtin CISCO_AP_AUTO_SMARTPORT
ACCESS_VLAN=17
macro auto execute Retail-POS builtin CISCO_PHONE_AUTO_SMARTPORT ACCESS_VLAN=11
VOICE_VLAN=13
macro auto execute POS-Systems remote scp://SMARTPORT@192.168.42.122/POS-Systems.txt
ACCESS_VLAN=11 VOICE_VLAN=13
!
macro auto mac-address-group Retail-POS
 oui list 001C26
 oui list 001C25
 mac-address list 0021.5C02.1DEF
 mac-address list 001C.25BE.99C2
macro auto device media-player ACCESS_VLAN=12
macro auto device ip-camera ACCESS_VLAN=20
macro auto device phone ACCESS_VLAN=17 VOICE_VLAN=13
macro auto device access-point ACCESS_VLAN=18
macro auto device lightweight-ap ACCESS_VLAN=18
!
macro auto global processing fallback cdp
!
interface GigabitEthernet0/9
 macro description CISCO_SWITCH_EVENT
```

More information about Cisco SmartPorts can be found at the following URL: http://www.cisco.com/en/US/docs/switches/lan/auto_smartports/12.2_55_se/configuration/guide/asp_cg.html

### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco switches are able to track and monitor all administrative user access, events such as port up/down, as well as device authentication events when using 802.1x.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*

  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

  Cisco switches track individual administrator actions as identified in the requirement above (10.1, 10.2, and 10.3) through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging trap debugging
logging 192.168.42.124
logging buffered 50000

login on-failure log
login on-success log


archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
```

Cisco switches use NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP server was hosted at the data center site. Cisco switches use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162

clock timezone PST -8 0
clock summer-time PDT recurring

service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

  To learn more about NTP, visit:
  http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

**Note** The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

To meet all of the requirements listed below, the PCI solution for retail uses a central logging repository located in the data center. RSA enVision collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

#### Requirement 11: Regularly Test Security Systems and Processes

The following requirements can be addressed using Cisco Network Admission Control.

- **PCI 11.1.b**—*Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:*
  - *WLAN cards inserted into system components*
  - *Portable wireless devices connected to system components (for example, by USB, etc.)*
  - *Wireless devices attached to a network port or network device*
- **PCI 11.1.d**—*If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel.*

  Cisco NAC capabilities can be configured on the store switches to automate the verification of approved devices being attached to the network. In addition to configuring the NAC authentication services in the data center, add the following configurations to the switch and switch interface ports where NAC is to be used (for example, publicly accessible ports):

```
Pre-requirements for NAC (domain name, name server, time settings, crypto keys):
 ip domain-name cisco-irn.com
 ip name-server 192.168.42.130
 Crypto key generate rsa 1024
 ntp server 192.168.62.161 prefer
 ntp server 192.168.62.162
 clock timezone PST -8
 clock summer-time PDT recurring
!
! ----Configurations to add for NAC ----
!
aaa new-model
!
!
aaa authentication dot1x default group radius local
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
 client 192.168.42.111
 server-key 7 <removed>
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 5 tries 3
radius-server host 192.168.42.111 auth-port 1812 acct-port 1813 key 7 <removed>
radius-server vsa send accounting
radius-server vsa send authentication
!
authentication mac-move permit
!
!
ip device tracking
ip admission name ise proxy http inactivity-time 60
!
cts sxp enable
cts sxp default source-ip 10.10.111.13 {use Switch Management IP}
!
dot1x system-auth-control
!
fallback profile ise
 ip access-group ACL-DEFAULT in
 ip admission ise
!
! ----Auto Smart Ports Macro method for port configurations-------
!
macro name dot1x
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 13
 ip arp inspection limit rate 1000
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab webauth
 authentication priority dot1x mab
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 authentication fallback ise
 mab
 snmp trap mac-notification change added
 dot1x pae authenticator
 dot1x timeout tx-period 5
```

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

## Cisco Catalyst Switches—Data Center

The Cisco Catalyst family of data center switches securely switches data; from servers to high speed trunks, maintaining the integrity of segmented scopes of compliance. They provide scalable inter-switch connectivity, high port density for wired endpoints, and the ability to segment them into sensitive scope networks. VLANs are used to put sensitive PCI applications and devices onto their own network and segregate them from devices that are on non-sensitive networks. Data center Cisco Catalyst switches are highly redundant, capable of delivering high performance switching, with feature options depending on the needs of the business.

Modular functionality provides the ability to insert security technology to enforce compliance needs.

- Security services include access control, firewall, and intrusion prevention.
- Wireless services can be aggregated into these switches for central policy control of unified wireless access points.
- Application services include quality of service (QoS), content filtering, and load balancing.

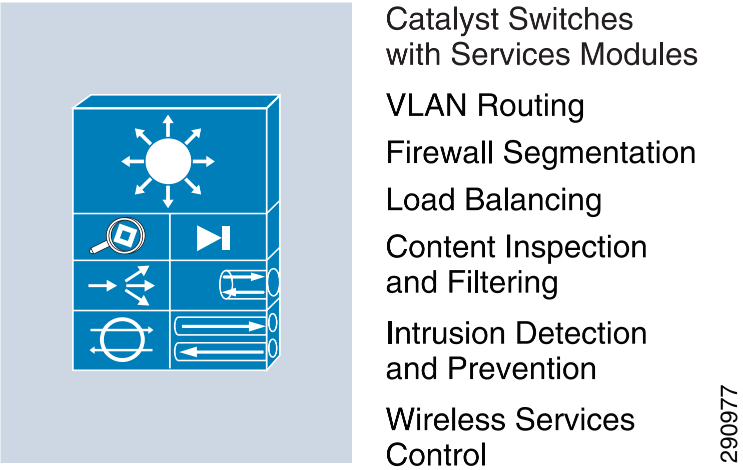
*Table 5-42 PCI Assessment Summary—Cisco Catalyst Data Center Switches*

| **Models Assessed** | |
|---|---|
| Catalyst6509-Sup720-3BXL version s72033-adventerprisek9_wan-mz.122-33.SXJ.bin<br>WS-C3750-48P version c3750-ipbasek9-mz.122-55.SE1.bin<br>WS-C4948-10GE version cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin | |
| **PCI Sub-Requirements Passed** | |
| **PCI 1** | 1.2.2 |
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 9** | 9.1.1 |
| **PCI 10** | 10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

## Primary PCI Function

The primary PCI compliance feature of Cisco Catalyst data center switches is securing the infrastructure. Cisco Catalyst switches have firewall/IDS modules for perimeter security. (See Figure 5-93.)

*Figure 5-93 Cisco Catalyst Data Center Switches*



The main function of the Cisco Catalyst data center switches is segmentation of PCI scope and enforcement of that new scope boundary. These switches have five primary functions/capabilities in relation to PCI:

- Using VLANs, Cisco Catalyst switches allow a retailer to put its payment networks into separate VLANs (scopes) from other non-sensitive data (out of scope).
- The Layer 3 Cisco Catalyst switch acts as a router, directing traffic between networks. By segmenting a network into sub-networks, a retailer can isolate sensitive information from non-sensitive information. The Cisco Catalyst switch can perform the ability to segment and route sensitive traffic from non-sensitive and reduce the overall scope of a company's cardholder data environment. Depending on risk vectors, different levels of enforcement are required at the segmented scope boundary level. See the following bullets for details.
- The Layer 3 Cisco Catalyst switch acts as a router with ACLs, restricting traffic between the cardholder data environment and other areas of the network. A Cisco Catalyst switch with ACLs can be used to enforce segmented traffic if the ACLs are used only to filter and segment private networks of the retailer. ACLs may not be used to segment untrusted networks.
- The Cisco Catalyst switch with a firewall service module restricts traffic between the cardholder data environment and other areas of the network. As soon as any untrusted network is introduced, firewalling and IDS/IPS must be deployed.
- The Layer 3 Cisco Catalyst switch with an intrusion prevention module inspects all traffic going to and from the cardholder data environment. As soon as any untrusted network is introduced, firewalling and IDS/IPS must be deployed.

Table 5-42 lists the component assessment details for the Cisco Catalyst data center switches.

***Table 5-43 Component Capability Assessment—Cisco Catalyst Data Center Switches***

| Cisco Catalyst Data Center Switches | |
|---|---|
| PRIMARY FUNCTION | **Requirement 1, 11 (1.2, 1.3, 11.4)** |
| Provide secure access to payment infrastructure and servers using VLANs, ACLs, and firewall/IPS. | |
| CAPABILITY | ASSESSMENT |
| Secure Services | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| Authentication | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| Logs | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

### Design Considerations

- The configurations of the Cisco Catalyst switches in the data center and Internet edge architectures are maintained within EMC Ionix Network Configuration Manager (alternatively CiscoWorks Resource Manager Essentials, a component of C-LMS, can be used as well).
- The use of VLANs on the Cisco Catalyst switch enables the retailer to provide same-box wired access to its devices while maintaining segregated addressing schemes.
- Using the stacking capability of Cisco Catalyst switches improves high availability designs while simplifying configuration and support.
- Disable the HTTP server on the switch and enable the HTTP secure server.
- Set the **session** and **exec timeout** commands to 15 minutes or less.
- Configure appropriate banner messages on login, incoming, and exec modes of the switch. The login banner warning should not reveal the identity of the company that owns or manages the switch. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the switch to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the switch itself in the event of a WAN or Cisco Secure ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the switch.

### PCI Assessment Detail—PCI Sub-Requirements Satisfied

#### Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

  Router and switch configuration files are backed up centrally using EMC Ionix Network Configuration Manager (NCM). This tool also verifies that running and startup configurations of routers and switches are synchronized.

#### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco switches can be configured to use secure protocols for all system functions. This includes SSH and HTTPS for remote management and SCP for file transfers. Insecure services can be disabled or blocked using configuration statements and access lists.

```
no ip http server
ip http secure-server
ip scp server enable
snmp-server user remoteuser remoteuser v3
line vty 0 4
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
```

```
transport preferred none
transport input ssh
transport output none
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco switches may have several services that are enabled by default that can be disabled.

  ```
  no service pad
  no service udp-small-servers
  no service tcp-small-servers
  no service finger
  no ip http server
  ```

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco switches support administrative protocols with strong cryptography such as SSH version 2 and HTTPS with 3DES.

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco switches. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at: http://www.cisco.com/cisco/software/navigator.html

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*

- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco switches are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default in Cisco switches, no users are allowed access unless specifically configured and assigned appropriate passwords. The following configuration statements create an authentication group called *RETAIL*, which is assigned to various interfaces. This group uses the TACACS+ protocol to communicate with the Cisco ACS server where individual user groups and roles are configured, limiting and logging access as appropriate.

```
aaa new-model
    aaa authentication login RETAIL group tacacs+ local
    aaa authentication enable default group tacacs+ enable
    aaa authorization exec default group tacacs+ if-authenticated
    aaa accounting update newinfo
    aaa accounting exec default start-stop group tacacs+
    aaa accounting commands 15 default start-stop group tacacs+
    aaa accounting system default start-stop group tacacs+
    aaa session-id common
    tacacs-server host 192.168.42.131
    tacacs-server directed-request
    tacacs-server domain-stripping
    tacacs-server key 7 <removed>
```

  Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username bart privilege 15 secret 5 <removed>
username emc-ncm privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

  These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
ip http authentication aaa login-authentication RETAIL

line con 0
 login authentication RETAIL

line vty 0 4
 login authentication RETAIL

line vty 5 15
 login authentication RETAIL
```

### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

The switch is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco switches support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

```
    username bart privilege 15 secret 5 <removed>
    username emc-ncm privilege 15 secret 5 <removed>
```

```
username bmcgloth privilege 15 secret 5 <removed>
username csmadmin privilege 15 secret 5 <removed>
```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco switches require setting of a password.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  In addition to the use of service password encryption to encrypt line interface passwords, the switches also support the use of AES encryption of pre-shared keys.

  ```
  service password-encryption
  password encryption aes
  ```

  Use the **username secret** command to configure a username and MD5-encrypted user password when creating local fall back user accounts.

  ```
  username bart privilege 15 secret 5 <removed>
  username emc-ncm privilege 15 secret 5 <removed>
  username bmcgloth privilege 15 secret 5 <removed>
  username csmadmin privilege 15 secret 5 <removed>
  ```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco switches do not support an automated capability to perform this function at this time; the user account would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco switches do not support an automated capability to perform this function at this time; user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco switches do not support the ability to specify a minimum password length for local accounts; this would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco switches do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco switches do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco switches support the local ability to block logins after a specified number of failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco switches support the local ability to block logins after a specified time after failed login attempts with the following command:

  ```
  login block-for 1800 attempts 6 within 65535
  ```

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco switch management interfaces are configured as follows to meet this requirement:

  ```
  ip http timeout-policy idle 900

  line con 0
   session-timeout 15 output
   exec-timeout 15 0
  line vty 0 4
   session-timeout 15  output
   exec-timeout 15 0
  line vty 5 15
   session-timeout 15  output
   exec-timeout 15 0
  ```

#### Requirement 9: Restrict Physical Access to Cardholder Data

- **PCI 9.1.1**—*Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. Note: “Sensitive areas” refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*

#### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco switches are able to track and monitor all administrative user access, events such as port up/down, as well as device authentication events when using 802.1x.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*

- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

  Cisco switches track individual administrator actions as identified in the requirement above (10.1, 10.2, and 10.3) through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging trap debugging
logging 192.168.42.124
logging buffered 50000

login on-failure log
login on-success log


archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
```

Cisco switches use NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP server was hosted at the data center site. Cisco switches use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162

clock timezone PST -8 0
clock summer-time PDT recurring

service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

  To learn more about NTP, visit:
  http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

**Note** The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

To meet all of the requirements listed below, the PCI solution for retail uses a central logging repository located in the data center. RSA enVision collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

## Cisco Nexus 1000V Switch—Data Center

The Cisco Nexus 1000V Series Switch provides connectivity for virtual servers with the ability to segment them onto their own sensitive scope networks. VLANs are used to put sensitive PCI applications and devices onto their own network and segregate them from devices that are on non-sensitive networks.

The Cisco Nexus 1000V Series Switch provides advanced networking functions and a common network management model in a virtualized server environment. The Cisco Nexus 1000V Series Switch replaces the virtual switching functionality of the VMware vCenter data center container of servers. Each server in the data center container is represented as a line card in the Cisco Nexus 1000V Series Virtual Supervisor Module (VSM) and is managed as if it were a line card in a physical Cisco switch.

Key benefits of the Nexus 1000V include the following:

- Policy-based virtual machine (VM) connectivity
- Mobile VM security and network policy
- Non-disruptive operational model for your server virtualization, and networking teams

*Table 5-44 PCI Assessment Summary—Cisco Nexus 1000V Series Switch*

| **Models Assessed** | |
|---|---|
| Cisco Nexus 1000V version 4.2(1)SV1(4) | |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10. 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |

*Table 5-44 PCI Assessment Summary—Cisco Nexus 1000V Series Switch (continued)*

| PCI Sub-Requirements Failed |
|---|
| No sub-requirements were failed. |

## Primary PCI Function

The primary PCI compliance feature of Cisco Nexus switches is secure aggregation and access layer connectivity.

- Using VLANs, Cisco Nexus switches allow a retailer to put its payment network into separate VLANs (scopes) from other non-sensitive data (out of scope).
- The Layer 3 Cisco Nexus switch acts as a router, directing traffic between networks. By segmenting a network into sub-networks, a retailer can isolate sensitive information from non-sensitive information. The Cisco Nexus switch can segment and route sensitive traffic separately from non-sensitive traffic to reduce the overall scope of a company's cardholder data environment. Depending on risk vectors, various levels of enforcement are required at the segmented scope boundary level.
- The Layer 3 Cisco Nexus switch acts as a router with ACLs, restricting traffic between the cardholder data environment and other areas of the network. A Cisco Nexus switch with ACLs can be used to enforce segmented traffic if the ACLs are used only to filter and segment private networks of the retailer. ACLs may not be used to segment untrusted networks.
- The Cisco Nexus switch uses *virtualization contexts*, which are essentially virtualized switches. Each virtualized context has its own configuration and management interfaces that can be used to segregate not only data but administration as well.

Table 5-44 lists the component assessment details for the Cisco Nexus 1000V Series Switch.

*Table 5-45 Component Capability Assessment—Cisco Nexus 1000V Series Switch*

| Cisco Nexus 1000V Series Switch | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 1** |
| Secure aggregation and access layer connectivity. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

The Cisco Nexus 1000V Series Switch includes the Cisco Integrated Security features that are found on Cisco physical switches to prevent a variety of attack scenarios. For example, a rogue virtual machine can spoof its MAC and IP addresses so that it appears to be an existing production virtual machine, send a rogue Address Resolution Protocol (ARP) transaction mimicking the way that VMware vMotion announces the location of a migrated virtual machine, and divert traffic from the production virtual machine to the rogue virtual machine. With Cisco Integrated Security features, this type of attack can easily be prevented with simple networking policy. Because server virtualization is being used for desktop and server workloads, it is critical that this type of security feature be deployed for the proper operation of a virtualized environment.

The Cisco Nexus 1000V Series implementation has two main components:

- Virtual Supervisor Module (VSM)
- Virtual Ethernet module (VEM)

The Cisco Nexus 1000V VSM is installed as an appliance server on either a standalone Cisco UCS server (Cisco Nexus 1010) or as a virtual appliance on VMware ESXi server running on a blade of the Cisco UCS system.

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  On the Cisco Nexus 1000V, you can turn off the unwanted services such as Telnet and HTTP.

  ```
  no feature http-server
  no feature telnet
  ```

  The remote access is restricted to SSH when you turn off the Telnet service.

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  Cisco SMARTnet services provide ongoing access to software updates and security patches. Cisco Nexus 1000V update software includes fixes for security vulnerabilities along with other bug fixes. The software is available directly from the Cisco website.

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database. It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*

- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  TACACS+ provides for separate authentication, authorization, and accounting services. The TACACS+ daemon provides each service independently.

  First, you have to enable the TACACS+ feature on the Cisco Nexus 1000V:

  ```
  config t
  feature tacacs+
  ```

  The following commands show how to configure the TACACS+ server:

  ```
  tacacs-server key 7 password
  tacacs-server host 192.168.42.131
  aaa group server tacacs+ CiscoACS
      server 192.168.42.131
      use-vrf management
      source-interface mgmt0
  aaa group server tacacs+ tacacs
  aaa authentication login default group CiscoACS
  ```

  Number *7* in the key command specifies an encrypted string (key) to follow.

  Local is the default and is used when no methods are configured or when all the configured methods fail to respond. Configure the local user with encrypted passwords for fallback authentication:

  ```
  username admin password 5 <removed>  role network-admin
  username retail password 5 <removed>  role network-operator
  ```

  Both roles used in the **username** commands are pre-defined roles in the Cisco Nexus 1000V. The network admin role has access to all commands on the switch, whereas the network operator role has access to all read commands on the switch.

#### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services. Configure AAA services as shown in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters. PCI Sub-Requirements with Compensating Controls*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

#### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco Nexus Switches are able to track and monitor all administrative user access, events such as port up/down, as well as device authentication events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

  Cisco Nexus switches track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

  ```
  logging server 192.178.42.124 6 facility syslog

  aaa accounting default group CiscoACS
  ```

Cisco Nexus switches use NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco Nexus switches use NTP to meet these requirements by implementing the following configuration statements.

