



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 C, "Verizon Business Reference Architecture Report—Cisco PCI Solution."

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 As	ssessed
Cisco Cat	alyst Switch
PCI Sub-R	lequirements 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, 10.5.1, 10.5.2, 10.5.3, 10.5.5
PCI Sub-Req	uirements Requiring Compensating Controls
No compens	ating controls were required to satisfy any sub-requirements.
PCI Sub-Req	uirements Failed
No sub-requ	irements were failed.

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

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 5-2.

Cisco Component PRIMARY FUNCTION [Description of primary PCI function] REQUIREMENT: [PCI requirement addressed]		
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	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)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
\checkmark	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.
+	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)
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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)
\checkmark	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 5-2
 Capability Assessment Example

The PCI DSS 2.0 security standard is written from the perspective of helping an organization 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-coded icons used in the tables.

Table 5-3 Color-Coded Icon Definitions

lcon	Description
\checkmark	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.
Ø	The component has no capability to satisfy the requirement.

L

Design Considerations

This section provides compliance principles as well as best practices for each technology deployed within an enterprise 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

The endpoints 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.

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

Models As	sessed
Cisco Unit	fied Communication Manager 8.5.1
PCI Sub-Re	equirements 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 5-5 lists the component assessment details for Cisco Unified Communications Manager.

 Table 5-5
 Component Capability Assessment – Cisco Unified Communications Manager

PRIMARY FUN Securely ma REQUIREMEN	anage IP phones and communicat	tion flows
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	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)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
\checkmark	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
\checkmark	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.
\checkmark	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)
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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)
1	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.)

CIECO	CM Administration Navigation Cisco Unified CM Administratio mmunications Solutions bmcgloth Search Documentation About	Logo
ystem 👻 Call Routing 👻 Media Resourc	irces 👻 Advanced Features 👻 Device 👻 Application 👻 User Management 👻 Bulk Administration 👻 Help 👻	
nterprise Parameters Configurat	ition	
🔜 Save p Set to Default 🛛 😋 Res	eset 🥒 Apply Config	
- Secured Phone URL Parameters	c	
	· · · · · · · · · · · · · · · · · · ·	
Secured Authentication URL	https://cm-2.cisco-irn.com:8443/ccmcip/authenticate.jsp	
Secured Authentication URL	https://cm-2.cisco-irn.com:8443/ccmcip/authenticate.jsp	
Secured Authentication URL Secured Directory URL	https://cm-2.cisco-irn.com:8443/ccmcip/authenticate.jsp	
Secured Authentication URL Secured Directory URL Secured Idle URL	https://cm-2.cisco-irn.com:8443/ccmcip/authenticate.jsp https://cm-2.cisco-irn.com:8443/ccmcip/xmldirectory.jsp	

Figure 5-1 Enterprise Parameters Configuration

• **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 (PSIRT) 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

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT, see the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