```
enable NTP
ntp server 192.168.62.161 use-vrf management
ntp server 192.168.62.162 use-vrf management

clock timezone PST -8 0
clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
```

To learn more about NTP, visit:
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

## Cisco Nexus Switches—Data Center

The Cisco Nexus family of data center switches securely switches data; from payment application servers to high speed trunks of the core, maintaining the integrity of segmented scopes of compliance. They provide scalable inter-switch connectivity and high port density for wired endpoints. VLANs are used to put sensitive PCI applications and devices onto their own network and segregate them from devices on non-sensitive networks.

Cisco Nexus switches are ideal for enterprise-class server and aggregation layer deployments. These multipurpose, multilayer switches can be deployed across a diverse set of traditional, virtualized, unified, and high-performance computing environments. They enable diverse transports over Ethernet (including Layer 2, Layer 3, and storage traffic) on one common platform. Nexus switches help transform your data center, with a standards-based, multipurpose, multiprotocol, Ethernet-based fabric.

*Table 5-46 PCI Assessment Summary—Cisco Nexus Data Center Switches*

| **Models Assessed** | |
|---|---|
| Cisco Nexus5020 Chassis (“40x10GE/Supervisor”) version n5000-uk9.5.0.3.N1.1b.bin<br>Cisco 7010 Chassis (“Supervisor module-1X”) version n7000-s1-dk9.5.1.2.bin | |
| **PCI Sub-Requirements Passed** | |
| **PCI 1** | 1.2.2 |

*Table 5-46 PCI Assessment Summary—Cisco Nexus Data Center Switches (continued)*

| | |
|---|---|
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10. 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

## Primary PCI Function

The primary PCI compliance feature of Cisco Nexus data center switches is secure aggregation and access layer connectivity.

- Using VLANs, Cisco Nexus switches allow a retailer to put its payment network into separate VLANs (scopes) from other non-sensitive data (out of scope).
- The Layer 3 Cisco Nexus switch acts as a router, directing traffic between networks. By segmenting a network into sub-networks, a retailer can isolate sensitive information from non-sensitive information. The Cisco Nexus switch can segment and route sensitive traffic separately from non-sensitive traffic to reduce the overall scope of a company’s cardholder data environment. Depending on risk vectors, various levels of enforcement are required at the segmented scope boundary level.
- The Layer 3 Cisco Nexus switch acts as a router with ACLs, restricting traffic between the cardholder data environment and other areas of the network. A Cisco Nexus switch with ACLs can be used to enforce segmented traffic if the ACLs are used only to filter and segment private networks of the retailer. ACLs may not be used to segment untrusted networks.
- The Cisco Nexus switch uses virtualization contexts, which are essentially virtualized switches. Each virtualized context has its own configuration and management interfaces that can be used to segregate not only data but administration as well.

Table 5-46 lists the component assessment details for the Cisco Nexus data center switches.

*Table 5-47 Component Capability Assessment —Cisco Nexus Data Center Switches*

| Cisco Nexus Data Center Switches | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 1 (1.3.5)** |
| Secure access to payment infrastructure and servers using segmentation of trusted networks (VLANs, ACLs). | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

- Configuration was done manually on the router CLI, and backup of configuration and monitoring of configuration for changes and non-compliance were done through the EMC Ionix Network Configuration Manager (alternatively CiscoWorks Resource Manager Essentials, a component of C-LMS, can be used as well).
- Configure appropriate banner messages on login, incoming, and EXEC modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the router to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the router itself in the event of a WAN or Cisco Secure ACS failure.
- Nexus switches in the data center were implemented using guidance from the Enterprise Data Center Design guide based on a Data Center 3.0 Architecture:
  http://www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html

  Enterprise Internet Edge Design Guide:
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/IE_DG.html
- The Cisco Nexus 7010 and the Cisco Nexus 5000 were used for the aggregation block portions of the lab validation network.

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

  Cisco Nexus configuration files are backed up centrally using EMC Ionix Network Configuration Manager (NCM). This tool also verifies that running and startup configurations are synchronized.

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco Nexus switches can be configured to use secure protocols for all system functions. This includes SSH for remote management, SCP, and SFTP for file transfers. Insecure services can be disable or blocked using configuration statements and access lists.

  ```
  no feature telnet
  no telnet server enable
  feature ssh
  ```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco Nexus switches have no extraneous services that are enabled by default.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco Nexus switches support administrative protocols with strong cryptography such as SSH version 2.

**Note** Strong cryptography—Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible). Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher). See NIST Special Publication 800-57 (www.csrc.nist.gov/publications/) for more information.

```
! Generate keys with 1024 or larger bit key generation NOT the default 512

ssh key rsa 1024 force

! Cisco Nexus switches utilize SSH version 2.
```

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

Cisco SMARTnet services provide ongoing access to software updates and security patches: http://www.cisco.com/cisco/software/type.html?mdfid=282099479&flowid=3088.

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

Cisco Nexus switches are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels have access to only the information they require for their job function. By default in Cisco Nexus switches, no users are allowed access unless specifically configured and assigned.

```
feature tacacs+

aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable

tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
```

Local user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username admin password 5 <removed>  role network-admin
username retail password 5 <removed>  role network-admin
username bart password 5 <removed>  role network-admin
username emc-ncm password 5 <removed>  role network-admin
```

These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
```

### Requirement 8: Assign a Unique ID to Each Person with Computer Access

For Cisco Nexus switches to meet all of the user access restrictions specified in Requirement 8, an external authentication service such as Cisco Secure Access Control Server must be implemented. Configure AAA services as shown above in Requirement 7.

The switch is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco Nexus switches support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts. They should be individually unique as specified by policy.

  ```
  username admin password 5 <removed>  role network-admin
  username retail password 5 <removed>  role network-admin
  username bart password 5 <removed>  role network-admin
  username emc-ncm password 5 <removed>  role network-admin
  ```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*

  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco Nexus switches support the ability to specify a password.

  ```
  username admin password 5 <removed>  role network-admin
  username retail password 5 <removed>  role network-admin
  username bart password 5 <removed>  role network-admin
  username emc-ncm password 5 <removed>  role network-admin
  ```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  Local user fall back accounts are created with the **username** command and use MD5-encryption for the user password. Communication to the AAA server using RADIUS or TACACS+ is encrypted when using centralized authentication.

  ```
      username admin password 5 <removed>  role network-admin
      username retail password 5 <removed>  role network-admin
      username bart password 5 <removed>  role network-admin
      username emc-ncm password 5 <removed>  role network-admin
  ```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco Nexus switches do not support an automated capability to perform this function at this time; user accounts would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco Nexus switches do not support an automated capability to perform this function at this time; user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager.

Requirements 8.5.10–8.5.11 can be satisfied with a single configuration statement as identified below.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.PCI Sub-Requirements with Compensating Controls*

  The NX-OS software accepts only strong passwords when you have password strength checking enabled (default) using the **password strength-check** command. The characteristics of a strong password include the following:

  - At least eight characters long
  - Does not contain many consecutive characters (such as "abcd")
  - Does not contain many repeating characters (such as "aaabbb")
  - Does not contain dictionary words
  - Does not contain proper names
  - Contains both uppercase and lowercase characters
  - Contains numbers

  ```
  password strength-check
  ```

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco Nexus switches do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco Nexus switches do not support the ability to lock out local accounts after failed login attempts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco Nexus switches do not support the ability to manage lockout of local accounts after failed login attempts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco Nexus switch management interfaces are configured as follows to meet this requirement:

  ```
  line console
    exec-timeout 15

  line vty
    exec-timeout 15
  ```

### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco Nexus switches are able to track and monitor all administrative user access, events such as port up/down, as well as device authentication events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*

  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

  Cisco Nexus switches track individual administrator actions through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging server 192.168.42.124 6
!
! --- for implementations using VRF's ----
!
logging server 192.168.42.124 6 use-vrf servers1

aaa accounting default group CiscoACS
```

Cisco Nexus switches use NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco Nexus switches use NTP to meet these requirements by implementing the following configuration statements.

```
    ! NTP can only be configured in the default VDC
    !
    enable NTP
    ntp server 192.168.62.161 use-vrf management
    ntp server 192.168.62.162 use-vrf management

    clock timezone PST -8 0
    clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
```

  To learn more about NTP, visit:
  http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

## Wireless

Cisco Wireless technologies provide connectivity for mobile clients within the store. They can secure connectivity for traditional business functions such as guest access or inventory control, without increasing risk. Innovative customer experience services such as mobile point-of-sale are equally secure. In addition to expanding business functionality, Cisco wireless technology seamlessly provides the capability to detect rogues.

Industry-leading performance is available with Cisco Aironet access points for highly secure and reliable wireless connections for both indoor and outdoor environments. Cisco offers a broad portfolio of access points targeted to specific business needs and topologies.

Cisco wireless controllers help reduce the overall operational expenses of Cisco Unified Wireless Networks by simplifying network deployment, operations, and management. They extend the Cisco Borderless Network policy and security from the wired network to the wireless edge.

Cisco Wireless Control System (WCS) delivers full visibility and control of Cisco Aironet access points, Cisco Wireless LAN Controllers (WLC) and the Cisco Mobility Services Engine (MSE) with built-in support for Cisco adaptive wireless intrusion prevention systems (wIPS) and Cisco context-aware services. This robust platform helps you reduce total cost of ownership and maintain a business-ready wireless network.

*Table 5-48 PCI Assessment Summary—Cisco Wireless Products*

| **Models Assessed** | |
|---|---|
| AIR-CT5508-12-K9 version 7.0.114.112<br>MSE3550 version 7.0.200.125<br>Cisco WCS Manager version 7.0.171.107<br>AIR-CAP1042N<br>AIR-CAP3502i<br>AIR-CAP3502E<br>AIR-LAP1262N | |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.1.1, 2.2, 2.2.2, 2.2.4, 2.3 |

*Table 5-48 PCI Assessment Summary—Cisco Wireless Products (continued)*

| | |
|---|---|
| **PCI 4** | 4.1, 4.1.1 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3 |
| **PCI 11** | 11.1.b, 11.1.d |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

## Primary PCI Function

The primary PCI function of Cisco Unified Wireless is secure connectivity of wireless clients (4.1) and rogue detection (1.1).

Table 5-48 lists the component assessment details for Cisco wireless products.

*Table 5-49 Component Capability Assessment —Cisco Wireless Products*

| Cisco Wireless Products | |
|---|---|
| PRIMARY FUNCTION | **Requirement 4, 11 (4.1, 11.1)** |
| Secure access to payment infrastructure and servers using segmentation of trusted networks (VLANs, ACLs). | |
| CAPABILITY | ASSESSMENT |
| Secure Services | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| Authentication | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| Logs | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

### Design Considerations

Rogue detection for wireless technology in the store is required at a minimum of once a quarter, whether or not the retailer has wireless deployed. A hacker might infiltrate a store and install a rogue wireless device (for example, access point, wireless-enabled printer, or radio-enabled USB stick). This would allow a hacker remote access into the store (from the parking lot, for example) that is hard to detect. The PCI DSS offers several methods for detecting rogue devices. Cisco Unified Wireless offers the benefit of continuous rogue detection while simultaneously passing normal wireless traffic.

The PCI-DSS states that wireless technology is an untrusted network connection. Wireless technology in the store requires firewall and intrusion detection services to segment and protect the cardholder data environment. Stateful firewalls must be configured to limit traffic to and from the wireless environment (all enabled services, protocols, and ports must have documented justification for business purposes). All other access must be denied.

When including point-of-sale clients in the wireless network, strong wireless encryption technology needs to be implemented.

⚠ **Caution** Wireless clients must be protected from each other, as well. For example, when using hand-held scanners and mobile POS, the scanners need to be on separate SSIDs and networks from the POS, and protected with firewall and intrusion detection services that are restricted to justified business access.

Wireless compliance is broken into the stages listed in Table 5-50.

*Table 5-50 Wireless Compliance Stages*

| Wireless Deployment | Risk | Required Measure |
|---|---|---|
| No wireless deployed | Hacker deploys wireless into store | Rogue detection |
| Wireless deployed, no wireless POS/CDE | Hacker deploys unknown wireless into store, or hacks into existing wireless | Rogue detection<br>Stateful firewall separating wired from wireless LAN<br>Intrusion Detection System |
| Wireless deployed, includes wireless POS/CDE | Hacker deploys unknown wireless into store, or hacks into existing wireless | Rogue detection<br>Stateful firewall separating wired from wireless LAN<br>Intrusion Detection System<br>Strong wireless encryption for CDE (e.g., WPA2)<br>Wireless CDE must be protected from other wireless and wired segments using a stateful firewall (Req. 1,2,3) |

Cisco recommends using the Unified Wireless (controller-based) architecture for retail wireless deployments because of the Cisco ongoing wireless strategy. The autonomous Cisco IOS access points are not being enhanced. Future security and user enhancements will be developed on the controller-based architecture.

For WCS servers running software versions prior to 4.1, Cisco recommends a combination of documented password policies, manual audit procedures, and firewall segmentation for WCS servers within the data center.

- Configure unique SSIDs
- Disable broadcast of the SSIDs

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

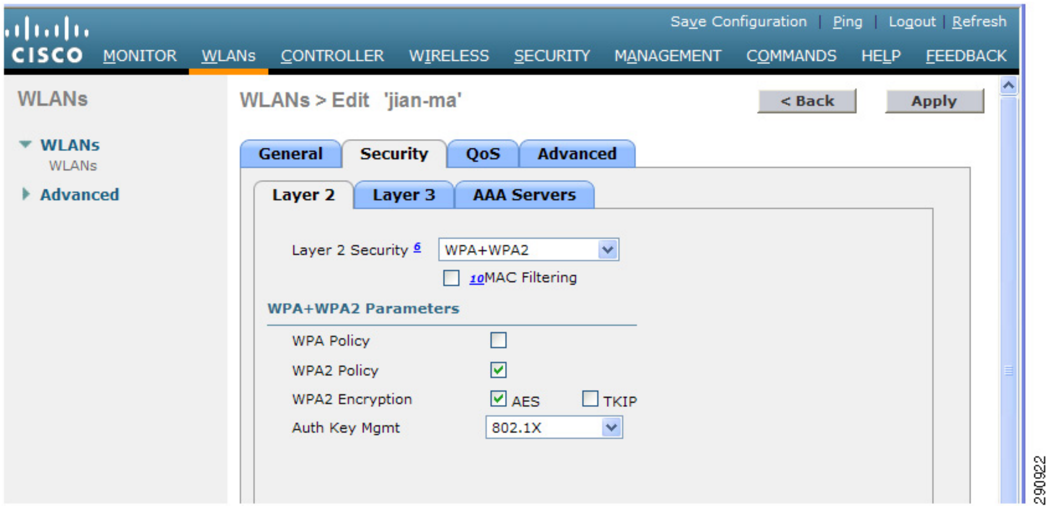
Whenever possible, a screenshot highlighting the appropriate Cisco Wireless Control System functionality is provided.

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.1.1**—*For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.*

  The Cisco Unified Wireless Network supports both Wi-Fi Protected Access (WPA) and WPA2 and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption (see Figure 5-94 and Figure 5-95). There is no default PSK, and all PSKs must be created during configuration. The Cisco Unified Wireless Network architecture does not use SNMP at the access points.

***Figure 5-94 WLANs Security Screen***



WLANs > Edit 'jian-ma'

Layer 2 Security 6 WPA+WPA2

□ 10MAC Filtering

WPA+WPA2 Parameters

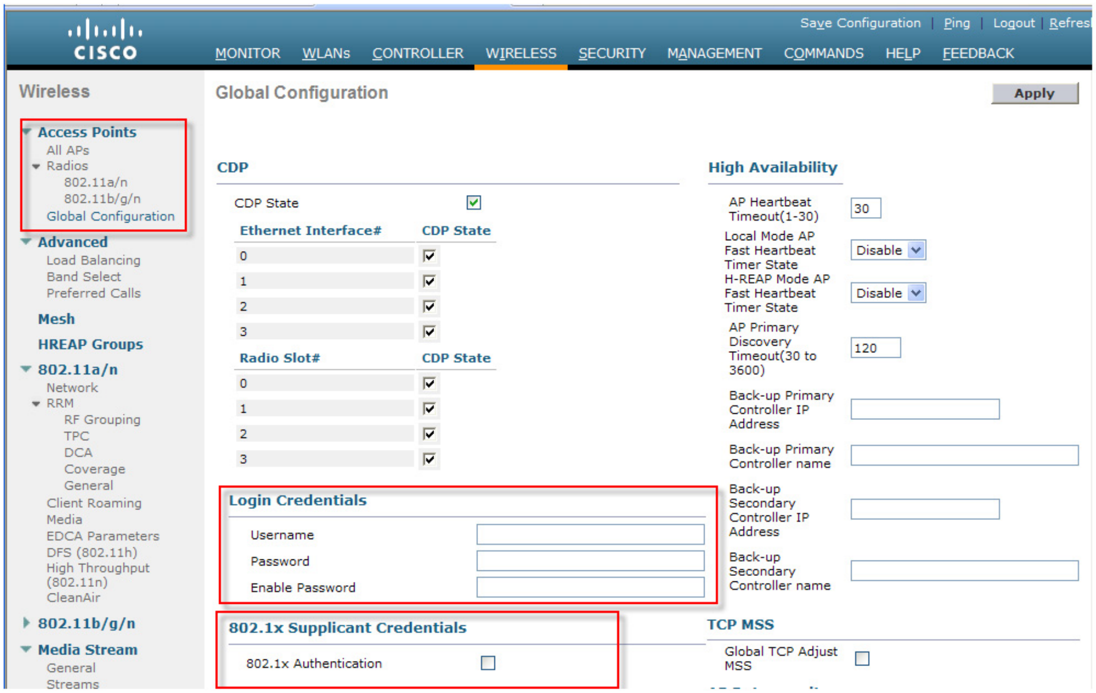
WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑ AES □ TKIP

Auth Key Mgmt 802.1X

*Figure 5-95 Wireless Global Configuration Screen*



Global Configuration

CDP

CDP State ☑

| Ethernet Interface# | CDP State |
|---|---|
| 0 | ☑ |
| 1 | ☑ |
| 2 | ☑ |
| 3 | ☑ |

| Radio Slot# | CDP State |
|---|---|
| 0 | ☑ |
| 1 | ☑ |
| 2 | ☑ |
| 3 | ☑ |

Login Credentials

| | |
|---|---|
| Username | |
| Password | |
| Enable Password | |

802.1x Supplicant Credentials

802.1x Authentication ☐

High Availability

| | |
|---|---|
| AP Heartbeat Timeout(1-30) | 30 |
| Local Mode AP Fast Heartbeat Timer State | Disable |
| H-REAP Mode AP Fast Heartbeat Timer State | Disable |
| AP Primary Discovery Timeout(30 to 3600) | 120 |
| Back-up Primary Controller IP Address | |
| Back-up Primary Controller name | |
| Back-up Secondary Controller IP Address | |
| Back-up Secondary Controller name | |

TCP MSS

Global TCP Adjust MSS ☐

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  There are no unnecessary services enabled by default on the Cisco Unified Wireless Control Server system. Cisco Unified Wireless Control Server should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository.

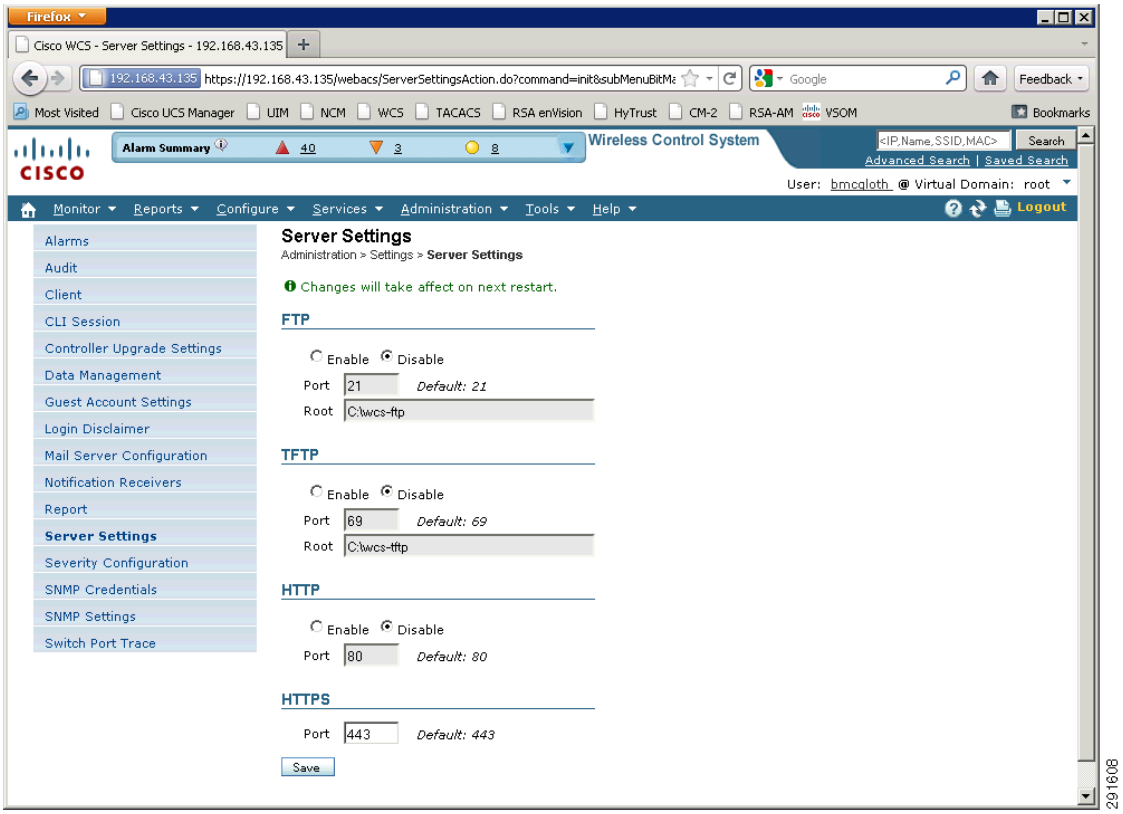
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers*

  Cisco Unified Wireless Control Server system should be installed on a hardened operating system. Hardening guidance can be found at the National Checklist Program Repository: http://web.nvd.nist.gov/view/ncp/repository

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.*

  Cisco Unified Wireless Control Server system can be configured for secure management using strong cryptography. Figure 5-96, Figure 5-97, Figure 5-98, and Figure 5-99 show where to disable non-encrypted management interfaces (for example, Telnet and HTTP).

*Figure 5-96 WCS Server Secure Management*



Server Settings

Administration > Settings > **Server Settings**

Changes will take affect on next restart.