L

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

and List Roles			
Add New 🔠 Select All 🔛 Clear All 💥 Delete Selected			
Name *	Application	Description	Сору
Standard AXL API Access	Cisco Call Manager AXL Database	Access the AXL APIs	6
Standard Admin Rep Tool Admin		Administer CAR	l)
Standard Audit Log Administration	Cisco Call Manager Serviceability	Serviceability Audit Log Administration	D
Standard CCM Admin Users		All users with access to CCM web site	ľ
Standard CCM End Users		Access to CCM User Option Pages	ß
Standard CCM Feature Management	Cisco Call Manager Administration	Standard CCM Feature Management	l <u>b</u>
Standard CCM Gateway Management	Cisco Call Manager Administration	Standard CCM Gateway Management	Ū)
Standard CCM Phone Management	Cisco Call Manager Administration	Standard CCM Phone Management	B
Standard CCM Route Plan Management	Cisco Call Manager Administration	Standard CCM Route Plan Management	ľ
Standard CCM Service Management	Cisco Call Manager Administration	Standard CCM Service Management	ß
Standard CCM System Management	Cisco Call Manager Administration	Standard CCM System Management	l <u>b</u>
Standard CCM User Management	Cisco Call Manager Administration	Standard CCM User Management	ß
Standard CCM User Privilege Management	Cisco Call Manager Administration	Standard CCM User Privilege Management	Ð
Standard CCMADMIN Administration	Cisco Call Manager Administration	Administer all aspects of CCMAdmin system	ľ
Standard CCMADMIN Administration	Cisco Call Manager Dialed Number Analyser	Administer all aspects of CCMAdmin system	ß
Standard CCMADMIN Read Only	Cisco Call Manager Administration	Read access to all CCMAdmin resources	ß
Standard CCMADMIN Read Only	Cisco Call Manager Dialed Number Analyser	Read access to all CCMAdmin resources	6
Standard CCMUSER Administration	Cisco Call Manager End User	Administer all aspects of CCMUser system	ß
Standard CTI Allow Call Monitoring	Cisco Computer Telephone Interface (CTI)	Allow monitoring of calls	6
Standard CTI Allow Call Park Monitoring	Cisco Computer Telephone Interface (CTI)	Allow monitoring of call park DNs	6
Standard CTI Allow Call Recording	Cisco Computer Telephone Interface (CTI)	Allow recording of calls	ß
Standard CTI Allow Calling Number Modification	Cisco Computer Telephone Interface (CTI)	Allow calling number modification	ľù.
Standard CTI Allow Control of All Devices	Cisco Computer Telephone Interface (CTI)	Allow control of all CTI controllable devices	6
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	ß
Standard CTI Allow Control of Phones supporting Rollover Mode	Cisco Computer Telephone Interface (CTI)	Standard CTI Allow Control of Phones supporting Rollover Mode	6
Standard CTI Allow Reception of SRTP Key Material	Cisco Computer Telephone Interface (CTI)	Allows access to SRTP key material	6
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	6
Standard CUReporting	Cisco Unified Reporting	Allows application users to generate reports from various sources	lîn 🖉

- 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.)

ystem ▼ Call Routing ▼ Media Resources ▼ Advanced Features ▼	Device - Application -	User Management 👻	Bulk Administration 👻	Help 👻		
ole Configuration					Related Links: Back To Find/List	
Copy 💾 Add New						
Role Information						
Application* Cisco Call Manager Administration						
Name* Standard CCM Service Management						=
Description Standard CCM Service Management						
esource Access Information						
Resource		Description			Privilege	
AAR Group web pages				🖾 n	ead 🔲 update	
Access List				🖾 n	ead 🔲 update	
Add Unity User				🖾 r	ead 🔲 update	
Announcement				- n	ead 🔲 update	
Annunciator web pages				V re	ead 🗹 update	
Application Dial Rules web pages				🔲 re	ead 🔲 update	
Application Server				🗔 re	ead 🔲 update	
Application User CAPF				🛄 n	ead 🔲 update	
Application User Web Pages				🖾 n	ead 🔲 update	
BLF Directed Call Park					ead 🔲 update	
BLF Speeddial				🖾 n	ead 🔲 update	
Blocked Learned Pattern				🔲 n	ead 🔲 update	
Blocked Learned Patterns				🖾 n	ead 🔲 update	
Bulk Add/Update Lines				🔲 n	ead 🔲 update	
Bulk Add/Update Phones				🛄 n	ead 🔲 update	
Bulk CUPS User Page				🔲 n	ead 🔲 update	
Bulk Config Tool Export				🖾 n	ead 🔲 update	
Bulk Config Tool Import				🔲 n	ead 🔲 update	
Bulk Config Tool Import Validation				🗖 re	ead 🔲 update	
Bulk Delete Access List				🗖 re	ead 🔲 update	
Bulk Delete Call Pickup Group				🗖 re	ead 🔲 update	
Bulk Delete Client Matter Codes				🗖 n	ead 🔲 update	
Bulk Delete Fallback Profile				🖾 n	ead 🔲 update	
Bulk Delete Forced Authorization Codes				🗐 n	ead 🔲 update	
Bulli Delete Cetemone			10			-
one						2 🖾 🖂 🕲 🕅

Figure 5-3 Role Configuration

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.

System • Call Routing • Me	edia Resources 👻 Advanced Features 👻 Device 👻 Application 👻	Us	er Management 👻	Bulk Administration 👻	Help 👻	1
System + Cal Routing + Mu End User Configuration Save Status Status: Ready User ID* Password Confirm Password PIN Last name * Middle name First name Telephone Number Mail ID Manager User ID Department User Lozie	dia Resources × Advanced Features × Device × Application ×	Use	er Management + Credential Policy I Credential Policy I Application User Role User Group User/Phone Add Application User End User CAPF P SIP Realm	Default CAPF Profile	Related Links: Back to Find List Users Go	
Associated PC Digest Credentials Confirm Digest Credentials						

Figure 5-4 End User Configuration

- 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.

System Call Routing Media Resources Advanced Feature	ures 👻 Device 👻 Application 👻 User Management 👻 B	Jlk Administration	
Credential Policy Configuration		Related Links: Back To Find/List	Go
Add New 🗋 Copy			
Status			
i 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			
Add New Copy			
(i) *- indicates required item.			
Check for Trivial Check this	check box to require the system	to disallow credential that are easily	
	ch as common words, repeated c		
		•	=
The default	setting checks the check box.		

Figure 5-5 User Credential Policy Configuration

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.

For Cisco Unified CM Ad		Admir	Navigation Cisco Unifie nistrator Search Docum	
Call Routing 👻 Media Resources 👻	Advanced Features - Device - Application - User Management -	Bulk Administration 👻 Help 💌		
Configuration		Related Links: Ba	sck To Find/List	•
	2	Related Links. De	ick to HindyElse	
e 🗙 Delete 📄 Copy 🎦 Reset	: 🖉 Apply Config 🖕 Add New			
	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			Override Common
		?	Param	Settings
	Disable Speakerphone			
	Disable Speakerphone and Headset			
	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			

Figure 5-6 Phone Configuration

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 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

61660	Cisco Unified Operating System Admi For Cisco Unified Communications Solutions	nistration Navigation Cisco Unified OS Administration - Go admin Search Documentation About Logout
Show 👻 Set	ings ✔ Security ✔ Software Upgrades ✔ Services ✔ Help ✔	
NTP Server	List	
Add New	Select All 🔛 Clear All 💥 Delete Selected	
Status —		
i 2 recor	ds found	
NTP Serve	r	
	Hostname or IP Address	Status
	192.168.62.161	The NTP service is accessible.
	192.168.62.162	The NTP service not accessible.
Add New	Select All Clear All Delete Selected	

To meet all of the requirements listed below, the PCI solution 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.

ahaha	Cisco Unified CM Ad	ministration			Navigation 🔽	Cisco Unified	CM Administrat	ion 🔻 Go
cisco	For Cisco Unified Communicat	tions Solutions		bmcglo	th Search	Documentat	ion About	Logout
System 👻	Call Routing 👻 Media Resources 👻 🖉	Advanced Features 👻	Device 👻	Application 👻	User Managem	ent 👻 Bulk A	dministration 👻	Help 👻
nterprise	Parameters Configuration							
📄 Save	🧬 Set to Default	Apply Config						
-Cisco S	vslog Agent	Apply Config						
-Cisco S	vslog Agent	Apply Config 192.168.42.124						