FTP

○ Enable ● Disable

Port 21 *Default: 21*

Root C:\wcs-ftp

TFTP

○ Enable ● Disable

Port 69 *Default: 69*

Root C:\wcs-tftp

HTTP

○ Enable ● Disable

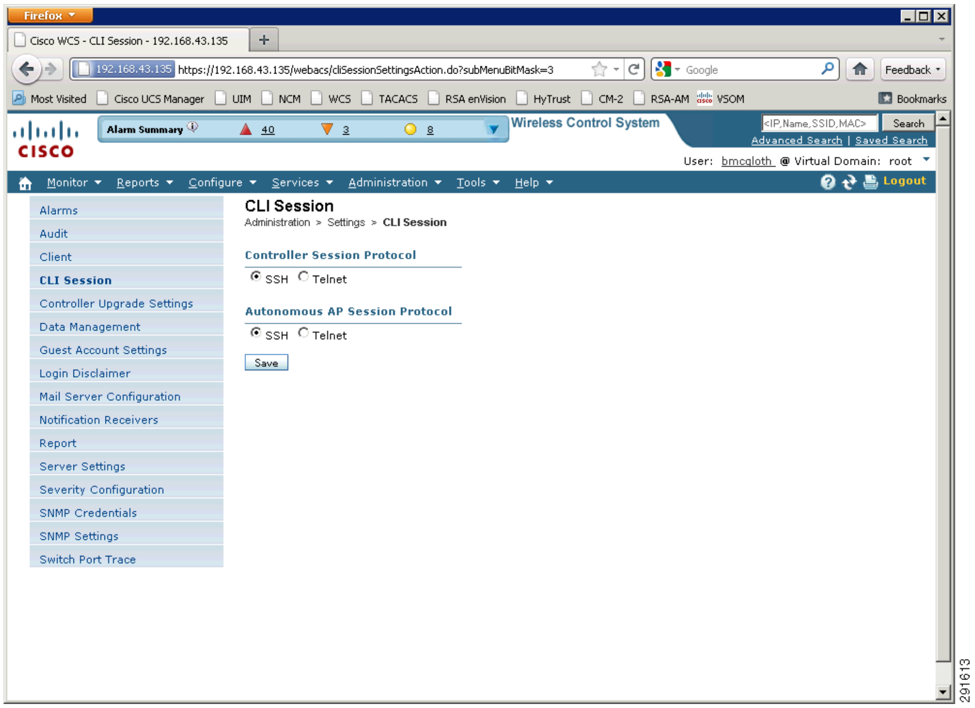
Port 80 *Default: 80*

HTTPS

Port 443 *Default: 443*

Save

*Figure 5-97 CLI Session Secure Management*



CLI Session

Administration > Settings > **CLI Session**

Controller Session Protocol

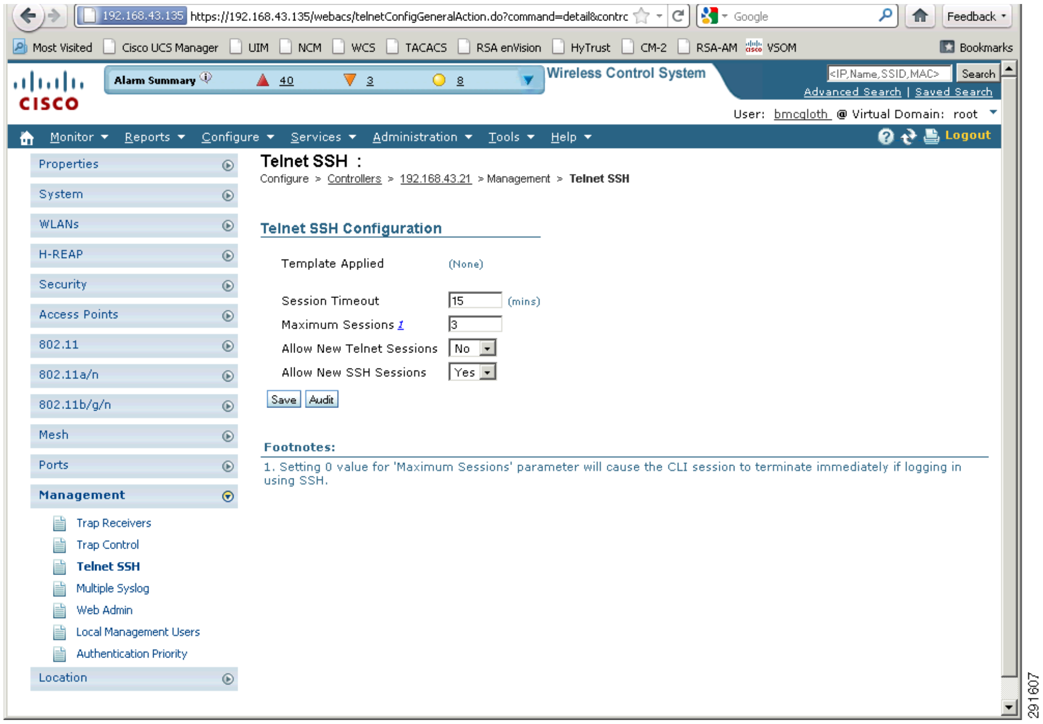
● SSH ○ Telnet

Autonomous AP Session Protocol

● SSH ○ Telnet

Save

*Figure 5-98 Controller Secure Management for SSH*



Telnet SSH :

Configure > Controllers > 192.168.43.21 > Management > Telnet SSH

Telnet SSH Configuration

Template Applied (None)

Session Timeout 15 (mins)

Maximum Sessions 1 3

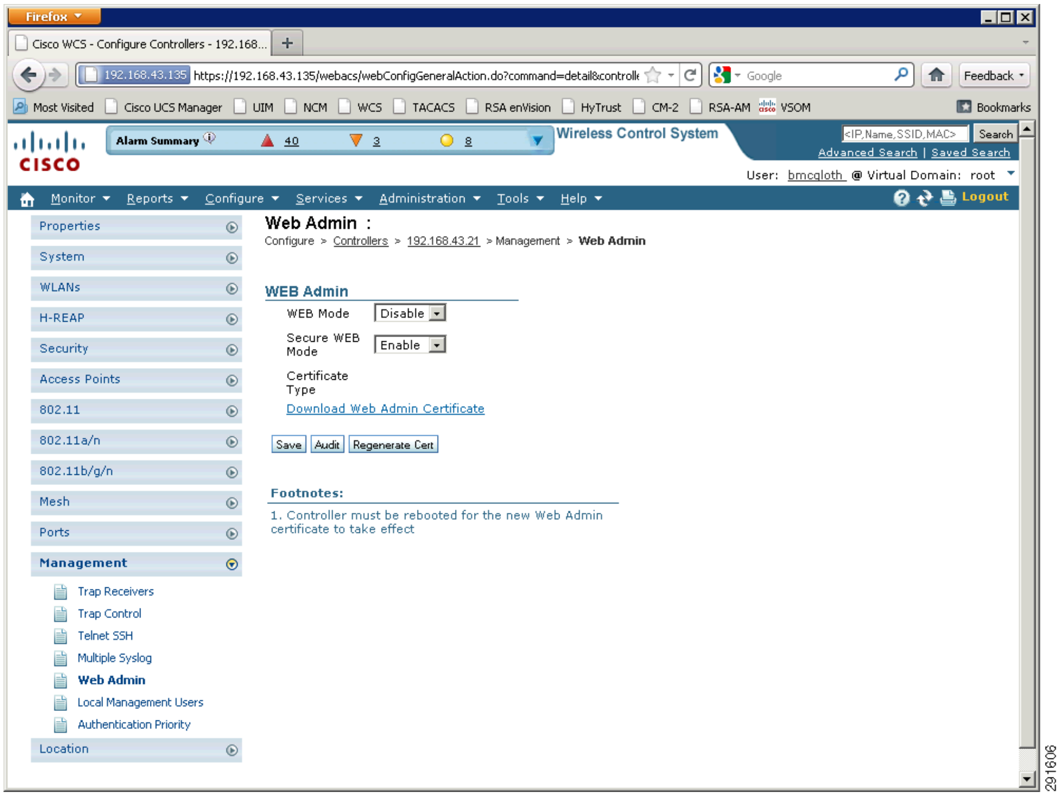
Allow New Telnet Sessions No

Allow New SSH Sessions Yes

Footnotes:

1. Setting 0 value for 'Maximum Sessions' parameter will cause the CLI session to terminate immediately if logging in using SSH.

*Figure 5-99 Controller Secure Management for HTTPS*



Web Admin :

Configure > Controllers > 192.168.43.21 > Management > Web Admin

WEB Admin

WEB Mode Disable

Secure WEB Mode Enable

Certificate Type

Download Web Admin Certificate

Footnotes:

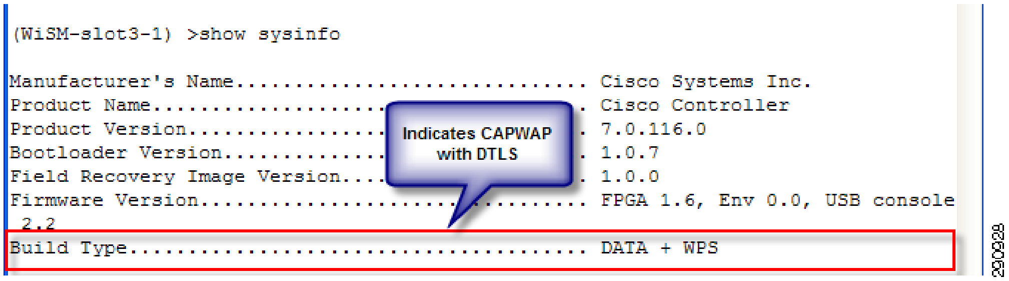
1. Controller must be rebooted for the new Web Admin certificate to take effect

### Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*
  - *The Internet*
  - *Wireless technologies,*
  - *Global System for Mobile communications (GSM)*
  - *General Packet Radio Service (GPRS)*

  Cisco offers Control and Provisioning of Wireless Access Points (CAPWAP)-compliant DTLS encryption to ensure full-line-rate encryption between access points and controllers across remote WAN/LAN links (see Figure 5-100). The Cisco Unified Wireless Network defaults to the highest CipherSuite available on the network. Furthermore, fallback on less secure SSL versions (that is, SSLv2 and SSLv1) can also be disabled, thus always forcing use of SSLv3. The Cisco Unified Wireless Network provides 256-bit encryption and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption/authentication configurations.

***Figure 5-100 CAPWAP with DTLS***



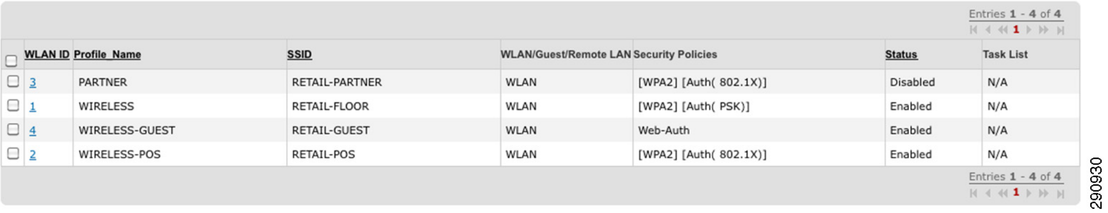
```
(WiSM-slot3-1) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 7.0.116.0
Bootloader Version............................... 1.0.7
Field Recovery Image Version..................... 1.0.0
Firmware Version................................. FPGA 1.6, Env 0.0, USB console
 2.2
Build Type....................................... DATA + WPS
```

Indicates CAPWAP with DTLS

- **PCI 4.1.1**—*Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. Note: The use of WEP as a security control was prohibited as of 30 June 2010.*

  Cisco supports both WPA and WPA2 and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption. Cisco does not advertise the organization’s name in the Service Set ID (SSID) broadcast. Cisco also disables SSID broadcast by default for non-guest networks. Cisco supports WPA2 Personal mode with a minimum 13-character random pass-phrase and Advanced Encryption Standard (AES) encryption, and provides automated vulnerability scanning in the WCS to identify WLANs using suboptimal encryption/authentication configurations. (See Figure 5-101.)

***Figure 5-101 WLAN Information***



Entries 1 - 4 of 4

| □ | WLAN ID | Profile_Name | SSID | WLAN/Guest/Remote LAN | Security Policies | Status | Task List |
|---|---|---|---|---|---|---|---|
| □ | 3 | PARTNER | RETAIL-PARTNER | WLAN | [WPA2] [Auth( 802.1X)] | Disabled | N/A |
| □ | 1 | WIRELESS | RETAIL-FLOOR | WLAN | [WPA2] [Auth( PSK)] | Enabled | N/A |
| □ | 4 | WIRELESS-GUEST | RETAIL-GUEST | WLAN | Web-Auth | Enabled | N/A |
| □ | 2 | WIRELESS-POS | RETAIL-POS | WLAN | [WPA2] [Auth( 802.1X)] | Enabled | N/A |

Entries 1 - 4 of 4

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Unified Wireless. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS using TACACS+ and RADIUS services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

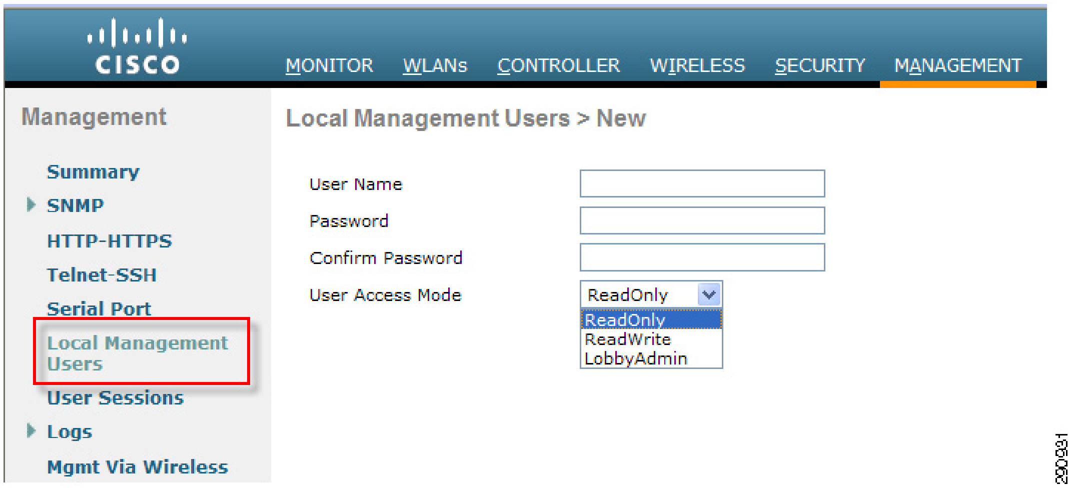
- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

Cisco Unified Wireless allows the network administrator to set user IDs that can be monitored and restricted with respect to access and other privileges when necessary.

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  The Cisco solution uses profiles where a user is assigned to the profile to ensure appropriate access to ensure network security, and user access can be restricted as shown in Figure 5-102 and Figure 5-103.

*Figure 5-102 Local Management Users Screen*



Local Management Users > New

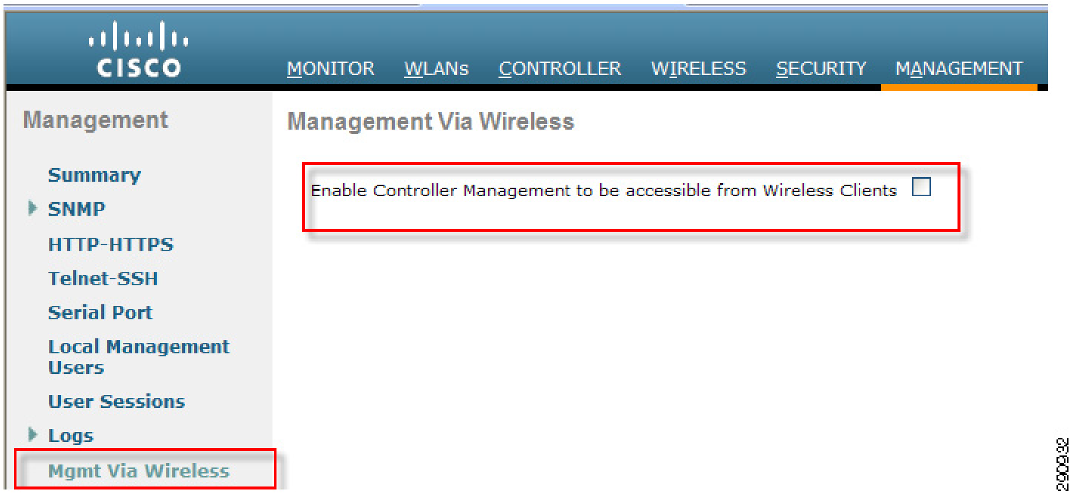
User Name

Password

Confirm Password

User Access Mode: ReadOnly

*Figure 5-103 Management Via Wireless Screen*

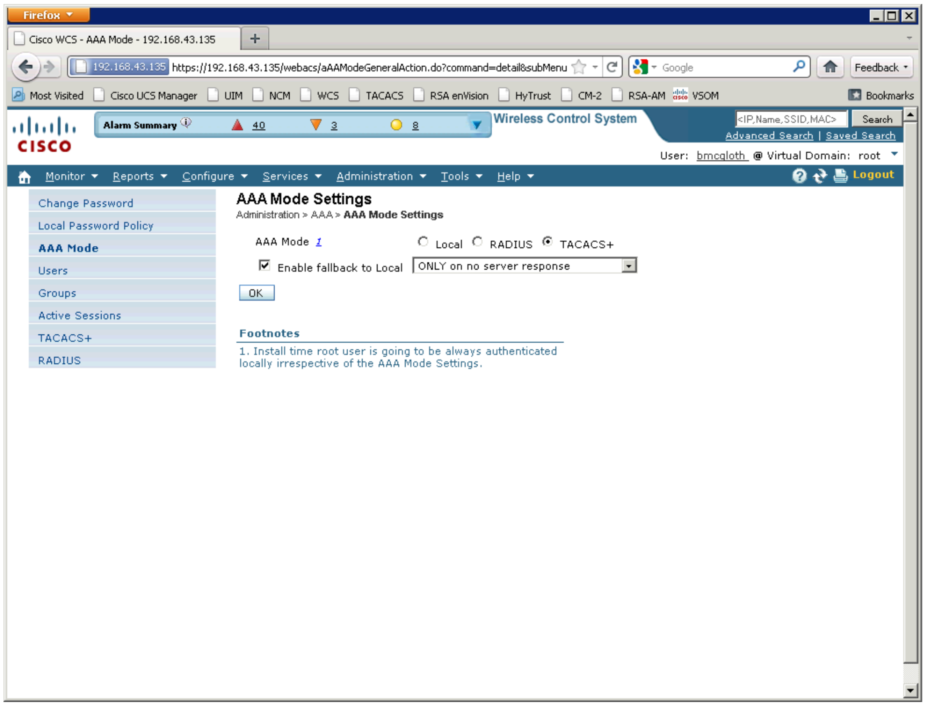


Management Via Wireless

Enable Controller Management to be accessible from Wireless Clients ☐

Cisco WCS is configured to use TACACS+ for authentication of administrators, as shown in Figure 5-104.

*Figure 5-104 WCS Manager AAA Authentication Mode*



AAA Mode Settings

Administration > AAA > **AAA Mode Settings**

AAA Mode 1 ○ Local ○ RADIUS ● TACACS+

☑ Enable fallback to Local ONLY on no server response

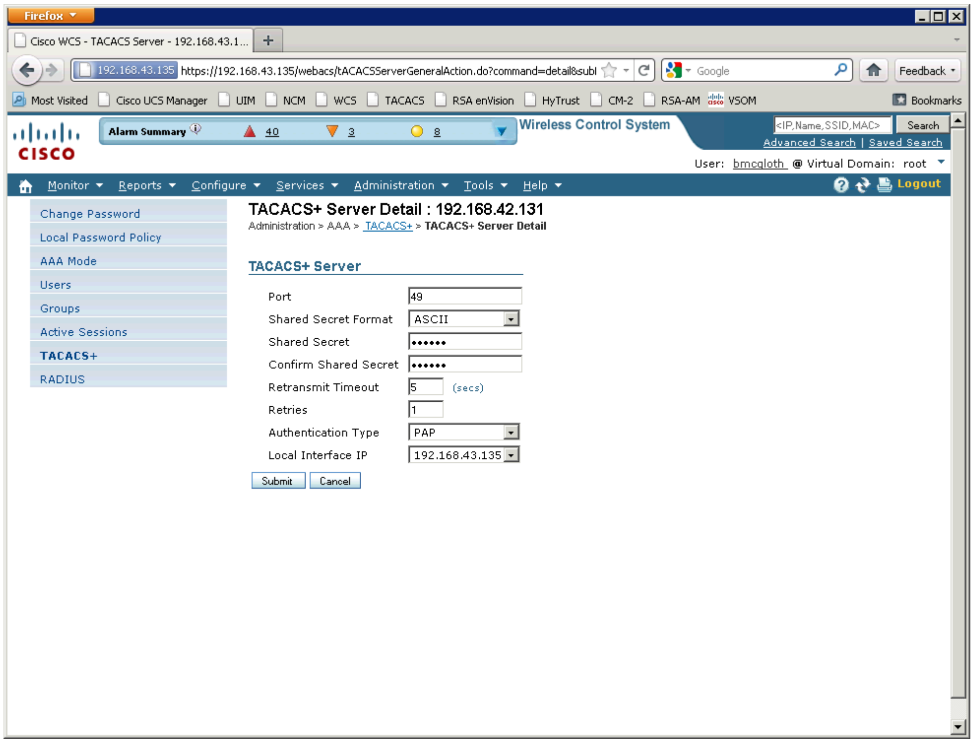
OK

Footnotes

1. Install time root user is going to be always authenticated locally irrespective of the AAA Mode Settings.

The authentication servers for TACACS+ in WCS Manager are configured as shown in Figure 5-105.