Figure 5-8 Enterprise Parameters Configuration

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

Figure 5-9 Audit Log Configuration

cisco	Cisco Unified Serviceability For Cisco Unified Communications Solutions	Navigation Cisco Unified Serviceability JGO bmcgloth About Logout
<u>A</u> larm v <u>T</u>	jrace ▾ Tools ▾ Snmp ▾ Help ▾	
Audit Log	Configuration	
🔚 Save	e 🧀 Set to Default	
Status (j) Status	: Ready	
Select S		
	m-2.cisco-irn.com 🔽 Go to All Nodes	
	to All Nodes	
— Applicati Filter Se	on Audit Log Settings ttings	
	Enable Audit Log	
	Enable Purging	
	Enable Log Rotation	
Remote		
Ser	ver Name ¹ 192.168.42.124	Remote Syslog Audit Event Level 🛛 Informational 💌
	mum No. of Files* 366 366 366 366 366 366 366 366 366 366	
Databas	e Audit Log Filter Settings	
	Enable Audit Log	Debug Audit Level Schema Only 🔽
Output S	-	
	Enable Audit Log Rotation	
	ximum No. of Files* 40 . of Files Deleted on Log Rotation* 20	
— Save	Set to Default	20 50 50

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 branch and data center 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

Models As	sessed
Cisco Vide	eo Surveillance Manager version 6.3.1
PCI Sub-Re	equirements 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-Re	equirements Requiring Compensating Controls
No compe	nsating controls were required to satisfy any sub-requirements.
PCI Sub-Re	equirements Failed
No sub-rec	quirements were failed.

Table 5-6 PCI Assessment Summary—Cisco Video Surveillance

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 5-7 lists the component assessment details for the Cisco Video Surveillance solution.

PRIMARY FUN Monitor phy REQUIREMEN	ysical access to sensitive areas with	hin the cardholder environment
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove al unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
\checkmark	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.
+	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)
+	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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)
1	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 5-7 Component Capability Assessment – Cisco Video Surveillance

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/b estprac_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 (PSIRT) 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

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT, see the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

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

+) + [# http://msp-dc-1/vsom/index.	.php?cnd=user				1	े - C) 🚼	* Google		P 1	Feedback *
Most Visited 🗋 Cisco UCS Manager	UDM 🗋 NOM 🗋	wcs 🗋 1		RSA enVision	CM-2	RSA-AM	NSOM			Bookmarks
Operations Manager	Administrat	ion > Useri							and the second se	Super User
Devices		ers								
Servers (3) Encoders (0) Analog Cameras (0) Phletwork Cameras (3) PTZ Configuration (0) Monitors (0)	Clisk th	Help: List		<u>Llabels</u> fetails: Parameters can be m	anaged by click	ing the applicab	le icon.			
Video Feeds				Search		List of Us	ers		l.	1
Group Overview		User Name	Name	Email	Roles	Last Login	Parent Server	Authentication	Status Action	u
Batch Administration Archives (2)2) Wews (0)		fmacias	Femando Macias		Administrator Administrator			LDAP	Enabled D	
Accounts		grvarga	Oneg Varga		Operator			LDAP	Enabled 🍞 🤅	9
Solution (3)		bmcgloth	Bart McGlothin	bmcgloth@cisco.com	Administrator Operator	2011-04-05 17:37:45		LDAP	Enabled 🍞 🤅	•
User Account Sync				(3)	esults found, di	splaying 1 - 3				
System Events (0) Schedules (0) Schedules (0) Settings Pepots Verview Health Dashboard Utilities										
Councies .										

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

Function *				
Kideo Surveillance Operations Manag	er 🛛 🖄 Video Surveillance Managemeni	Console × +		-
(+) > P http://msp-dc-1/v	smc.html	🏫 = 🕑 🛃 = Google	P 1	Feedback *
Anost Visited Cisco UCS Manager		RSA enlision 🗋 HyTrust 🗋 CM-2 📄 RSA-AM 🗮 VSOM		Dockmarks
cisco		Video Surveillan	ce Management	Console
Overview	Operations Manager C	opfiguration	0	-
installed Packages	operations manager o	olinguiadoli		
Status Console	Log Level			
Monitoring	Log Level	Notice (Default)		
Archives	Database Connection			
Archive Backup		Ry301 5.0 -		
System Log	Database Server			
Mediaout	Database Usemame			
Server Status	Database Password			
Configuration	Database Name			
SNMP Trap Destinations	Database Version			
Manage Drivers	Catabase version.	0.0.1-12		
Media Server	Database Configuration Validatio	a		
Media Server Backup	Database Status	Validate DB		
Operations Manager		(Unsaved configurations can not be validated)		
🚳 Operations Manager Backup				
🖏 Virtual Matrix	SMTP Parameters			
4 Console Password	SMTP Server			
🖏 Camera Firmware Upgrade	SMTP "From." Address	support@cisco.com		
Server Upgrade		(Only affects to newly created or updated event setups)		
Restart Server	User Login Authentication			
Reboot Server	Authentication Type	LDAP Server		
Other Utilities				
	LDAP Configuration			
BWT Pages		171.68.38.106		
Media Server User Guide	Host Port			
Support Report	Relative Distinguished Names (RDN)	CN+%username%,00+Employees,00+Cisco Users		
	Domain Controllers (DC)	dc=cisco,dc=com		
	Delimiter			
	Select Homepage			
	Change default homepage to VSOM	e		
	Change default homepage to VSMC	c		
		Update Reset		
				1