*Figure 5-105 WCS Manager TACACS+ Server Configuration*



TACACS+ Server Detail : 192.168.42.131

Administration > AAA > TACACS+ > **TACACS+ Server Detail**

TACACS+ Server

| | |
|---|---|
| Port | 49 |
| Shared Secret Format | ASCII |
| Shared Secret | •••••• |
| Confirm Shared Secret | •••••• |
| Retransmit Timeout | 5 (secs) |
| Retries | 1 |
| Authentication Type | PAP |
| Local Interface IP | 192.168.43.135 |

Submit Cancel

### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

Cisco Unified Wireless is able to meet some of the requirements locally, as identified below.

- **PCI 8.1**—Assign all users a unique ID before allowing them to access system components or cardholder data.

  Cisco WCS supports the creation of local user accounts with unique IDs. These can be used for local fallback user accounts. They should be individually unique as specified by policy.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco WCS Manager and controllers support the ability to specify a password.

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  Local user fall back accounts use MD5-encryption for the user password. Communication to the AAA server using RADIUS or TACACS+ is encrypted when using centralized authentication.

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

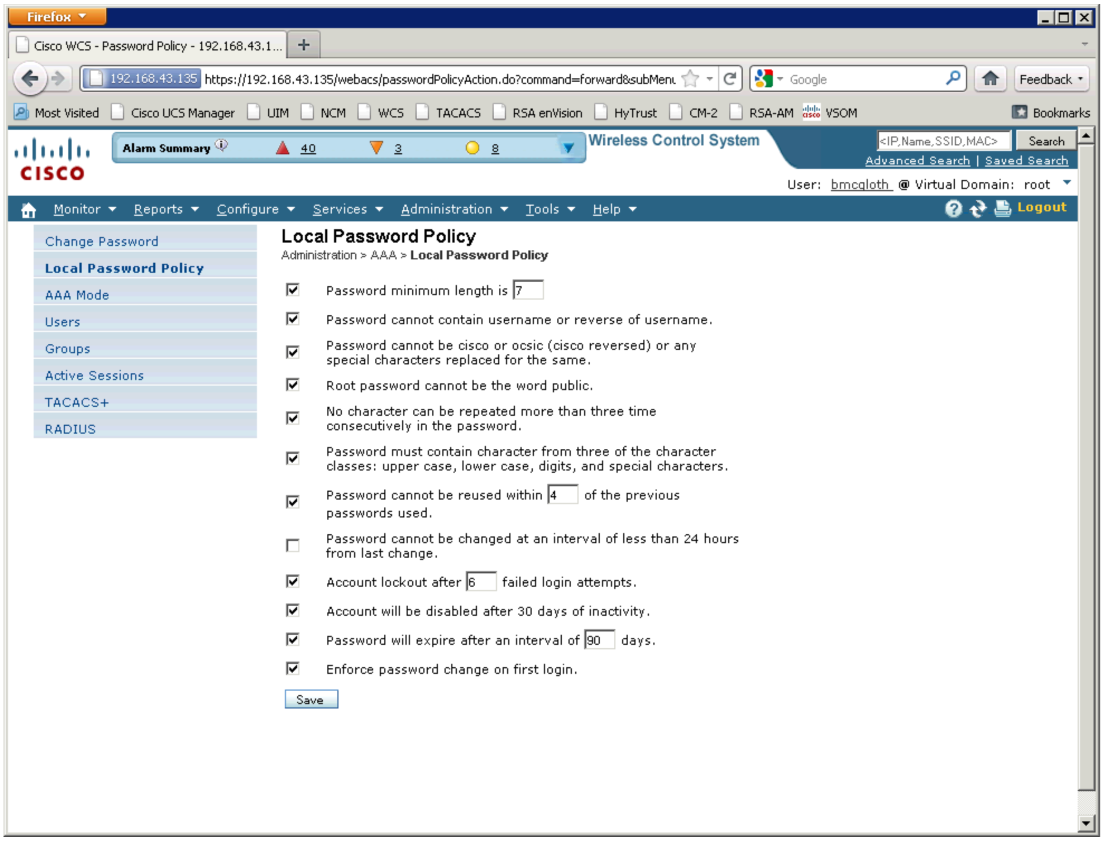
  Cisco Unified Wireless does not support an automated capability to perform this function at this time, user account would have to be manually reviewed in the device configurations every 90 days.

  The next several requirements (8.5.9–8.5.14) are addressed with the local password policy.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Figure 5-106 shows the local password policy that has been modified to meet the minimum requirements as specified by the preceding requirements.

*Figure 5-106 WCS Manager Local Password Policy*



Local Password Policy

Administration > AAA > **Local Password Policy**

- ☑ Password minimum length is 7
- ☑ Password cannot contain username or reverse of username.
- ☑ Password cannot be cisco or ocsic (cisco reversed) or any special characters replaced for the same.
- ☑ Root password cannot be the word public.
- ☑ No character can be repeated more than three time consecutively in the password.
- ☑ Password must contain character from three of the character classes: upper case, lower case, digits, and special characters.
- ☑ Password cannot be reused within 4 of the previous passwords used.
- □ Password cannot be changed at an interval of less than 24 hours from last change.
- ☑ Account lockout after 6 failed login attempts.
- ☑ Account will be disabled after 30 days of inactivity.
- ☑ Password will expire after an interval of 90 days.
- ☑ Enforce password change on first login.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to reactivate the terminal or session.*

  Cisco WCS Manager limits sessions, as shown in Figure 5-98 above.

### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

The Cisco Unified Wireless system is able to track and monitor all administrative user access and events.

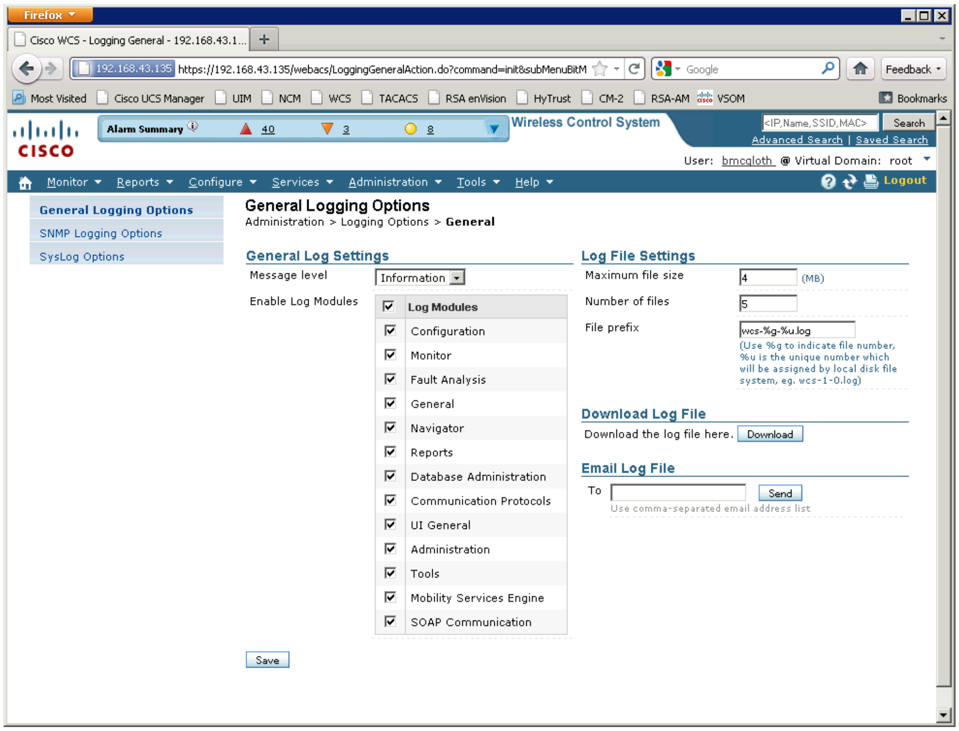
- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*

  Cisco Unified Wireless tracks individual administrator actions through several mechanisms including AAA, logging, and system events.

- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Figure 5-107 shows the configuration of local logging settings, and Figure 5-108 shows the syslog server configuration used to send logs to RSA enVision.

***Figure 5-107 Local Logging Configuration***



General Logging Options
Administration > Logging Options > **General**

General Log Settings

Message level: Information

Enable Log Modules:
- ☑ Log Modules
- ☑ Configuration
- ☑ Monitor
- ☑ Fault Analysis
- ☑ General
- ☑ Navigator
- ☑ Reports
- ☑ Database Administration
- ☑ Communication Protocols
- ☑ UI General
- ☑ Administration
- ☑ Tools
- ☑ Mobility Services Engine
- ☑ SOAP Communication

Save

Log File Settings

| | |
|---|---|
| Maximum file size | 4 (MB) |
| Number of files | 5 |
| File prefix | wcs-%g-%u.log<br>(Use %g to indicate file number, %u is the unique number which will be assigned by local disk file system, eg. wcs-1-0.log) |

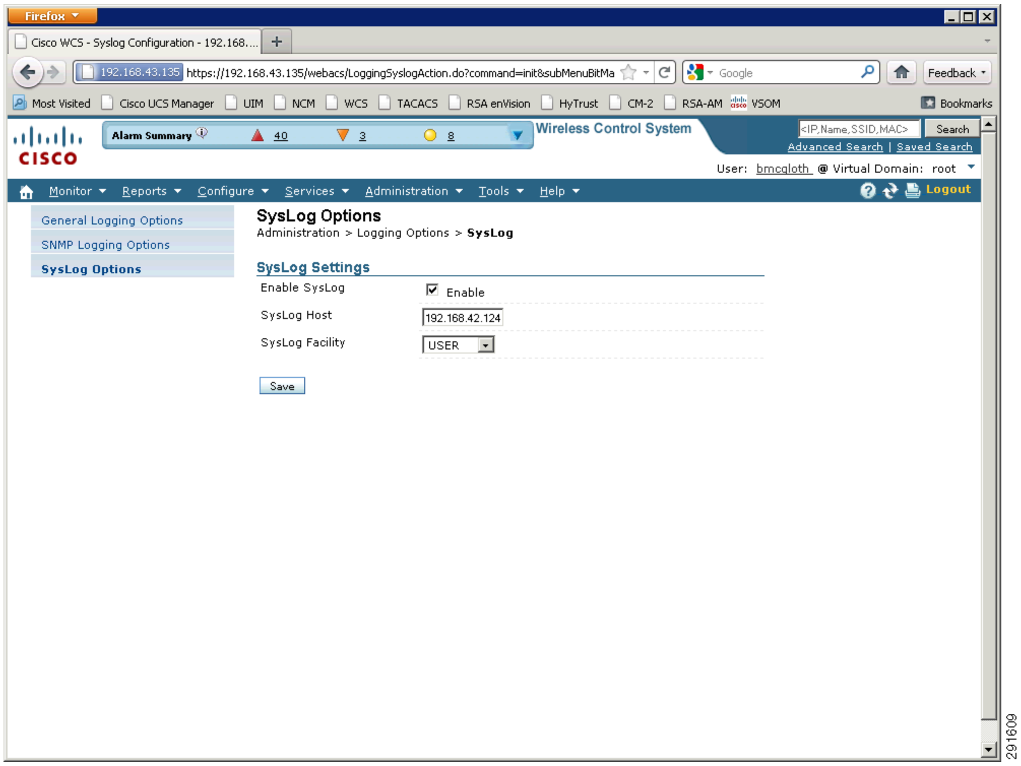
Download Log File

Download the log file here. Download

Email Log File

To ____ Send
Use comma-separated email address list

*Figure 5-108 WCS Manager Syslog Configuration*



SysLog Options

Administration > Logging Options > **SysLog**

SysLog Settings

| | |
|---|---|
| Enable SysLog | ☑ Enable |
| SysLog Host | 192.168.42.124 |
| SysLog Facility | USER |

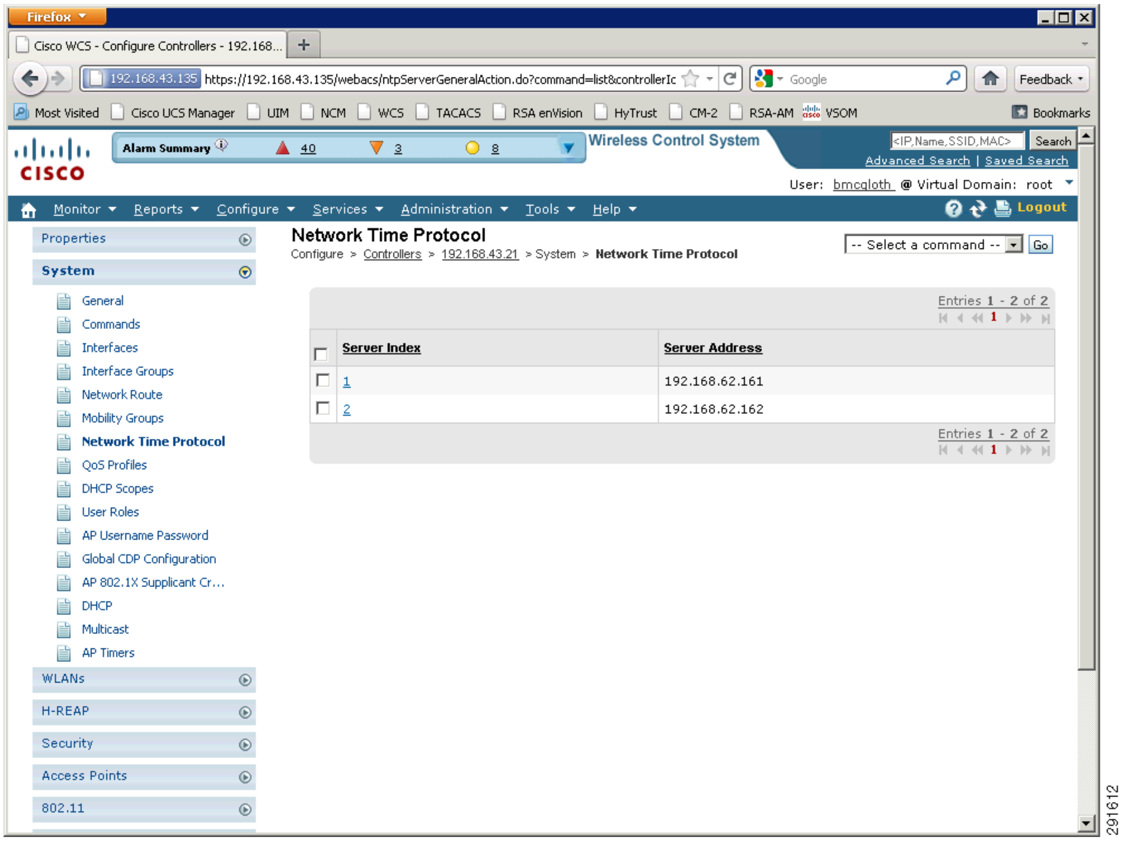
Cisco WCS uses the local clock facilities of the host server on which it is installed to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

Time synchronization for Windows servers is specified through the domain policy. Servers synchronize their clocks with the domain controller, which in turn is synchronized using NTP. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

A Network Time Protocol server can be configured within the Cisco WCS and Controllers to meet this requirement for all wireless devices, as shown in Figure 5-109.

*Figure 5-109 NTP Servers Screen for Controllers*



Network Time Protocol

Configure > Controllers > 192.168.43.21 > System > Network Time Protocol

| □ | Server Index | Server Address |
|---|---|---|
| □ | 1 | 192.168.62.161 |
| □ | 2 | 192.168.62.162 |

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

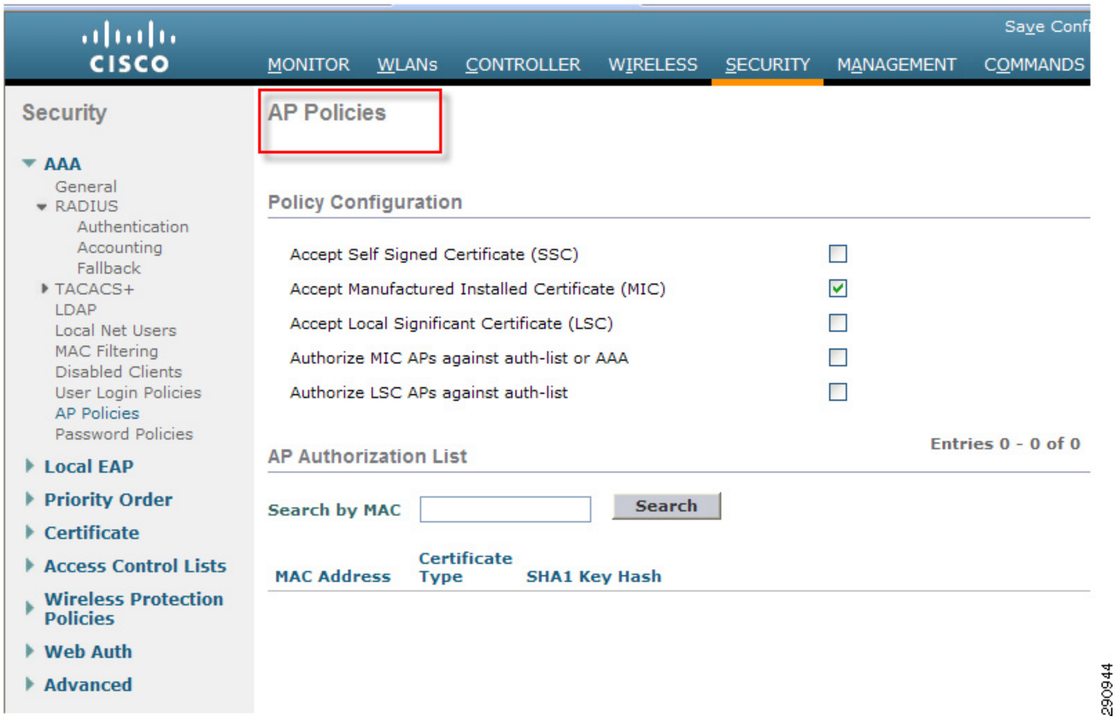
- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

## Requirement 11: Regularly Test Security Systems and Processes

- **PCI 11.1.b**—*Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:*
  - WLAN cards inserted into system components
  - Portable wireless devices connected to system components (for example, by USB, etc.)
  - Wireless devices attached to a network port or network device

  The Cisco WLAN performs 24-hour scanning to immediately detect and contain unauthorized and rogue wireless devices. Threats to network security can occur in between quarterly scans, creating the need to continuously scan and to use automatic alerts and containment mechanisms. Similarly, physical and/or port scanning on the wired network is not enough. Cisco Wireless LAN Controllers include wIPS and wIDS that find and stop rogue devices and attacks. WCS is a single point of management for WLAN devices, the mobility services engine, and mobility services. Cisco context-aware location services in the Cisco 3300 Series Mobility Services Engine (MSE) can locate multiple rogue devices. Cisco enhanced local mode (ELM) access points offer monitor mode wIPS on local mode access points for additional protection without a separate overlay network. Cisco CleanAir technology allows the detection and location of rogue devices on nonstandard Wi-Fi channels. (See Figure 5-110 and Figure 5-111.)