• **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 branch.

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 branches. 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 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
binarv
cd $serverDIR
mput VSOM_MSP-DC-1_backup_20$(date +%y%m%d)*.tar.gz
quit
EOF
```

exit O

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 organizations 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).



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.

Models As	sessed
Cisco Phys	sical Access Manager version 1.2.0
PCI Sub-Re	equirements 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-Re	equirements Requiring Compensating Controls
No compe	nsating controls were required to satisfy any sub-requirements.
PCI Sub-Re	equirements Failed
No sub-red	quirements were failed.

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

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 5-9 lists the component assessment details for Cisco Physical Access Control.

PRIMARY FUN Limit and m REQUIREMENT	nonitor pysical access to sensitive a	areas within the cardholder environment
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	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]
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.
+	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)
+	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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)
1	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 5-9 Component Capability Assessment – Cisco Physical Access Control

Design Considerations

Best practices are as follows:

- Use high availability for Cisco Physical Access Manager (PAM) servers.
- Map each branch 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

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT, see the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

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

To meet all of the requirements listed below, the PCI solution 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.)

Г

Events & Alarms Users Doors Admin Reports O	ptions Help		
📝 Edit 📑 Add 📄 Duplicate 🔟 Disable	🕤 📓 Repo	rt 🐙 Column:	s 🚔 Filter 🝷
Name	Enabled	Site	
le Administrators	Yes	SanJose	
Administrators Door Monitors System Config Users	Yes	SanJose	
lisers System Config Users	Yes	SanJose	

Figure 5-13 Profiles Module Main Window



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	~	ų
	ОК	Cancel	24716

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

Figure 5-15 Profile—General Tab

🔞 Edit - Pro	ofile	
📳 Save and C	ilose 👜 Report	
Profile name:	Administrators	
	Enabled	
Site:	SanJose	
General M	odules Device Commands Data Types	Allow access to the application
Ge	neral	Allow issuing device commands
	ents/Alarms	Allow access to external hyperlinks
He	lp	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.		
<i>Require device commands to be commented</i>	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.		
Allow logoff without password	Allows user to logoff without a password.		
Events/Alarms: Alarm Annotations (A	.ck., 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. Adobe PDF viewer is required.

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

- **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	Allow access to module
🖃 🧁 Modules 🛛 🔼	Default Filter
🖻 🗁 Navigation	
🛄 Quick Launch	
🕂 🏫 Start Page	
Web Browser	
🖻 🗁 Monitoring	
Events	
- Alarms	
Audit Trail	
Event Photos	
Graphic Map Viewer	
EDI Monitoring	
Officer Post	
Camera Manager	
<	467
	076.467

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

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

Edit - Profile	
Save and Close 🛛 👜 Report	
rofile name: Administrators	
Enabled	
Site: SJC	
General Modules Device Commands Data Types	Allow command to be issued: Default 👻
🖨 💭 Gateway Driver 🔼	Filter
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 - Pr	ofile					
🔚 Save and 🤇	Ilose (🖻 Report				
Profile name:	Admin	istrators				_
	🗹 Ena	bled				
Site:	SJC					
General M	odules	Device Commands	Data Ty	ypes	View	
🖃 🗁 Da			_	^	Create	
	Badge Badge	Custom Value 0		=	Modify Delete	
	-	Custom Value 1 Custom Value 2				
	-	Custom Value 3				
	-	Custom Value 4				
		Custom Value 5 Custom Value 6				
	-	Custom Value 7				
		ct Information				
		Idresses				
		nail Addresses Ione Numbers				
	Depar					
		omments				
	🔷 Na	ame		~		
<			>			
						_

- **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 5-11Profile – 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

	5015 20015	Admin Repo	rts Options	Help			
🖁 Edit 📑 😭 Add	I 💥 Disa	ble 👌 Report	t 🐙 Colur	nns 📫 Filter 🔹 🔍 Search 🝷			
Username	Validity	Effective	Expires	Assigned to	Comments	Site	^
6 CEO	Active			CEOO, Dr. CEO1		SJC	
5 cpamadmin	Active					SJC	
gwashington	Active					SJC	
jadams	Active					SJC	_
5 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	
LIRL D	Active			URL, Ms, URL Delete-user?NoView		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.



e 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

ave and Close 🗎		
General	General	
Profiles Audit Records	Username:	gwashington
Recent Events	Password:	•••••
	Confirm password:	•••••
	Assigned to:	View Select Clear
	Validity:	Active
	Effective:	5/1/2009
	Expires:	7/1/2011
	Site:	SJC
	Comments:	First user

<u>Note</u>

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

Field	Description
Username	Required—The username of the login.
Password	Required—Password to access the system.
Confirm pass- word	Required—The value must be entered exactly as it was in the Password field.
Assigned to	The personnel record the login is assigned to.
	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, "Config-
	uring 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 indefi-
	nitely.
Site	Read-only—A site is a single instance of a Cisco PAM database.
Comments	Comments or notes about the login.

Table 5-12 General Tab Fields

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.



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.

General Profiles Audit Records Recent Events	Profiles				
	All egran-wxp04 Administrators W	egran-wxp04 - Hardware (

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.

🐻 System Configuration - Cisco Physical Access Manager
Events & Alarms Users Doors Admin Reports Options Help
🔚 Save
LDAP Personnel ID Number Generator
Events/Alarms
Data Entry/Validation - Personnel
Data Entry/Validation - Badge
Password Policy Custom Personnel Fields
Custom Device Fields
Custom Badge Fields
Personnel ID Number Generator
PIN Generator
Card Number Generator
Support Contact Information
Badge Design Miscellaneous
Cisco Settings
Cisco setungs
Alarms: 1 active cisco - cpam-demo

Figure 5-23 Using the Personnel ID Number Generator

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

Add - Personnel Record			•
Save and Close 📓 Report			
General	General		
Occupational Information Contact Information	No Photo.	Title: First name:	
Badges Logins		Middle name:	L
Custom Audit Records		Last name:	
Recent Events		Suffix:	
		Date of birth:	
		ID# ▼ Comments:	870542135
	🚵 Import	1	cpam-demo
	No Signature.	-	
	🔁 Import]	

290967
- **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 5-13LDAP 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://	
	Example: ldap://192.168.1.1:389	
	Note 389 is the port number.	
Principle suffix	Appended to the username for authentication. See above.	

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.
	• 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.
	• 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

Table 5-13 LDAP System Configuration Settings (continued)

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

System Configuration - Cisco Pl	hysical Access Manager	
Events & Alarms Users Doors Admin	Reports Options Help	
Events & Alarms Users Doors Admin Save LDAP — Password Policy — Events/Alarms — Data Entry/Validation - Personnel — Data Entry/Validation - Badge — Custom Personnel Fields — Custom Device Fields — Custom Badge Fields — Custom Badge Fields — Personnel ID Number Generator — PIN Generator — Card Number Generator — Support Contact Information — Miscellaneous — Cisco Settings	Reports Options Heip LDAP LDAP server URL: Idap://10.10.82.14:389 Principal suffix: @ad1.cpamlab Principal prefix: Search root: DC=ad1,DC=cpamlab LDAP version: JNDI authentication type: simple JNDI factory: com.sun.jndi.ldap.LdapCtxFactory	