**Figure 5-110 Security—AP Policies Screen**



AP Policies

Policy Configuration

| | |
|---|---|
| Accept Self Signed Certificate (SSC) | □ |
| Accept Manufactured Installed Certificate (MIC) | ☑ |
| Accept Local Significant Certificate (LSC) | □ |
| Authorize MIC APs against auth-list or AAA | □ |
| Authorize LSC APs against auth-list | □ |

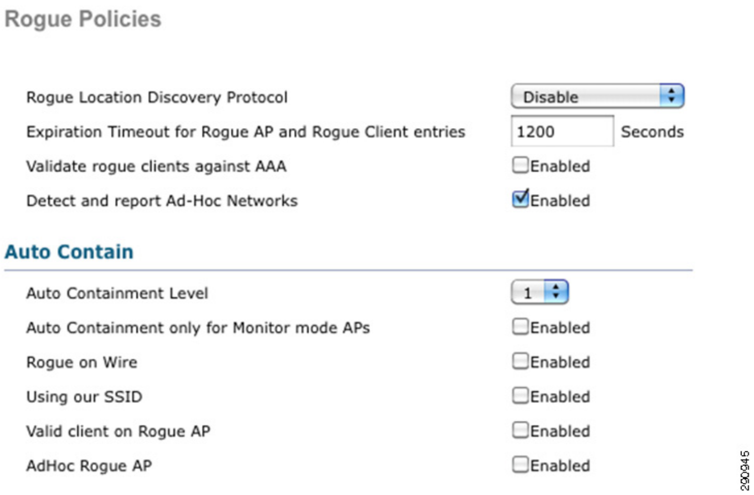
AP Authorization List

Entries 0 - 0 of 0

Search by MAC

| MAC Address | Certificate Type | SHA1 Key Hash |
|---|---|---|

**Figure 5-111 Rogue Policies Screen**



Rogue Policies

| | |
|---|---|
| Rogue Location Discovery Protocol | Disable |
| Expiration Timeout for Rogue AP and Rogue Client entries | 1200 Seconds |
| Validate rogue clients against AAA | □ Enabled |
| Detect and report Ad-Hoc Networks | ☑ Enabled |

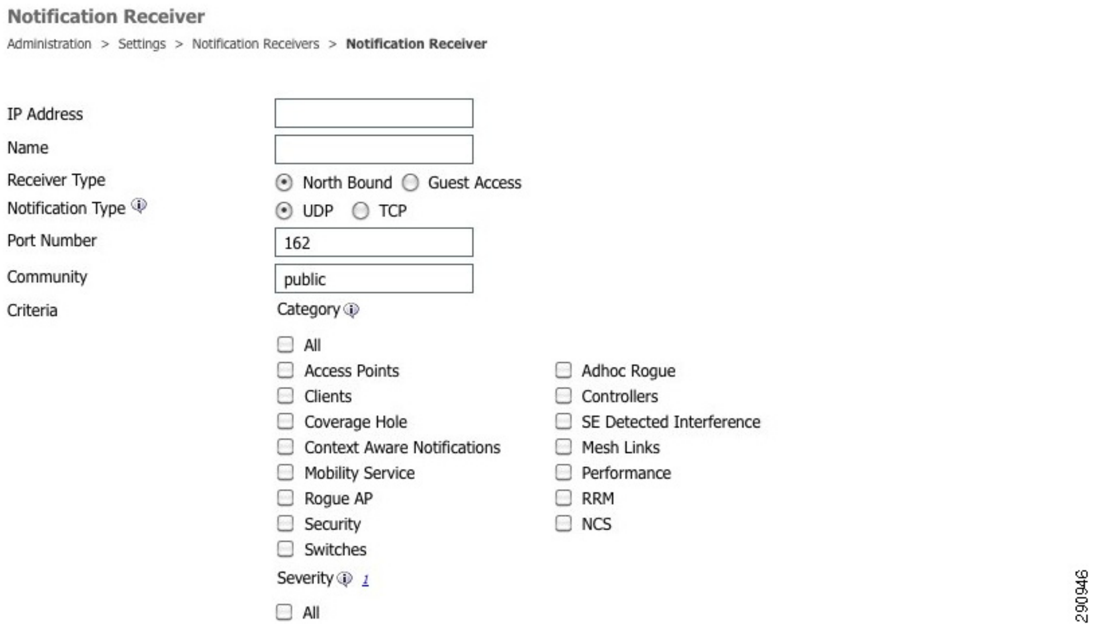
Auto Contain

| | |
|---|---|
| Auto Containment Level | 1 |
| Auto Containment only for Monitor mode APs | □ Enabled |
| Rogue on Wire | □ Enabled |
| Using our SSID | □ Enabled |
| Valid client on Rogue AP | □ Enabled |
| AdHoc Rogue AP | □ Enabled |

- **PCI 11.1.d**—*If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel.*

Cisco WCS has the ability to forward alerts to e-mail addresses. The system can forward all or selected alerts to multiple receivers. (See Figure 5-112.)

*Figure 5-112 Notification Receiver Screen*



Notification Receiver

Administration > Settings > Notification Receivers > **Notification Receiver**

| | |
|---|---|
| IP Address | |
| Name | |
| Receiver Type | ● North Bound ○ Guest Access |
| Notification Type | ● UDP ○ TCP |
| Port Number | 162 |
| Community | public |
| Criteria | Category |

□ All

□ Access Points
□ Clients
□ Coverage Hole
□ Context Aware Notifications
□ Mobility Service
□ Rogue AP
□ Security
□ Switches

□ Adhoc Rogue
□ Controllers
□ SE Detected Interference
□ Mesh Links
□ Performance
□ RRM
□ NCS

Severity

□ All

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

# Storage

## Cisco MDS Storage Switches

Cisco MDS storage switches provide the central switching infrastructure connecting servers to storage. They provide the added capability to encrypt all information on the fly between these systems for specified targets; specifically, the EMC storage array and Cisco UCS servers in the solution.

The Cisco MDS 9000 Series Multilayer SAN Switches can help lower the total cost of ownership of the most demanding storage environments. By combining robust and flexible hardware architecture with multiple layers of network and storage management intelligence, the Cisco MDS 9000 Series helps you build highly available, scalable storage networks with advanced security and unified management.

*Table 5-51 PCI Assessment Summary—Cisco MDS Storage Switches*

| **Models Assessed** | |
|---|---|
| MDS 9506 (“Supervisor/Fabric-2”) version m9500-sf2ek9-mzg.5.0.1a.bin.S4<br>MDS 9506 (“Supervisor/Fabric-2”) version m9500-sf2ek9-mz.5.0.4.bin | |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2.2, 2.2.4, 2.3 |
| **PCI 3** | 3.4.1, 3.5, 3.5.1, 3.5.2, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

## Primary PCI Function

The main function of Cisco MDS storage switches is to securely encrypt cardholder data at rest as it passes from server to storage. (3.4)

Table 5-51 lists the component assessment details for Cisco MDS storage switches.

*Table 5-52 Component Capability Assessment—Cisco MDS Storage Switches*

| Cisco MDS Storage Switches | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 3 (3.4)** |
| Securely encrypt cardholder data at rest. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

The MDS 9500s were configured for zoning and LUN masking to secure the logical partitioning of disk used for storing cardholder data. Only host machines in the data center that require access to that logical disk partition were allowed access. Configuration of the VSANs, host UUIDs, and mappings was partially performed using EMC Unified Infrastructure Manager as directed by the Vblock architecture by VCE. Vblock requires specific software versions and pre-configurations to be completed as specified in the Vblock preparation guide.

More information of Vblock designs can be found at the following URL:
http://www.vceportal.com/solutions/68580567.html#

Information in installing and configuring Cisco MDS can be found at the following URL:
http://www.cisco.com/en/US/products/hw/ps4159/ps4358/tsd_products_support_series_home.html

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

The Cisco MDS 9000 NX-OS Software does not use defaults for system passwords and other security parameters, but instead prompts the user for this information at power-up and can enforce the use of PCI-compliant passwords.

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  There are two ways to do this: initial setup, or configuration after the fact.

  1. Initial setup

```
 ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): yes
Do you want to enforce secure password standard (yes/no) [y]: yes
Create another login account (yes/no) [n]:
Configure read-only SNMP community string (yes/no) [n]: yes
Configure read-write SNMP community string (yes/no) [n]: yes
Enter the switch name :
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:
Mgmt0 IPv4 address :
Configure the default gateway? (yes/no) [y]:
IPv4 address of the default gateway :
Configure advanced IP options? (yes/no) [n]:
Enable the ssh service? (yes/no) [y]: yes
Type of ssh key you would like to generate (dsa/rsa) [rsa]:
Number of rsa key bits <768-2048> [1024]:
Enable the telnet service? (yes/no) [n]: no
Enable the http-server? (yes/no) [y]: no
Configure clock? (yes/no) [n]:
Configure timezone? (yes/no) [n]:
Configure summertime? (yes/no) [n]:
Configure the ntp server? (yes/no) [n]: yes
Configure default switchport interface state (shut/noshut) [shut]: shut
Configure default switchport trunk mode (on/off/auto) [on]:
Configure default switchport port mode F (yes/no) [n]: yes
Configure default zone policy (permit/deny) [deny]: deny
Enable full zoneset distribution? (yes/no) [n]:
Configure default zone mode (basic/enhanced) [basic]:
```

  2. By configuration after the fact

```
Configure terminal
Password strength-check
snmp-server community <password> ro
snmp-server community <password> rw
feature ssh
ssh key dsa or ssh key rsa <768-2048>
no feature telnet
no feature http-server
ntp server <ip address>
system default switchport shutdown
system default switchport mode f
no system default zone default-zone permit
```

  3. Additional

```
Secure access to management port:
ip access-list 23 permit ip 127.0.0.1 0.0.0.0 <mgmt port ip address> 0.0.0.0
ip access-list 23 permit ip <ip address of mgmt workstation> 0.0.0.0 <mgmt port ip
address> 0.0.0.0
ip access-list 23 permit ip <ip address of snmp workstation> 0.0.0.0 <mgmt port ip
address> 0.0.0.0
ip access-list 23 permit ip <ip address of AAA server> 0.0.0.0 <mgmt port ip
address> 0.0.0.0
ip access-list 23 permit ip <ip address of NTP workstation> 0.0.0.0 <mgmt port ip
address> 0.0.0.0
ip access-list 23 deny ip any any log-deny
interface mgmt0
ip address <ip address> <mask>
ip access-group 23 in
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  The Cisco MDS switch is a hardened device that does not allow changes to the operating system.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  The Cisco MDS switch uses SSL for web-based administrative and user access, and uses SSH for remote terminal access by implementing the configurations shown above.

#### Requirement 3: Protect Stored Cardholder Data

Cisco Storage Media Encryption (SME) provides protection of cardholder data by delivering disk and tape encryption. Cisco SME stores the keys in the Cisco key management server or in a secure third-party key manager such as RSA KM.

- **PCI 3.4.1**—*If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.*

  Although the Cisco MDS does not natively provide disk encryption (a feature normally found in software on a storage device), these switches provide the capability to encrypt all information on the fly between these systems for specified targets; specifically, the EMC storage array and Cisco UCS servers in the solution.

  The SME feature of the Cisco MDS 9000 SAN fabric is independent of the native operating system access control. Decryption keys are managed by the Cisco Key Manager, which is part of the SME feature. Keys are tied to individual tapes or LUNs, not to user accounts.

- **PCI 3.5**—*Protect any keys used to secure cardholder data against disclosure and misuse. Note: This requirement also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.*

  All keys are stored in encrypted form, and are always encrypted for transmission within the fabric.

- **PCI 3.5.1**—*Restrict access to cryptographic keys to the fewest number of custodians necessary.*

  Only recovery officers have access to the master key, stored in the PIN-protected smart cards. Only the key administrators have access to the disk and tape keys, stored in encrypted format in the Cisco Key Manager Center (KMC) or the RSA key manager.

- **PCI 3.5.2**—*Store cryptographic keys securely in the fewest possible locations and forms.*

Keys are stored in encrypted form in Cisco Key Manager, or stored by Cisco Key Manager in the RSA Key Manager. Both key managers provide for secure backup and recovery of keys, and for their secure storage in an alternate location. The master key is spread across multiple smart cards, each protected by a PIN chosen by the depository recovery officer.

- **PCI 3.6.1**—*Generation of strong cryptographic keys*

  The cryptographic keys (AES 256 bits) are generated by the encryption engine within the services node.

- **PCI 3.6.2**—*Secure cryptographic key distribution*

  The keys are never transmitted in clear text, but always using secure protocols (HTTPS and SSL).

- **PCI 3.6.3**—*Secure cryptographic key storage*

  Key-encrypting keys are stored in encrypted format in the Cisco KMC. Master keys are stored in PIN-encrypted format in the smart cards.

- **PCI 3.6.4**—*Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of ciphertext has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).*

  Cisco SME offers the capability to re-key and change keys as needed. Customers must enforce and document this procedure appropriately.

- **PCI 3.6.5**—*Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*

  Cisco KMC can manage the complete key lifecycle. Customers need to implement and document this procedure appropriately.

#### Requirement 6: Develop and Maintain Secure Systems and Applications

Cisco MDS 9000 NX-OS provides the capability to use a test VSAN to validate any new configuration before production. Cisco MDS 9000 NX-OS has also been developed with secure coding guidelines and is tested against common vulnerabilities.

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco MDS switches. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

Cisco MDS 9000 Family security features such as VSANs, advanced zoning, fabric binding, port security, Fibre Channel Security Protocol (FC-SP) authentication, and role-based access control (RBAC) with SNMPv3 and SSH make the Cisco MDS 9000 Family an excellent platform for enforcing this requirement. SSH RBAC in particular, if used in conjunction with VSANs, is especially designed to support tight partitioning of the physical infrastructure.

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS using TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- This is accomplished using the user role feature (see 7.2.2).
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- This is accomplished using the user role feature (see 7.2.2).
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*

The following configurations demonstrate how to configure the Cisco MDS for TACACS+ authentication to a central server.

```
Feature tacacs+

tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131

aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
aaa authorization ssh-certificate default group CiscoACS
aaa accounting default group CiscoACS
aaa authentication login error-enable
```

**Note** To configure LDAP authentication in NX-OS version 5.0 or higher, enable LDAP (**feature ldap**) and follow configuration steps in the Cisco MDS 9000 Family NX-OS Security Configuration Guide.

- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*

```
Feature privilege
    change admin user ID:
    username admin password <password> role network-admin (password will be 
encrypted when displayed)
    create network operator type user ID:
    username <assigned name> password <password> role network-operator (password 
will be encrypted when displayed)
    create default user ID:
    role name default-role
        description This is a system defined role and applies to all users.
        rule 5 permit show feature environment
        rule 4 permit show feature hardware
        rule 3 permit show feature module
        rule 2 permit show feature snmp
        rule 1 permit show feature system
    username <assigned name> password <password> role default-role (password will 
be encrypted when displayed)
    create custom user ID:
    role name <name>
        description User defined permissions define here:
        rule 1 permit show interface
        .
        .
        Rune 256 permit show module
    username <assigned name> password <password> role <name> (password will be 
encrypted when displayed)
```

- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  All user access is controlled by the user role function; there is no generic user access.

#### Requirement 8: Assign a Unique ID to Each Person with Computer Access

The Cisco MDS 9000 Family provides the capability to create an individual account for each administrator with a strong password. Authentication can be performed using the external authentication, authorization, and accounting (AAA) server of choice (for example, TACACS+) to implement the desired user authentication and password management policies.

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  To enforce session lengths, enable this using **terminal session-timeout** <*time in minutes*>.

  ```
  line vty
    exec-timeout 15
  line console
    exec-timeout 15
  ```

#### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

The Cisco MDS 9000 Family implements the Cisco Data Center Network Manager (DCNM), which continuously monitors the SAN and allows you to establish criteria and thresholds to generate real-time alarms and call-home functions. Syslog offers detailed entries and can be redirected to a log server to consolidate IT infrastructure monitoring information. Note that the log never contains application data.

Cisco MDS is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6—***Identity or name of affected data, system component, or resource.*

Cisco MDS uses the local clock facilities to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco MDS use NTP to meet these requirements by implementing the following configuration statements:

  ```
  clock timezone PST -8 0
  clock summer-time PST 1 Sun April 02:00 5 Sun Oct 02:00 60
  ntp server 192.168.62.161
  ```

```
ntp server 192.168.62.162
```

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  Cisco MDS is capable of sending system events to a centralized repository using the syslog function and SNMP traps. Logs stored locally are buffered and require operator level privileges on the router to be viewed. External logging and SNMP traps are enabled by implementing the following configuration statements:

  ```
  logging server 192.168.42.124 6
  ```

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

# Security

## Cisco ASA 5500 Series—Store

The Cisco ASA 5500 Series Adaptive Security Appliances provide secure segmentation within the store. Their stateful firewall and modular intrusion detection modules enable the store to securely connect public networks to the cardholder data environment.

The Cisco ASA 5500 Series delivers superior scalability, a broad span of technology and solutions, and effective, always-on security designed to meet the needs of a wide array of deployments. By integrating the world's most proven firewall; a comprehensive, highly effective intrusion prevention system (IPS) with Cisco Global Correlation and guaranteed coverage; high-performance VPN and always-on remote access, the Cisco ASA 5500 Series helps organizations provide secure, high performance connectivity and protects critical assets for maximum productivity.

The Cisco ASA 5500 Series includes the Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580, and 5585-X Adaptive Security Appliances-purpose-built, high-performance security solutions that take advantage of Cisco expertise in developing industry-leading, award-winning security and VPN solutions. Through Cisco Multi-Processor Forwarding (MPF), the Cisco ASA 5500 Series brings a new level of security and policy control to applications and networks. MPF enables highly customizable, flow-specific security policies that have been tailored to application requirements. The performance and extensibility of the Cisco ASA 5500 Series is enhanced through user-installable security service modules (SSMs). This adaptable architecture enables businesses to rapidly deploy security services when and where they are needed, such as tailoring inspection techniques to specific application and user needs or adding additional intrusion prevention and content security services such as those delivered by the Adaptive Inspection and Prevention (AIP) and Content Security and Control (CSC) SSMs. Furthermore, the modular hardware architecture of the Cisco ASA 5500 Series, along with the powerful MPF, provides the flexibility to meet future network and security requirements, extending the outstanding investment protection provided by the Cisco ASA 5500 Series and allowing businesses to adapt their network defenses to new threats as they arise.

All Cisco ASA 5500 Series appliances offer both IPsec and SSL/DTLS VPN solutions; clientless and AnyConnect VPN features are licensed at various price points, on a per-seat and per-feature basis. By converging SSL and IPsec VPN services with comprehensive threat defense technologies, the Cisco ASA 5500 Series provides highly customizable, granular network access tailored to meet the requirements of diverse deployment environments, while providing advanced endpoint and network-level security.

*Table 5-53 PCI Assessment Summary—Cisco ASA 5500 Series (Store)*

| **Models Assessed** | |
|---|---|
| Cisco ASA5510 w/SSM-10 version asa841-k8.bin and IDS version 7.0(4) | |
| **PCI Sub-Requirements Passed** | |
| **PCI 1** | 1.2.1, 1.2.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8 |
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 4** | 4.1 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3 |
| **PCI 11** | 11.4 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

## Primary PCI Function

The main function of the store Cisco ASA firewall is to securely segment public and cardholder data environment store networks, and provide intrusion detection capabilities. (1.2, 1.3, 11.4)

Table 5-53 lists the component assessment details for the Cisco ASA 5500 Series.

*Table 5-54 Component Capability Assessment—Cisco ASA 5500 Series (Store)*

| Cisco ASA 5500 Series (Store) | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 1, 11 (1.2, 1.3, 11.4)** |
| Segment public and cardholder data environment networks within the store. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

- Select the appropriate Cisco ASA model and SSM module for the traffic needs in the store.
- Connect the SSM module to the secure management segment of the store network using the external Ethernet interface.
- Configure security policies, objects, and rules centrally with Cisco Security Manager.

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.1**—*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*

  Cisco ASA firewalls are configurable to restrict traffic through the use of object and service-based access lists. By default, the firewall does not forward any traffic unless explicitly permitted.

- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

  Firewall configuration files are backed up centrally using EMC Ionix Network Configuration Manager (NCM). This tool also verifies that running and startup configurations of firewalls, routers, and switches are synchronized. Additionally, Cisco Security Manager stores a copy of the firewall configuration for the policies that it manages.

- **PCI 1.2.3**—*Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.*
- **PCI 1.3.1**—*Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.*
- **PCI 1.3.2**—*Limit inbound Internet traffic to IP addresses within the DMZ.*
- **PCI 1.3.3**—*Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.*
- **PCI 1.3.4**—*Do not allow internal addresses to pass from the Internet into the DMZ.*
- **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*
- **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*
- **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*
- **PCI 1.3.8**—*Do not disclose private IP addresses and routing information to unauthorized parties.*

The following configuration example shows how objects identify hosts and services within the network and their use in an access list to permit approved traffic:

```
!
interface Ethernet0/0
 nameif MSP-WAN
 security-level 0
 ip address 10.10.255.176 255.255.255.0
!
interface Ethernet0/1.1000
 vlan 1000
 nameif MANAGEMENT
 security-level 100
 ip address 10.10.191.1 255.255.255.0
!
! ----Defining Objects and Object Groups----
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 network-object 192.168.42.122 255.255.255.255
object-group network CSManager
 description Cisco Security Manager
 network-object 192.168.42.133 255.255.255.255
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 network-object 192.168.42.124 255.255.255.255
object-group network AdminStation3
 network-object 192.168.42.138 255.255.255.255
object-group network POS-Store-MSP
 network-object 10.10.176.81 255.255.255.255
!
object-group service CSM_INLINE_svc_rule_73014461184
 description Generated by CS-Manager from service of FirewallRule# 4
(ASA-Store_V2/mandatory)
 service-object tcp destination eq https
 service-object tcp destination eq ssh
 service-object object ORACLE-OAS
 service-object object TOMAX-8990
 group-object ORACLE-RMI
 group-object ORACLE-Weblogic
 group-object ORACLE-WAS
 group-object HTTPS-8443
!
object-group network CSM_INLINE_src_rule_73014461184
 description Generated by CS-Manager from src of FirewallRule# 4
(ASA-Store_V2/mandatory)
 group-object DC-POS-Tomax
 network-object object DC-POS
 group-object DC-POS-SAP
 group-object DC-POS-Oracle
!
! ----One line of the larger access-list permitting traffic----
!
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461184
object-group CSM_INLINE_src_rule_73014461184 object-group POS-Store-MSP
!
! ----Applying the access-list to an interface----
!
access-group OUTSIDE in interface MSP-WAN
```

#### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco ASA firewalls allow only administrative connections from authorized hosts/networks, as specified in the device configuration. The HTTP server supports only secure connections using SSL. If no hosts or networks are specified for the service, it is effectively disabled (for example, the Telnet service). The following configuration shows the authorized management hosts for SSH and HTTPS administration, and none for Telnet.