	cpamadmin -	SanJose

LDAP Example—sAMAccountName

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

Events & Alarms Users Doors Admin	Reports Options Help
Nave Save	
LDAP Password Policy Events/Alarms Data Entry/Validation - Personnel Data Entry/Validation - Badge Custom Personnel Fields Custom Device Fields Custom Badge Fields Personnel ID Number Generator PIN Generator Card Number Generator Support Contact Information Miscellaneous Cisco Settings	LDAP LDAP server URL: Idap://10.10.82.14:389 Principal suffix: CN=Users,DC=ad1,DC=cpamla Principal prefix: CN= Search root: CN=Users,DC=ad1,DC=cpamla LDAP version: 3 JNDI authentication type: simple JNDI factory: com.sun.jndi.ldap.LdapCtxFactor

Figure 5-26 sAMAccountName – LDAP Configuration Example

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

General	General	
Profiles Audit Records	Login type:	LDAP 💌
Recent Events	Username:	cpsm.user1
	Password:	•••••
	Confirm password:	•••••
	Assigned to:	View Select Clear
	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.



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 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.

Cisco PAM Server Administration Monitoring Setup Setup Setup Setup Date & Time Date and Time: Date a Time Date a Time Date a Time Date and Time: Date and Time:	(*) [192.168.44.111 https://192.1	X Wdeo Surveillance Management Console X + 168.44.111/setup/show/datetime 2 C Socie P feedback - JIM NCM WCS TACACS RSA enVision HyTrust CM-2 RSA-AM the VSOM Bookmarks
Wetwork Date and line: 06/28/11 15:08:41 DNS Time Zone: America/Los_Angeles Email Image: NTP Enable Locense NTP Server Address*: Locense NTP Server Address*: Backup Update Cancel Archive Restore	CISCO Monitoring Setup Commands La	aunch CPAM Client Downloads
@ 2008-2011 Cisco Systems, Inc. All Rights Reserved.	Wetwork DNS Email Date & Time License Log Level Backup Partorie Restore	Time Zone: America/Los_Angeles MTP Enable NTP Server Address*: 192.168.62.161 Update Cancel

Figure 5-28 Cisco PAM NTP Configuration

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 - Auto	mation Rule
🔡 Save and C	lose
	Enabled
Name:	Send Audit Reports
Trigger:	Edit New Clear
	Edit E Add A Move Up A Move Down S Delete
Actions:	
	Edit New Clear Image: Constraint of the second event when trigger fails Image: Constraint of the second event when action fails Image: Constraint of the second event when notification fails Image: Constraint of the second event when notification fails

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

Figure 5-30	Selecting Periodic
🔞 Select Trigger Ty	pe X
Type: Periodic	•
ОК	Cancel 8

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	
OK Cancel	02000

- Step 5 Under Actions, Click Add...
- Step 6 Select Report. (See Figure 5-32.)

Figure 5-32	Selecting Action	Туре
0	•	<i></i>

🐻 Sel	ect Action Type	×	
Type:	Report	-	
	Report		Ţ,
	Device Command CSV Import		290971

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

Figure 5-33 Audit Records–All

n Choose Report	
Audit Records - All	
More Cisco Templates Events - All Personnel - Active Schedule(s) - Not Used Audit Records - All Badges - All Access Policy - Door Groups vx_cred_valid_type vx_cred Badges - Access Policy	
Vx_dev Events - All - Count Sec nike assignment OK Cancel	

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

Figure 5	-34	Save and Close	
	D .		

×
Choose

. ...

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

🔞 Sel	ect Notification Type	×	
Type:	E-mail	-	
	E-mail		22
	FTP		2000
	Svsloa	2	ŝ

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

Figure 5-36 FTP Notification

ſ	🐻 FTP Notif	ication	
	Host:		
I	Username:		
	Password:		
	Path:		
		OK Cancel	200976

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.

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.

<u>Note</u>

Figure 5-37 Enable IronPort	t Message Tracking	