```
http server enable
http 10.19.151.99 255.255.255.255 north
http 192.168.41.101 255.255.255.255 south
http 192.168.41.102 255.255.255.255 south
http 192.168.42.122 255.255.255.255 south
http 192.168.42.124 255.255.255.255 south
http 192.168.42.133 255.255.255.255 south
http 192.168.42.138 255.255.255.255 south
telnet timeout 5
ssh 10.19.151.99 255.255.255.255 north
ssh 192.168.41.101 255.255.255.255 south
ssh 192.168.41.102 255.255.255.255 south
ssh 192.168.42.122 255.255.255.255 south
ssh 192.168.42.124 255.255.255.255 south
ssh 192.168.42.133 255.255.255.255 south
ssh 192.168.42.138 255.255.255.255 south
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco ASA firewalls do not have any unnecessary services enabled by default.
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

Cisco ASA firewalls support strong encryption for SSH and HTTPS. The following configurations are used to configure strong cryptography:

```
! ---Specify only Strong algorithms for SSL connections---
!
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1
!
! ---Specify strong encryption version of SSH
!
ssh version 2
!
```

### Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*
  - *The Internet*
  - *Wireless technologies,*
  - *Global System for Mobile communications (GSM)*
  - *General Packet Radio Service (GPRS)*

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco ASA Firewalls. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at: http://www.cisco.com/cisco/software/navigator.html

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS using TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*

- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco ASAs are configured to use a AAA model for user-based access. Users can be assigned to groups and, based on privilege levels, have access to only the information they require for their job function. By default in Cisco ASA, no users are allowed access unless specifically configured and assigned appropriate passwords.

```
aaa-server RETAIL protocol tacacs+
aaa-server RETAIL (MANAGEMENT) host 192.168.42.131
 key <removed>
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
```

  Local user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username csmadmin password <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
```

  These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
aaa authentication enable console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
aaa authentication ssh console RETAIL LOCAL
```

#### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services as shown in Requirement 7.

The Cisco ASA is able to meet some of the requirements locally, as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco ASA supports the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

```
username csmadmin password <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  Local user accounts on Cisco ASA require setting of a password.

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  In addition to the use of strong MD5-encrypted hashing of locally stored passwords, Cisco ASA also supports the use of AES encryption of pre-shared keys.

```
password encryption aes
```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco ASAs do not support an automated capability to perform this function at this time; the user account would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Security Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco ASA does not support an automated capability to perform this function at this time; user passwords would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using Cisco Security Manager.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco ASA does not support the ability to specify a minimum password length for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco ASA does not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco ASA does not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

  **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco ASA management interfaces are configured as follows to meet this requirement:

  ```
  http server idle-timeout 15
  ssh timeout 15
  ```

#### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco ASA 5500 is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*

- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*

  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*

  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco ASA uses the local clock facilities meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers. Cisco ASA use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.162 source MSP-WAN
ntp server 192.168.62.161 source MSP-WAN prefer
clock timezone PST -8
clock summer-time PDT recurring
```

Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  Cisco ASA is capable of sending system events to a centralized repository using the syslog function and SNMP traps. Logs stored locally are buffered and require operator level privileges on the router to be viewed. External logging and SNMP traps are enabled by implementing the following configuration statements:

```
logging enable
logging trap debugging
logging asdm debugging
logging host MSP-WAN 192.168.42.124
```

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

## Cisco ASA 5500 Series—Data Center

As a core component of Cisco Borderless Networks, Cisco ASA 5500 Series Adaptive Security Appliances provide:

- Context-aware firewall capabilities
- Proven firewall services
- Comprehensive real-time threat defense
- Effective, always-on, highly secure remote access
- Highly secure communication services

These solutions help reduce deployment and operational costs while delivering comprehensive network security for networks of all sizes.

Context-aware firewalling capabilities combine:

- In-depth local network context from TrustSec
- Real-time global threat intelligence from Cisco Security Intelligence Operations (SIO)
- Unique mobile client insight from AnyConnect

In addition, these solutions offer an advanced intrusion prevention system (IPS) with Global Correlation, which is twice as effective as a traditional IPS and includes Cisco guaranteed coverage.

*Table 5-55 PCI Assessment Summary—Cisco ASA 5500 Series (Data Center)*

| **Models Assessed** | |
|---|---|
| ASA5540 w/SSM-40 | asa841-k8.bin |
| ASA5540 w/SSM-20 | asa841-k8.bin |
| ASA5585-S60-2A-K9 | asa824-smp-k8.bin |
| **PCI Sub-Requirements Passed** | |
| **PCI 1** | 1.2.1, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8 |
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 4** | 4.1 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.3, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2.1, 10.2.2,10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.1, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3 |
| **PCI 11** | 11.4 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |

*Table 5-55 PCI Assessment Summary—Cisco ASA 5500 Series (Data Center) (continued)*

| |
|---|
| No compensating controls were required to satisfy any sub-requirements. |
| **PCI Sub-Requirements Failed** |
| No sub-requirements were failed. |

## Primary PCI Function

The primary functions of the data center firewalls are twofold. They operate as a firewall, restricting traffic between the cardholder data environment and other areas of the network; and they operate as an intrusion prevention system, inspecting all traffic going to and from the cardholder data environment. These controls map directly to satisfying a number of PCI sub-requirements including Requirements 1, 2, 4, 7, 8, 10, and 11. The following is a description of how each of the PCI sub-requirements is satisfied for store routers.

Table 5-55 lists the component assessment details for Cisco ASA 5500 Series.

*Table 5-56 Component Capability Assessment —Cisco ASA 5500 Series (Data Center)*

| Cisco ASA 5500 Series (Data Center) | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 1, 11 (1.2, 1.3, 11.4)** |
| Restrict traffic between the cardholder data environment and other network areas, and as an IPS. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***“Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

- Implementing Cisco ASA firewalls in transparent mode helps reduce network complexity.

- IDS/IPS modules require the external network interface port to be connected to the network for management and automated reporting and alerts to be sent.
- When configuring high availability, only the primary Cisco ASA needs to be fully configured; the secondary Cisco ASA mirrors the primary's configurations once the failover interface and IP information are configured.
- Cisco Adaptive Security Device Manager (ADSM) is a good tool for making policy changes in small environments. For large enterprises, Cisco Security Manager provides the best platform for managing rules with a large number of objects across many devices.
- Multi-context firewalls allow for traffic and administrative segmentation.
- Firewall rule sets must adhere to a "least amount of access necessary" policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports required for the cardholder data environment (for example, point-of-sale) networks.
- Configure the primary login authentication of the Cisco ASA to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the Cisco ASA itself in the event of a WAN or Cisco Secure ACS failure.
- Configure logs to be sent to a centralized syslog server such as RSA enVision.
- Configure NTP to ensure all logging is coordinated
- Cisco ASA firewalls were used for the store WAN, Internet edge, and data center aggregation block.

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.1**—*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*

  Cisco ASA firewalls are configurable to restrict traffic through the use of object and service-based access lists. By default, the firewall does not forward any traffic unless explicitly permitted.
- **PCI 1.3.1**—*Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.*
- **PCI 1.3.2**—*Limit inbound Internet traffic to IP addresses within the DMZ.*
- **PCI 1.3.3**—*Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.*
- **PCI 1.3.4**—*Do not allow internal addresses to pass from the Internet into the DMZ.*
- **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*
- **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*
- **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*
- **PCI 1.3.8**—*Do not disclose private IP addresses and routing information to unauthorized parties.*

  The following configuration example shows how objects identify hosts and services within the network and their use in an access list to permit approved traffic:

```
!
! ----Naming of interfaces as assigned from the Admin Context----
!
```

```
interface outside
 nameif north
 bridge-group 1
 security-level 0
!
interface inside
 nameif south
 bridge-group 1
 security-level 100
!
! ----Defining Objects and Object Groups----
!
object-group network EMC-NCM
 description EMC Network Configuration Manager
 network-object 192.168.42.122 255.255.255.255
object-group network CSManager
 description Cisco Security Manager
 network-object 192.168.42.133 255.255.255.255
object-group network RSA-enVision
 description RSA EnVision Syslog collector and SIM
 network-object 192.168.42.124 255.255.255.255
object-group network AdminStation3
 network-object 192.168.42.138 255.255.255.255
object-group network Admin-Systems
 group-object EMC-NCM
 group-object AdminStation
 group-object AdminStation2
 group-object CSManager
 group-object RSA-enVision
 group-object AdminStation3
 group-object AdminStation4-bart
!
object-group service CSM_INLINE_svc_rule_77309411635
 description Generated by CS-Manager from service of FirewallRule# 3 
(ASA-DC-1-vdc1_v1/mandatory)
 service-object tcp destination eq ssh
 service-object tcp destination eq https
 group-object HTTPS-8443
!
object-group network CSM_INLINE_dst_rule_77309411635
 description Generated by CS-Manager from dst of FirewallRule# 3 
(ASA-DC-1-vdc1_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
 group-object DC-DMZ
!
! ----One line of the larger access-list permitting traffic----
!
access-list CSM_FW_ACL_south extended permit object-group 
CSM_INLINE_svc_rule_77309411635 object-group Admin-Systems object-group 
CSM_INLINE_dst_rule_77309411635
!
! ----Applying the access-list to an interface----
!
access-group CSM_FW_ACL_south in interface south
```

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco ASA firewalls allow only administrative connections from authorized hosts/networks, as specified in the device configuration. The HTTP server supports only secure connections using SSL. If no hosts or networks are specified for the service, it is effectively disabled (for example, the Telnet service). The following configuration shows the authorized management hosts for SSH and HTTPS administration, and none for Telnet.

```
http server enable
http 10.19.151.99 255.255.255.255 north
http 192.168.41.101 255.255.255.255 south
http 192.168.41.102 255.255.255.255 south
http 192.168.42.122 255.255.255.255 south
http 192.168.42.124 255.255.255.255 south
http 192.168.42.133 255.255.255.255 south
http 192.168.42.138 255.255.255.255 south
telnet timeout 5
ssh 10.19.151.99 255.255.255.255 north
ssh 192.168.41.101 255.255.255.255 south
ssh 192.168.41.102 255.255.255.255 south
ssh 192.168.42.122 255.255.255.255 south
ssh 192.168.42.124 255.255.255.255 south
ssh 192.168.42.133 255.255.255.255 south
ssh 192.168.42.138 255.255.255.255 south
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco ASA firewalls do not have any unnecessary services enabled by default.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco ASA firewalls support strong encryption for SSH and HTTPS. The following configurations are used to configure strong cryptography:

```
! ---Specify only Strong algorithms for SSL connections---
!
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1
!
! ---Specify strong encryption version of SSH
!
ssh version 2
!
```

#### Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*
  - *The Internet*
  - *Wireless technologies,*
  - *Global System for Mobile communications (GSM)*
  - *General Packet Radio Service (GPRS)*

### Requirement 6: Develop and Maintain Secure Systems and Applications

**PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco ASA firewalls. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

Software support for all Cisco products can be located at:
http://www.cisco.com/cisco/software/navigator.html.

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

To meet all of the requirements listed below, the PCI solution for retail uses a centralized user database in the Active Directory, which is linked via LDAP, RADIUS, and TACACS+ services. This server is located in the data center. Individual user IDs are assigned, and roles are based on group membership. This resource is used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

Cisco ASA firewalls are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default in Cisco ASA firewalls, no users are allowed access unless specifically configured and assigned appropriate passwords. The following configuration statements create an authentication group called *RETAIL*, which is assigned to various interfaces. This group uses the TACACS+ protocol to communicate with the Cisco ACS server where individual user groups and roles are configured, limiting and logging access as appropriate.

```
aaa-server RETAIL protocol tacacs+
aaa-server RETAIL (south) host 192.168.42.131
 key *****
aaa authentication ssh console RETAIL LOCAL
aaa authentication enable console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
aaa accounting ssh console RETAIL
aaa accounting enable console RETAIL
aaa accounting command privilege 15 RETAIL
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
aaa authorization exec authentication-server
```

Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username csmadmin password <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
```

These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
aaa authentication ssh console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
```

#### Requirement 8: Assign a Unique ID to Each Person with Computer Access

For Cisco firewalls to meet all of the user access restrictions specified in Requirement 8, an external authentication service such as Cisco Secure Access Control Server must be implemented. Configure AAA services as shown above in requirement 7.

The firewall is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco firewalls support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

  ```
  username csmadmin password <removed> encrypted privilege 15
  username retail password <removed> encrypted privilege 15
  username bmcgloth password <removed> encrypted privilege 15
  ```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*

  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  When configuring local user accounts, you must specify a password to achieve PCI compliance. Do not use the “nopassword” option.

  ```
  username csmadmin password <removed> encrypted privilege 15
  username retail password <removed> encrypted privilege 15
  username bmcgloth password <removed> encrypted privilege 15
  ```

- **PCI 8.3**—*Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) Note: Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.*

  Using AAA services, Cisco ASA firewalls can support two-factor authentication by pointing to an external authentication server (as described in Requirement 7). In the test environment, a second authentication service was set up using RSA Access Manager and SecurID tokens for generating one-time passwords. The following configurations show the setup of the additional AAA RADIUS server and authentication group for SSL VPN access from external sources.

```
aaa-server partnerauth protocol radius
aaa-server partnerauth (inside) host 192.168.42.137
 timeout 5
 key *****
 radius-common-pw *****

webvpn
 enable outside
 internal-password enable
 smart-tunnel list AllExternalApplications All-Applications * platform windows
group-policy DfltGrpPolicy attributes
 webvpn
  url-list value page1
  smart-tunnel enable AllExternalApplications
group-policy Retail-PCI internal
group-policy Retail-PCI attributes
 vpn-tunnel-protocol ssl-clientless
!
tunnel-group DefaultRAGroup general-attributes
 authentication-server-group partnerauth
tunnel-group DefaultWEBVPNGroup general-attributes
 authentication-server-group partnerauth
tunnel-group Retail-Lab type remote-access
tunnel-group Retail-Lab general-attributes
 authentication-server-group partnerauth LOCAL
 default-group-policy Retail-PCI
```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  All local passwords on the firewall are stored using strong encryption. Additionally, the following command can be used to encrypt local keys:

  ```
  key config-key password-encryption
  password encryption aes
  ```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco ASA firewalls do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager or Cisco Security Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco ASA firewalls do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager or Cisco Security Manager.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco ASA firewalls do not support the ability to specify a minimum password length for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco ASA firewalls do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

Cisco ASA firewalls do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco ASA firewalls do not support the ability to lock out users due to failed login attempts for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco ASA firewalls do not support the ability to lock out users due to failed login attempts for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco ASA firewalls are able to time-out administrative sessions using the following configuration statements:

  ```
  !
  http server idle-timeout 15
  !
  ssh timeout 15
  !
  console timeout 15
  ```

#### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco ASA firewalls are able to track and monitor all administrative user access, events such as interface up/down, dropped or filtered traffic, device authentications, and VPN sessions, to name a few.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco ASA firewalls track individual administrator actions as identified in the requirements above (10.1, 10.2 and 10.3) through several mechanisms including AAA, logging, and system events by implementing the following configuration statements:

```
logging enable
logging trap debugging
logging asdm debugging
logging host inside 192.168.42.124
```

Cisco ASA firewalls use NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.1**—*Critical systems have the correct and consistent time.*
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP server was hosted at the data center site. Cisco ASA firewalls use NTP to meet these requirements by implementing the following configuration statements:

```
ntp server 192.168.62.162 source inside
ntp server 192.168.62.161 source inside prefer

clock timezone PST -8
clock summer-time PDT recurring
```

To learn more about NTP, visit:
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

**Note** The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

To meet all of the requirements listed below, the PCI solution for retail uses a central logging repository located in the data center. RSA enVision collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

## Cisco Firewall Services Module (FWSM)—Data Center

The Cisco Firewall Services Module (FWSM) is an integrated module installed inside a Cisco Catalyst 6500 Series Switch or Cisco 7600 Internet Router. The Cisco FWSM allows any port on the Cisco Catalyst switch to operate as a firewall port and integrates firewall security inside the network infrastructure.

The Cisco FWSM includes a number of advanced features that help reduce costs and operational complexity while enabling organizations to manage multiple firewalls from the same management platform. Features such as the resource manager help organizations limit the resources allocated to any security context at any time, thus ensuring that one security context does not interfere with another. The transparent firewall feature configures the Cisco FWSM to act as a Layer 2 bridging firewall, resulting in minimal changes to network topology.

*Table 5-57 PCI Assessment Summary—Cisco FWSM*

| **Models Assessed** | |
|---|---|
| WS-SVC-FWM version c6svc-fwm-k9.4-1-5.bin | |
| **PCI Sub-Requirements Passed** | |
| **PCI 1** | 1.2.1, 1.2.2, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.3.8 |
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 4** | 4.1 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

### Primary PCI Function

The primary function of the Cisco FWSM is to restrict traffic between the cardholder data environment and other areas of the network (1.2, 1.3).

Table 5-57 lists the component assessment details for the Cisco FWSM.

*Table 5-58 Component Capability Assessment—Cisco FWSM*

| Cisco FWSM | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 1 (1.2, 1.3)** |
| Restrict traffic between the cardholder data environment and other network areas. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

- Firewall rule sets must adhere to a "least amount of access necessary" policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports.
- For Internet edge, disable **icmp permit** on the outside interface of Cisco FWSM. If users need to access servers in the DMZ segment, make sure that external users can reach the servers using very specific protocol and ports.
- Configure the **ip verify reverse path** command on all interfaces to provide anti-spoofing functionality.
- Configure the console timeout commands to 15 minutes or less on the console of the Cisco FWSM.
- Configure appropriate banner messages on login, incoming, and exec modes of the Cisco FWSM. The login banner warning should not reveal the identity of the company that owns or manages the Cisco FWSM. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the Cisco FWSM to be directed to the Cisco Secure ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the Cisco FWSM itself in the event of connectivity or Cisco Secure ACS failure.
- Change default passwords and community strings to appropriate complexity.

- Allow only SSHv2 (and not Telnet or SSHv1) connection from network management station to Cisco FWSM.

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2.1**—*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*

  Cisco FWSM firewalls are configurable to restrict traffic through the use of object and service-based access lists. By default, the firewall does not forward any traffic unless explicitly permitted.

- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

  Firewall configuration files are backed up centrally using EMC Ionix Network Configuration Manager (NCM). This tool also verifies that running and startup configurations of firewalls, routers, and switches are synchronized. Additionally, Cisco Security Manager stores a copy of the firewall configuration for the policies that it manages.

- **PCI 1.3**—*Prohibit direct public access between the Internet and any system component in the cardholder data environment.*

  Cisco FWSM firewalls track and monitor the state of communications and are configurable to restrict traffic through the use of object and service-based access lists. By default, the firewall does not forward any traffic unless explicitly permitted. FWSM firewalls have multiple interfaces and VLAN support, allowing for segmentation of traffic and the creation of DMZ zones or areas with differing security policies. Cisco ASA firewalls can also perform NAT to aid in securing/obscuring the private IP addressing information used within an enterprise.

  - **PCI 1.3.1**—*Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.*
  - **PCI 1.3.2**—*Limit inbound Internet traffic to IP addresses within the DMZ.*
  - **PCI 1.3.3**—*Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.*
  - **PCI 1.3.4**—*Do not allow internal addresses to pass from the Internet into the DMZ.*
  - **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*
  - **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*
  - **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*
  - **PCI 1.3.8**—*Do not disclose private IP addresses and routing information to unauthorized parties.*

  The following configuration example shows how objects identify hosts and services within the network and their use in an access list to permit approved traffic:

```
!
! ----VLAN's assigned from the Host Catalyst Switch----
!
interface Vlan21
 nameif inside
 security-level 100
 ip address 192.168.21.10 255.255.255.0
!
```

```
interface Vlan22
 nameif outside
 security-level 0
 ip address 192.168.22.1 255.255.255.0 standby 192.168.22.2
!!
! ----Defining Objects and Object Groups----
!
object-group network DC-ALL
 description All of the Data Center
 network-object 192.168.0.0 255.255.0.0
object-group network Stores-ALL
 description all store networks
 network-object 10.10.0.0 255.255.0.0
!
object-group service CSM_INLINE_svc_rule_81604379580 tcp
 description Generated by CS-Manager from service of FirewallRule# 7 
(FWSM-DMZ-1_v1/mandatory)
 port-object eq smtp
 port-object eq https
 port-object eq ssh
!
object-group network CSM_INLINE_src_rule_81604379580
 description Generated by CS-Manager from src of FirewallRule# 7 
(FWSM-DMZ-1_v1/mandatory)
 group-object DC-ALL
 group-object Stores-ALL
!
! ----One line of the larger access-list permitting traffic----
!
access-list INSIDE extended permit tcp object-group CSM_INLINE_src_rule_81604379580 
192.168.23.64 255.255.255.224 object-group CSM_INLINE_svc_rule_81604379580
!
! ----Applying the access-list to an interface----
!
access-group INSIDE in interface inside
```

#### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

  Cisco FWSM firewalls allow only administrative connections from authorized hosts/networks, as specified in the device configuration. The HTTP server supports only secure connections using SSL. If no hosts or networks are specified for the service, it is effectively disabled (for example, the Telnet service). The following configuration shows the authorized management hosts for SSH and HTTPS administration, and none for Telnet.

```
http server enable
http 10.19.151.99 255.255.255.255 north
http 192.168.41.101 255.255.255.255 south
http 192.168.41.102 255.255.255.255 south
http 192.168.42.122 255.255.255.255 south
http 192.168.42.124 255.255.255.255 south
http 192.168.42.133 255.255.255.255 south
http 192.168.42.138 255.255.255.255 south

ssh 10.19.151.99 255.255.255.255 north
ssh 192.168.41.101 255.255.255.255 south
ssh 192.168.41.102 255.255.255.255 south
ssh 192.168.42.122 255.255.255.255 south
ssh 192.168.42.124 255.255.255.255 south
ssh 192.168.42.133 255.255.255.255 south
ssh 192.168.42.138 255.255.255.255 south
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco FWSM firewalls do not have any unnecessary services enabled by default.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco FWSM firewalls support strong encryption for SSH and HTTPS. The following configurations are used to configure strong cryptography:

  ```
  !
  ! ---Specify strong encryption version of SSH
  !
  ssh version 2
  !
  ```

### Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- **PCI 4.1**—*Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*
  - *The Internet*
  - *Wireless technologies,*
  - *Global System for Mobile communications (GSM)*
  - *General Packet Radio Service (GPRS)*

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco FWSM modules. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS TACACS+ services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*

- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco FWSM firewalls are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default in Cisco FWSM firewalls, no users are allowed access unless specifically configured and assigned appropriate passwords. The following configuration statements create an authentication group called *RETAIL*, which is assigned to various interfaces. This group uses the TACACS+ protocol to communicate with the Cisco ACS server where individual user groups and roles are configured, limiting and logging access as appropriate.

```
aaa-server RETAIL protocol tacacs+
aaa-server RETAIL (south) host 192.168.42.131
 key <removed>
aaa authentication ssh console RETAIL LOCAL
aaa authentication enable console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
aaa accounting ssh console RETAIL
aaa accounting enable console RETAIL
aaa accounting command privilege 15 RETAIL
aaa authentication secure-http-client
aaa local authentication attempts max-fail 6
aaa authorization exec authentication-server
```

  Local individual user accounts are configured in the event that the centralized authentication server cannot be reached. These accounts must be manually updated to maintain compliance requirements regarding password rotation and expiration as specified in PCI Requirement 8.

```
username csmadmin password <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
```

  These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
aaa authentication ssh console RETAIL LOCAL
aaa authentication http console RETAIL LOCAL
```

#### Requirement 8: Assign a Unique ID to Each Person with Computer Access

For Cisco firewalls to meet all of the user access restrictions specified in Requirement 8, an external authentication service such as Cisco Secure Access Control Server must be implemented. Configure AAA services as shown above in requirement 7.

The firewall is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco firewalls support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

```
username csmadmin password <removed> encrypted privilege 15
username retail password <removed> encrypted privilege 15
username bmcgloth password <removed> encrypted privilege 15
```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*

  When configuring local user accounts, you must specify a password to achieve PCI compliance. Do not use the "nopassword" option.

  ```
  username csmadmin password <removed> encrypted privilege 15
  username retail password <removed> encrypted privilege 15
  username bmcgloth password <removed> encrypted privilege 15
  ```

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  All local passwords on the firewall are stored using strong encryption. Additionally, the following command can be used to encrypt local keys:

  ```
  password encryption aes
  ```

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

  Cisco FWSM firewalls do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager or Cisco Security Manager.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco FWSM firewalls do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days. This capability could be performed centrally through the device configurations management using EMC Ionix Network Configuration Manager or Cisco Security Manager.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco FWSM firewalls do not support the ability to specify a minimum password length for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco FWSM firewalls do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco FWSM firewalls do not support an automated capability to perform this function at this time; user account creation would have to follow this policy manually.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco FWSM firewalls do not support the ability to lock out users due to failed login attempts for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco FWSM firewalls do not support the ability to lock out users due to failed login attempts for local accounts. This would have to be met through a compensating control and corporate policy if a centralized authentication service with this capability could not be used.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco FWSM firewalls are able to time-out administrative sessions using the following configuration statements:

  ```
  !
  http server idle-timeout 15
  !
  ssh timeout 15
  !
  console timeout 15
  ```

#### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco FWSM firewalls are able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco FWSM firewalls use the local clock facilities of the host Cisco Catalyst chassis to meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

To meet all of the requirements listed below, the PCI solution for retail uses a central logging repository located in the data center. RSA enVision collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

## Cisco Virtual Security Gateway

The Cisco Virtual Security Gateway (VSG) for Cisco Nexus 1000V Series Switches was used in the data center for setting a boundary between the sensitive scope of the retailer's cardholder data environment and out-of-scope networks. It is a virtual firewall for Cisco Nexus 1000V Series Switches that delivers security and compliance for virtual computing environments. Cisco VSG uses virtual service data path (vPath) technology embedded in the Cisco Nexus 1000V Series Virtual Ethernet Module (VEM), offering transparent firewall insertion and efficient deployment. All the policy management for VSG is done via Virtual Network Management Center (VNMC). Cisco VSG provides the following:

- Zone-based security controls based on network as well as virtual machine attributes. This flexibility simplifies security policies, which are easy to troubleshoot and audit.
- Secure multi-tenant deployment, protecting tenant workloads on a shared compute infrastructure.
- Leverages vPath intelligence for efficient network-wide deployment and accelerated performance through fast-path off-load.
- IT security, network, and server teams to collaborate while helping ensure administrative segregation to meet regulatory and audit requirements and reduce administrative errors.

### Primary PCI Function

The main function of the Cisco VSG is segmentation of PCI scope and enforcement of that new scope boundary. The Cisco VSG serves as a stateful firewall, restricting traffic between the cardholder data environment and other areas of the network. (1.2, 1.3)

*Table 5-59 PCI Assessment Summary—Cisco VSG*

| **Models Assessed** | |
|---|---|
| Nexus VSG version 4.2(1)VSG1(1) | |
| **PCI Sub-Requirements Passed** | |
| **PCI 1** | 1.2.1, 1.2.2, 1.3.5, 1.3.6, 1.3.7 |
| **PCI 2** | 2.2, 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3, 10.5.5 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

Table 5-59 lists the component assessment details for the Cisco VSG.

*Table 5-60 Component Capability Assessment—Cisco VSG*

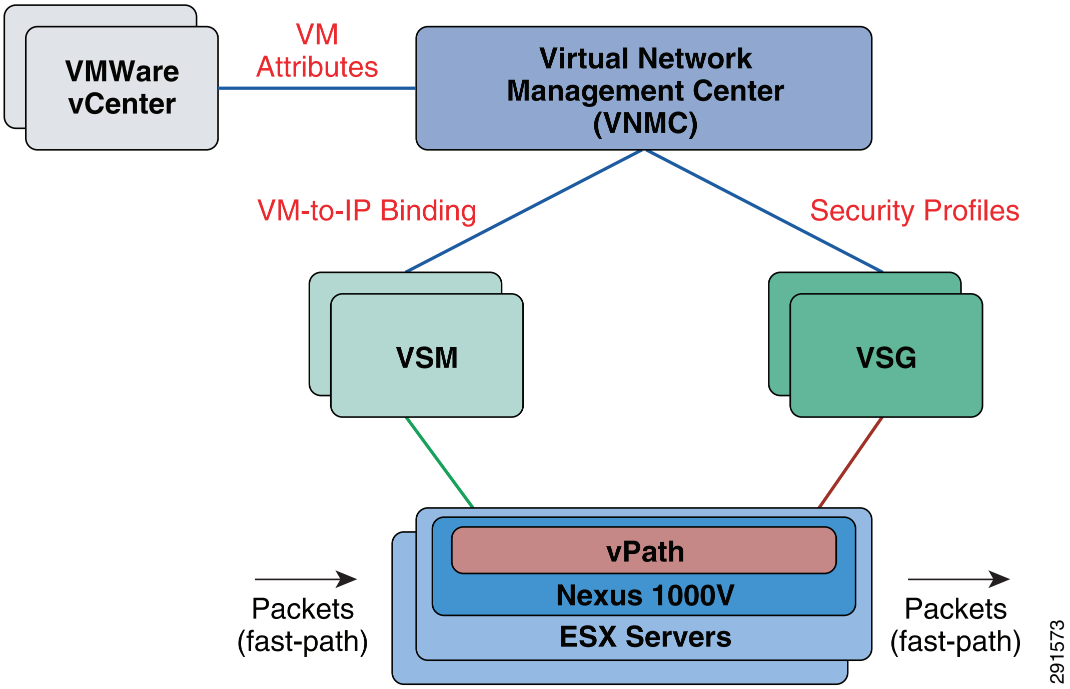
| Cisco VSG | |
|---|---|
| **PRIMARY FUNCTION** | **Requirement 1 (1.2, 1.3)** |
| Restrict traffic between the cardholder data environment and other network areas. | |
| **CAPABILITY** | **ASSESSMENT** |
| **Secure Services** | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| **Authentication** | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| **Logs** | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

### Design Considerations

Cisco VSG integrates with Cisco Nexus 1000V Series Switches to enforce security policies for your virtualized environment. VNMC provides policy management for a multitenant environment. One or more VSGs are required per tenant. VSG uses the vPath intelligence in the Virtual Ethernet Module (VEM) of the Cisco Nexus 1000V Series to provide the security policy enforcement.

Cisco VSG is deployed as a virtual appliance in vCenter. The primary function of Cisco VSG is to protect against unauthorized access to the cardholder environment.

*Figure 5-113 Cisco Nexus VSG System Architecture*



### PCI Assessment Detail—PCI Sub-Requirements Satisfied

#### Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

Cisco VSG can protect the cardholder data environment from untrusted networks by enforcing security policies for any network traffic entering or leaving a virtual machine. These security policies are enabled at a port-profile level in the Cisco Nexus 1000V. All the virtual machines connecting to the network with those port-profiles (port-groups) are protected through firewall policies.

- **PCI 1.2.1**—*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*
- **PCI 1.2.2**—*Secure and synchronize router configuration files.*

  Configuration files are backed up centrally using EMC Ionix Network Configuration Manager (NCM). This tool also verifies that running and startup configurations of devices are synchronized.
- **PCI 1.3.5**—*Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.*

- **PCI 1.3.6**—*Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.)*
- **PCI 1.3.7**—*Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.*

To insert the firewall into the network, you need to attach the security profile to the port profile. All the traffic traversing through the virtual ports associated with that port profile, is enforced by the security policy. The following two commands enable the firewall feature under the port profile:

```
Nexus1000V (config)# org root/TenantA
Nexus1000V (config)# vn-service ip-address VSG_Data_IP vlan VSG_Service_VLAN
security-profile SecureTenantA
```

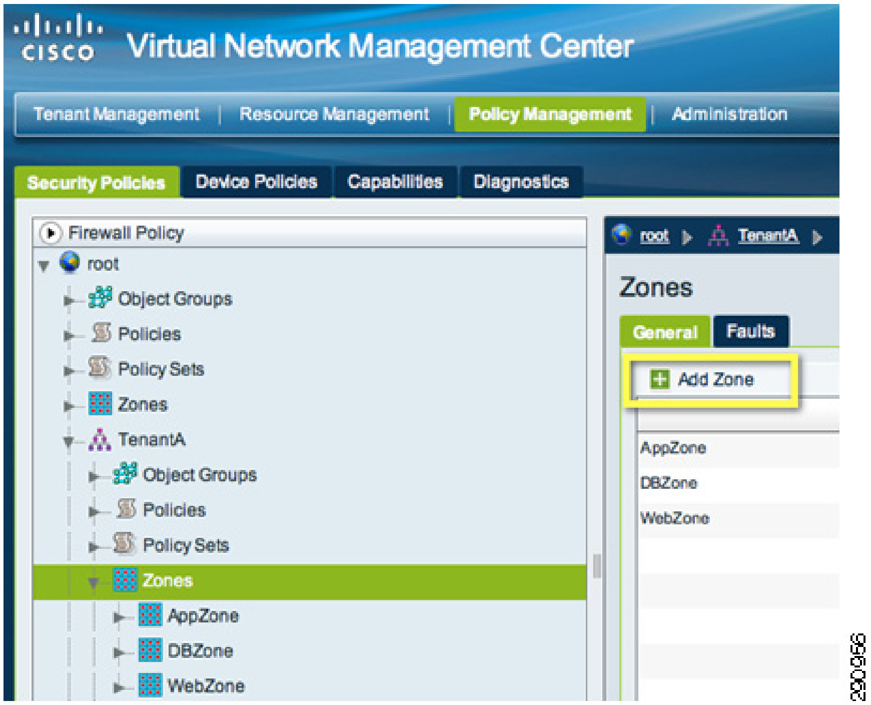
The first command specifies the tenant whose workload is being protected. The second command binds the security profile to the port-profile for that tenant. Once the firewall is enabled, the traffic is intercepted by vPath and sent to Cisco VSG over a dedicated VLAN. Cisco VSG evaluates the traffic against the security policy. It sends the decision (deny or allow) back to vPath, which enforces the Cisco VSG decision to the traffic flow. VNMC publishes the security policies for each tenant for individual Cisco VSGs. These policies are maintained and edited in the VNMC.

Placing cardholder data systems in security zones can isolate the environment from the DMZ and external network. These zones are leveraged in writing the security policies in the VNMC.

To create the Navigation pane, do the following:

1. Click the Policy Management tab, click the Security Policies subtab, and expand Firewall Policy > root to view the appropriate Zones node.
2. Select the organizational level (Tenant) where you want to add the zone. In the Work pane, click the Add Zone link. (See Figure 5-114.)

***Figure 5-114 Virtual Network Management Center—Policy Management***



### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2**—*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*
- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco Nexus VSG does not have any unnecessary services enabled by default.
- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Only SSH access is allowed for firewall console access over the network. The communication between Cisco VSG and Management Platform (VNMC) is all encrypted over SSL (443)

  Cisco Nexus VSG can be configured to use secure protocols for all system functions. This includes SSH for remote management, SCP, and SFTP for file transfers. Insecure services can be disable or blocked using configuration statements and access lists.

  ```
  no feature telnet
  no telnet server enable
  feature ssh
  ```

  Cisco Nexus VSG support administrative protocols with strong cryptography such as SSH version 2.

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco Nexus Virtual Security Gateway. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html.

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by the Cisco Nexus VSG using LDAP services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*

- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*
- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

User roles in VNMC contain one or more privileges that define the operations allowed for the user who is assigned the role. A user can be assigned one or more roles. A user assigned multiple roles has the combined privileges of all assigned roles. For example, if Role1 has policy-related privileges, and Role2 has tenant-related privileges, users who are assigned to both Role1 and Role2 have policy and tenant related privileges.

The system contains the following default user roles:

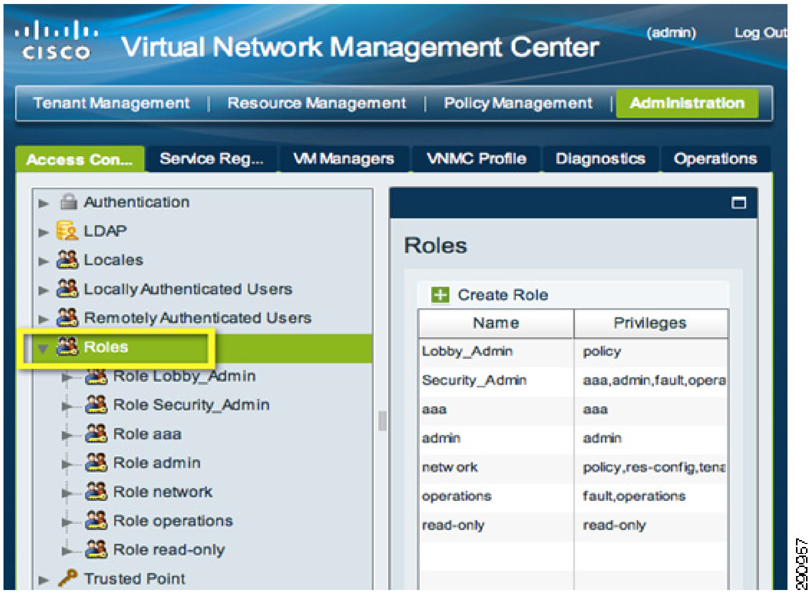
- aaa—User has read and write access to users, roles, and AAA configuration. Read access to the rest of the system.
- admin—User has complete read-and-write access to the entire system and has all privileges. The default admin account is assigned this role by default, and it cannot be changed.
- network—User creates organizations, security policies, and device profiles.
- operations—User acknowledges faults and performs some basic operations such as logging configuration.
- read-only—User has read-only access to system configuration and operational status with no privileges to perform any operations.

Roles can be created, modified to add new or remove existing privileges, or deleted. When a role is modified, the new privileges are applied to all users assigned to that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you can use a custom set of privileges to create a unique role. For example, the default Network and Operations roles have different sets of privileges, but a new Network and Operations role can be created that combines the privileges of both roles.

To configure roles in VNMC, do the following:

1. Click the **Administration** tab, then click the **Access Control** sub-tab.
2. In the Navigation pane, select the **Roles** node. In the Work pane, click **Create Roles** (see Figure 5-115.)

*Figure 5-115 Configuring Roles*

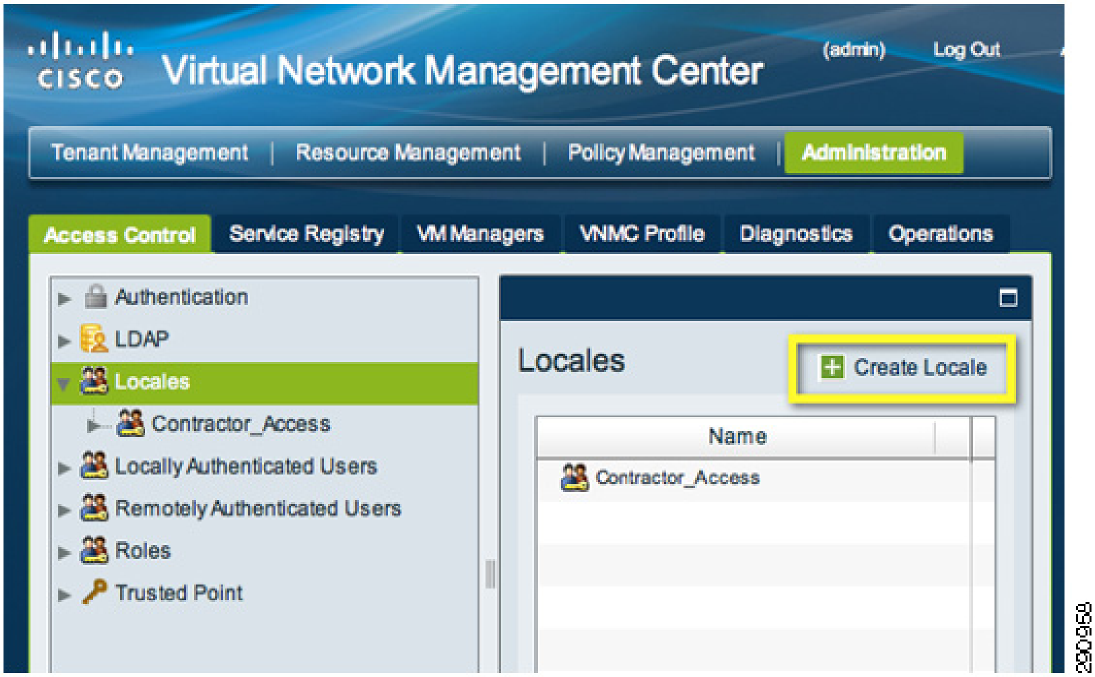


| Name | Privileges |
|---|---|
| Lobby_Admin | policy |
| Security_Admin | aaa,admin,fault,opera |
| aaa | aaa |
| admin | admin |
| netw ork | policy,res-config,tena |
| operations | fault,operations |
| read-only | read-only |

In addition to roles, the user is also provided another dimension of privilege, which limits the user to tenant level visibility, called *locale*. Each locale defines one or more organizations (domains) to which the user is allowed access, and access would be limited to the organizations specified in the locale. To configure locales in VNMC, do the following:

1. Click the Administration tab, then click the Access Control sub-tab.
2. In the Navigation pane, select the Locales node.
3. In the Work pane, click the Create Locale link. (See Figure 5-116.)

*Figure 5-116 Configuring Locales*



| Name |
|---|
| Contractor_Access |

CLI configuration of AAA services is as follows:

```
tacacs-server key 7 "<removed>"
tacacs-server host 192.168.42.131
aaa group server tacacs+ CiscoACS
    server 192.168.42.131
    use-vrf management
    source-interface mgmt0
aaa group server tacacs+ tacacs
!
aaa authentication login default group CiscoACS
aaa authentication login console group CiscoACS
```

#### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the LDAP authentication capabilities to the Windows Active Directory server for AAA services. Microsoft Active Directory contains the necessary user account services for all of the appropriate PCI 8 requirements. Configure AAA services as shown above in Requirement 7.

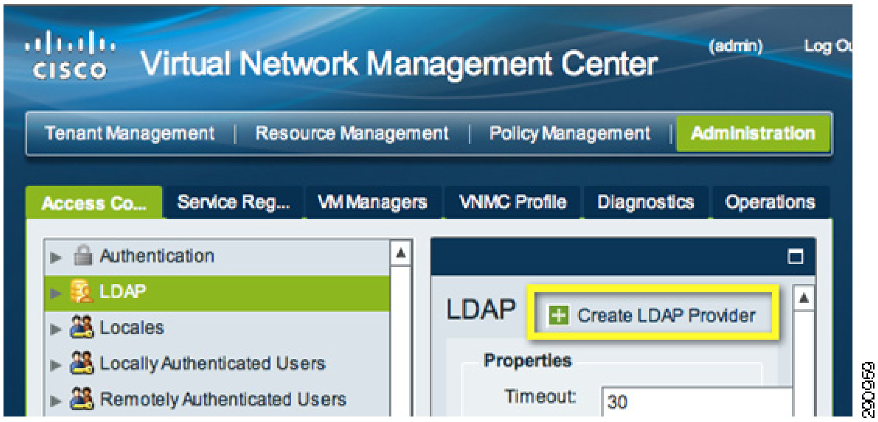
- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something you are, such as a biometric*
- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*
- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco VNMC provides remote authentication with LDAP servers for user authentication. When user accounts are created in the LDAP server, the accounts also include the roles and locales those users require for working in Cisco VNMC.

  To configure the LDAP server, do the following:

  1. Click the Administration tab, the click the Access Control sub-tab.
  2. In the Navigation pane, select the LDAP node.
  3. In the Work pane, click the Create LDAP Provider link. (See Figure 5-117.)

*Figure 5-117 Configuring LDAP Server*



Timeout: 30

### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

The Cisco Nexus VSG is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco Nexus VSG uses NTP to update and synchronize local clock facilities and meet the following requirements:

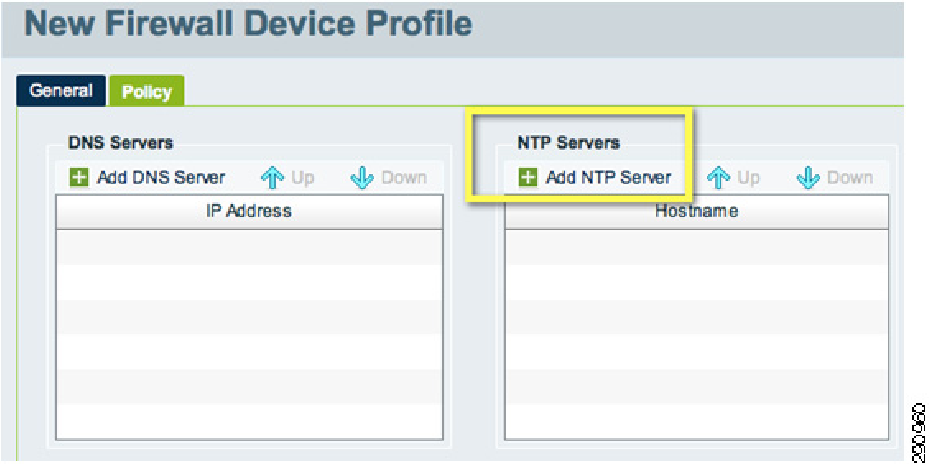
- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP servers were hosted at the data center site. The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

NTP is configured in the Firewall Device Profile for the Cisco VSG VNMC. The setting is published via the device policy to Cisco VSG.

1. In the navigation pane, click the Policy Management tab, then the Device Policies sub-tab, and expand the Device Profile for a tenant.
2. Click a Profiles node to add a firewall device profile, and you see the option to add NTP server, as shown in Figure 5-118.

***Figure 5-118 Configuring NTP***



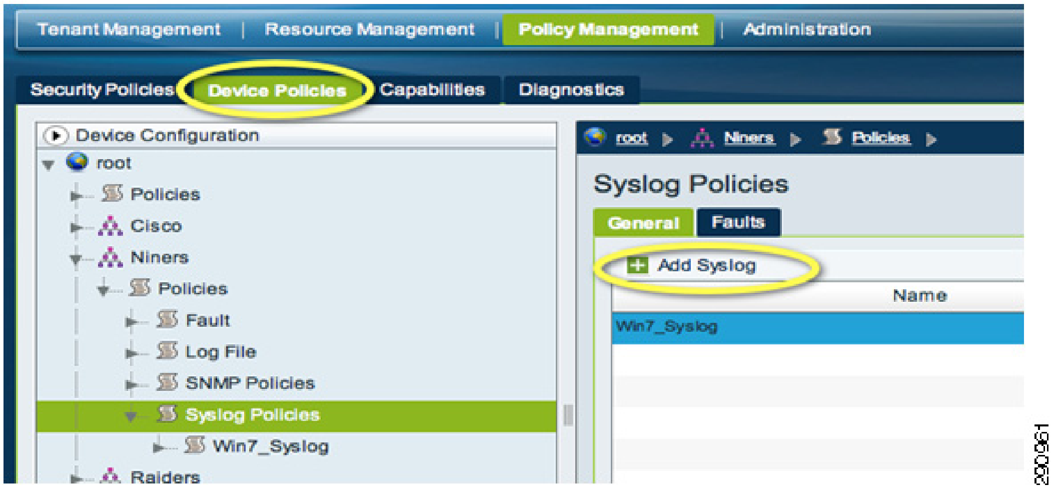
Requirement 10.5 was met using a central logging repository, RSA enVision, which collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

You can configure the syslog server for Cisco VSG to send all the logging information to a standard syslog server. This setting is available as part of the device profile.

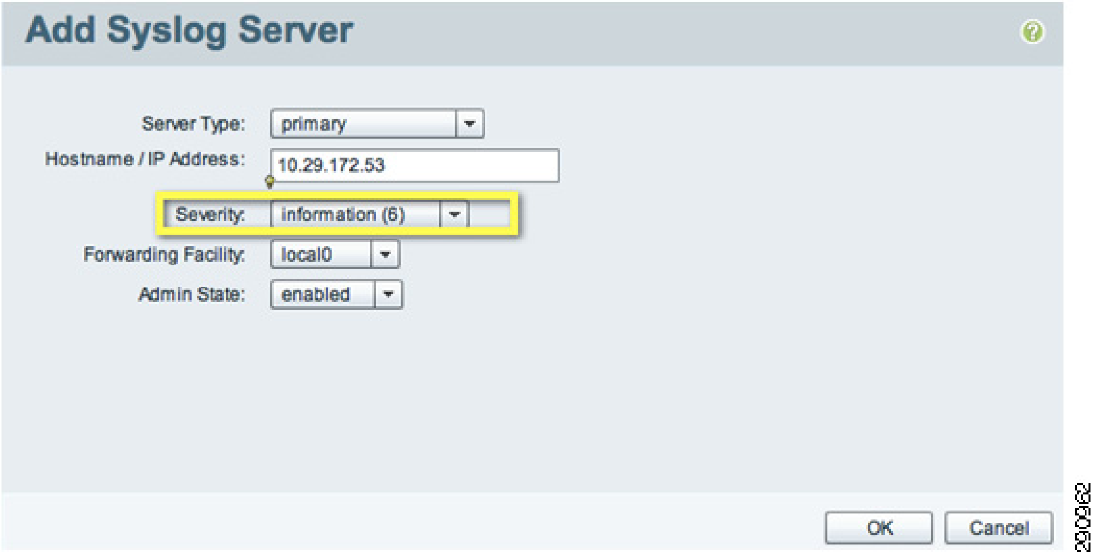
1. Navigate to Policy Management > Device Policies > Tenant> Policies > Syslog Policies. Add a syslog policy, as shown in Figure 5-119.

*Figure 5-119 Configuring Syslog*



2. The severity of the logging should be at level 6 to capture the firewall policy hit in the VSG. (See Figure 5-120).

*Figure 5-120 Configuring Logging Severity*



Add Syslog Server

Server Type: primary

Hostname / IP Address: 10.29.172.53

Severity: information (6)

Forwarding Facility: local0

Admin State: enabled

3. The syslog policy is attached to the Device Profile to enable the settings in the VSG.

## PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

## PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

# Intrusion Detection

## Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2

The Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2 (IDSM2) is an important intrusion prevention system (IPS) solution that protects switched environments by integrating full-featured IPS functions directly into the network infrastructure through the widely deployed Cisco Catalyst chassis. This integration allows the user to monitor traffic directly off the switch backplane.

The Cisco IDSM-2 with Cisco IPS Sensor Software v6.0 helps users stop more threats with greater confidence, through the use of the following elements:

- Multivector threat identification—Detailed inspection of Layer 2–7 traffic protects your network from policy violations, vulnerability exploitations, and anomalous activity.
- Accurate prevention technologies—The innovative Cisco Risk Rating feature and Meta Event Generator provide the confidence to take preventive actions on a broader range of threats without the risk of dropping legitimate traffic.

When combined, these elements provide a comprehensive inline prevention solution, providing the confidence to detect and stop the broadest range of malicious traffic before it affects business continuity.

*Table 5-61 PCI Assessment Summary—Cisco IDSM2*

| **Models Assessed** | |
|---|---|
| WS-SVC-IDSM-2 version 7.0(4) | |
| **PCI Sub-Requirements Passed** | |
| **PCI 2** | 2.2.2, 2.2.4, 2.3 |
| **PCI 6** | 6.1 |
| **PCI 7** | 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 7.2.2, 7.2.3 |
| **PCI 8** | 8.1, 8.2, 8.4, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15 |
| **PCI 10** | 10.1, 10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.4.2, 10.4.3, 10.5.1, 10.5.2, 10.5.3 |
| **PCI 11** | 11.4 |
| **PCI Sub-Requirements Requiring Compensating Controls** | |
| No compensating controls were required to satisfy any sub-requirements. | |
| **PCI Sub-Requirements Failed** | |
| No sub-requirements were failed. | |

### Primary PCI Function

The primary PCI function of the Cisco ISDM2 is to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises (11.4).

Table 5-61 lists the component assessment details for the Cisco ISDM2.

*Table 5-62 Component Capability Assessment—Cisco ISDM2*

| Cisco IDSM2 | |
|---|---|
| PRIMARY FUNCTION | Requirement 11 (11.4) |
| Monitor all traffic at the perimeter of the CDE as well as at critical points inside the CDE. | |
| CAPABILITY | ASSESSMENT |
| Secure Services | |
| **Disabled any unnecessary services—***"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.* (Sub-requirements 2.2.2, 2.2.4) | ● |
| **Secure administrative access—***Encrypt all non-console administrative access using strong cryptography.* (Sub-requirement 2.3) | ● |
| **Vendor supported—***Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.* (Sub-requirement 6.1) | ● |
| Authentication | |
| **Role-based access—***Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following. Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.* (Sub-requirement 7.1, 7.2) | ◉ |
| **Use secure, unique accounts—***Assign all users a unique ID before allowing them to access system components or cardholder data.; Strong Passwords.* (Sub-requirements 8.1, 8.2, 8.4, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14) | ◉ |
| Logs | |
| **Audit trails—***Secure audit trails so they cannot be altered. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.* (Sub-requirement 10.5, 10.5.3) | ◉ |
| **The ability to use Network Time Protocol—***Time data is protected; Time settings are received from industry-accepted time sources.* (Sub-requirements 10.4.2, 10.4.3) | ● |

## Design Considerations

- Configure the Cisco IDSM2 to lock accounts so that users cannot keep trying to login after a certain number of failed attempts.
- Allow secure management of the Cisco IDSM2 only from a specific host/hosts.
- Configure appropriate banner messages on login. The login banner warning should not reveal the identity of the company that owns or manages the Cisco IDSM2. The banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Change default passwords and community strings to appropriate complexity.

For more information, see the Installation Guide at the following URL:
http://www.cisco.com/en/US/docs/security/ips/6.0/configuration/guide/cli/cliInter.html

## PCI Assessment Detail—PCI Sub-Requirements Satisfied

### Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*

Cisco IDSM2 modules allow only administrative connections from authorized hosts/networks as specified in the device configuration. The following configuration shows the authorized management hosts for SSH and HTTPS administration, and disabling of Telnet.

```
! -----------------------------
service host
network-settings
host-ip 192.168.21.94/24,192.168.21.1
host-name DMZ-IDS2
telnet-option disabled
access-list 10.19.151.99/32
access-list 192.168.41.101/32
access-list 192.168.41.102/32
access-list 192.168.42.122/32
access-list 192.168.42.124/32
access-list 192.168.42.133/32
access-list 192.168.42.138/32
```

- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*

  Cisco IDSM2 modules do not have any unnecessary services enabled by default.

- **PCI 2.3**—*Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other nonconsole administrative access.*

  Cisco IDSM2 modules use strong encryption for SSH and HTTPS.

### Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

  The Cisco Product Security Incident Response Team site tracks and publishes information about any relevant exposures and vulnerabilities in Cisco IDSM2 modules. When vulnerabilities are announced, administrators can securely and easily download security patches and install them throughout the enterprise.

  Software support for all Cisco products can be located at:
  http://www.cisco.com/cisco/software/navigator.html

### Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

The relevant sub-requirements of Requirement 7 were met using a centralized user database (Active Directory). It is accessed by Cisco Secure ACS RADIUS services. Individual user IDs are assigned. Roles are defined and based on group membership. This configuration was used to address the following individual requirements:

- **PCI 7.1.1**—*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities*
- **PCI 7.1.2**—*Assignment of privileges is based on individual personnel's job classification and function*
- **PCI 7.1.3**—*Requirement for a documented approval by authorized parties specifying required privileges.*

- **PCI 7.1.4**—*Implementation of an automated access control system*
- **PCI 7.2.1**—*Coverage of all system components*
- **PCI 7.2.2**—*Assignment of privileges to individuals based on job classification and function*
- **PCI 7.2.3**—*Default "deny-all" setting. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

  Cisco IDSM2 modules are configured to use a AAA model for user-based access. Users can be assigned to groups and based on privilege levels, have access to only the information they require for their job function. By default, no users are allowed access unless specifically configured and assigned appropriate passwords. The following configuration statements use the RADIUS protocol to communicate with the Cisco ACS server where individual user groups and roles are configured, limiting and logging access as appropriate.

```
! -----------------------------
service aaa
aaa radius
primary-server
server-address 192.168.42.131
shared-secret <removed>
exit
nas-id DMZ-IDS1
local-fallback enabled
console-authentication radius-and-local
default-user-role administrator
exit
exit
! -----------------------------
```

### Requirement 8: Assign a Unique ID to Each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure ACS for AAA services and Microsoft Active Directory for user account services. Configure AAA services, as shown above in Requirement 7.

The Cisco IDSM2 module is able to meet some of the requirements locally as identified below.

- **PCI 8.1**—*Assign all users a unique ID before allowing them to access system components or cardholder data.*

  Cisco IDSM2 modules support the creation of local user accounts with unique IDs through the use of the **username** command. These can be used for local fallback user accounts.

```
sensor(config)# username username password password privilege
```

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
  - *Something you know, such as a password or passphrase*
  - *Something you have, such as a token device or smart card*
  - *Something yo*u are, such as a biometric

  When configuring local user accounts, you must specify a password to achieve PCI compliance.

- **PCI 8.4**—*Render all passwords unreadable during transmission and storage on all system components using strong cryptography.*

  All local passwords on the Cisco IDSM2 are stored using strong encryption.

- **PCI 8.5.5**—*Remove/disable inactive user accounts at least every 90 days.*

Cisco IDSM2 modules do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days.

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*

  Cisco IDSM2 modules do not support an automated capability to perform this function for local accounts at this time; user accounts would have to be manually reviewed in the device configurations every 90 days.

- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*

  Cisco IDSM2 modules support the ability to specify a minimum password length for local accounts.

```
! -----------------------------
service authentication
password-strength
size 7-64
! -----------------------------
```

- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*

  Cisco IDSM2 modules support the ability to specify alphanumeric passwords for local accounts.

```
! -----------------------------
service authentication
password-strength
digits-min 1
lowercase-min 1
other-min 1
! -----------------------------
```

- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*

  Cisco IDSM2 modules support the ability to specify that old passwords should not be re-used for local accounts.

```
! -----------------------------
service authentication
password-strength
number-old-passwords 4
! -----------------------------
```

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*

  Cisco IDSM2 modules support the ability to specify that only a limited number of attempts can be made when authenticating for local accounts.

```
! -----------------------------
service authentication
attemptLimit 6
! -----------------------------
```

- **PCI 8.5.14**—*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*

  Cisco IDSM2 modules support the ability to lockout local accounts after the specified number of failed attempts, requiring an administrator to re-enable them. Locked accounts are indicated by parentheses when using the **show users** command:

```
sensor# show users all
    CLI ID   User         Privilege
*   1349     bart         administrator
```

```
5824      (pauljones)  viewer
9802      christian    operator
```

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.*

  Cisco IDSM2 modules do not feature an explicit session timeout. Administration time limits would need to be enabled systemically through active directory policy to the admin workstation desktops.

### Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Cisco IDSM2 is able to track and monitor all administrative user access and events.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
  - **PCI 10.2.1**—*All individual accesses to cardholder data*
  - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
  - **PCI 10.2.3**—*Access to all audit trails*
  - **PCI 10.2.4**—*Invalid logical access attempts*
  - **PCI 10.2.5**—*Use of identification and authentication mechanisms*
  - **PCI 10.2.6**—*Initialization of the audit logs*
  - **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3**—*Record at least the following audit trail entries for all system components for each event:*
  - **PCI 10.3.1**—*User identification*
  - **PCI 10.3.2**—*Type of event*
  - **PCI 10.3.3**—*Date and time*
  - **PCI 10.3.4**—*Success or failure indication*
  - **PCI 10.3.5**—*Origination of event*
  - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource.*

Cisco IDSM2 uses NTP to update and synchronize their local clock facilities and meet the following requirements:

- **PCI 10.4.2**—*Time data is protected.*
- **PCI 10.4.3**—*Time settings are received from industry-accepted time sources.*

  NTP is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the network used NTP to synchronize their clocks. The NTP server was hosted at the data center site. Cisco IDSM2 uses NTP to meet these requirements by implementing the following configuration statements:

  ```
  time-zone-settings
  offset -8
  standard-time-zone-name PST
  exit
  ntp-option enabled-ntp-unauthenticated
  ntp-server 192.168.62.161
  exit
  summertime-option recurring
  ```

```
summertime-zone-name PDT
```

To learn more about NTP, visit: http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

**Note** The Cisco Retail Lab uses two NTP servers that are synchronized to external reference sources. All systems and devices in the lab are pointed to these two servers.

To meet all of the requirements listed below, the PCI solution for retail uses a central logging repository located in the data center. RSA enVision collects information from all devices to ensure the integrity and correlation of events.

- **PCI 10.5**—*Secure audit trails so they cannot be altered.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
- **PCI 10.5.5**—*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

  Cisco IDSM2 modules are capable of sending system events to a centralized repository using SNMP traps. Logs stored locally are buffered and require operator level privileges on the device to be viewed. External logging is enabled by implementing the following configuration statements to send them to the RSA enVision server:

```
! ------------------------------
service notification
trap-destinations 192.168.42.124
trap-community-name RSAenVision
exit
enable-notifications true
trap-community-name RSAenVision
exit
! ------------------------------
```

### Requirement 11: Regularly Test Security Systems and Processes

- **PCI 11.4**—*Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.*

  Cisco IDSM2 modules are capable of performing intrusion detection and prevention through the use of VLAN interfaces from the host Cisco Catalyst service chassis. IPS signature updates and configurations are managed centrally through Cisco Security Manager. The following configuration statements are necessary in the Cisco Catalyst service chassis to forward traffic via VLANs and enable the IDS inspection capability:

```
!
!
intrusion-detection module 2 management-port access-vlan 21
intrusion-detection module 2 data-port 1 trunk allowed-vlan 83,84
!
```

Cisco IDSM2 module interfaces are configured as follows to receive, inspect, and forward traffic across the assigned VLANs:

```
! -----------------------------
service interface
physical-interfaces GigabitEthernet0/7
subinterface-type inline-vlan-pair
subinterface 1
description INT1 vlans 83 and 84
vlan1 83
vlan2 84
exit
exit
exit
exit
! -----------------------------
```

### PCI Assessment Detail—PCI Sub-Requirements that Require Compensating Controls

No compensating controls were required to satisfy any sub-requirements.

### PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.