IRONPORT C670		Logged in as: bmcgloth on ESA-IE-1.cisco-irn.com Options Y Help and Support Y
Monitor 🗸 🛛 Mail Policies 🗡 Sec	curity Services 👻 🛛 Network 👻	System Administration 👻
Message Tracking Service Sel Message Tracking Service Renable Message Tracking Service	ttings	No Changes Pending
Message Tracking Service	C Centralized Tracking	racking, ensure that the Security Management Appliance is configured to appliance.
Rejected Connection Handling	: Save tracking information for For optimum performance, lea	
Cancel		Submit 50

• 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.



Severity Settings				
Critical Severity Settings				
Action Applied to Messages:	Drop			
⇒ Advanced	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:	Dinclude original message as an attachment.		
		PCI Compliance		
		Preview Message 🗗		
		Preview Message 🗗 (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

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 ٠

Table 5-14 PCI Assessment Summary-Cisco UCS

Models As	Models Assessed			
Cisco UCS	Cisco UCS Manager version 1.3(1p)			
PCI Sub-Re	equirements 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			

Γ

No sub rec	quirements were failed.
PCI Sub-Re	equirements Failed
No compe	nsating controls were required to satisfy any sub-requirements.
PCI Sub-Re	equirements Requiring Compensating Controls
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

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

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 an organization to separate its payment systems (in-scope) from other non-sensitive data (out-of-scope).

Table 5-15 lists the component assessment details for Cisco UCS.

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

PRIMARY FUN Securely ho REQUIREMEN ⁻	st payment applications			
ASSESSMENT	CAPABILITY			
	SECURITY SERVICES			
\checkmark	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)		
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)		
\checkmark	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)		
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)		
	AUTHENTICATION			
\checkmark	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.		
+	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)		
╋	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)		
	LOGS/ALERTS			
+	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)		
1	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.

L

Cisco Unified Computing System Manager - DC-U	CSFabric		
ault Summary	🔆 🕒 🗉 New - 🏹 Options 🛛 😯 🕕	0 Exit	
	>> 🛱 All > 🔚 Communication Management	Communication Services	Communication Service
0 15 9 4	Communication Services Events FSM	Communication Services	
uipment Servers LAN SAN VM Admin			
Filter: Al	НТТР	Telnet	
	Admin State: O enabled O disabled	Admin State: O enabled O disabled	
AI AI			
🖃 🕂 Faults, Events and Audit Log	HTTPS		
Core Files	Admin State: enabled disabled	Admin State: O enabled O disabled	
Faults			
	Port: 443		
Syslog	Key Ring: KeyRing default 🚽 🔻		
Grand System Grand System Grand System System			
Authorization	SNMP		
	Admin State: O enabled O disabled		
🖨 🖶 TACACS+			
192.168.42.131 (1)	SNMP Traps		
User Services			
🎇 Locales	🛨 🖃 💐 Filter 👄 Export 😸 Print		
E Cocally Authenticated Users	Name Community	Port 🐺	
Remotely Authenticated Users Reles	Community	Port	
Key Management			
KeyRing default			
Communication Management			
Call Home			
Communication Services			
DNS Management			
Management IP Pool (ext-mgmt)			
Management Interfaces	SNMP Users		
🖃 🖳 Stats Management			
🖃 🖳 Stats Policies	🛨 🖃 👄 Export 🍰 Print		
- 🗐 Collection Policy adapter	Name	R.	
Collection Policy chassis	- Norric		
Collection Policy host			
Collection Policy port			
S Collection Policy server			
arrie fabric			
Internal LAN LAN Cloud			
EAN Cloud			
⊡-å root			
S thr-policy-default			
Sub-Organizations	SMASH CLP	SSH	
Timezone Management			
Capability Catalog	Admin State: enabled	Port: 22	
Adapters			
CPUs			Save Changes Reset Values
			Save Changes Reset Values

Figure 5-40 Secure Management Protocols

• **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.)

Cisco Unified Computing System Manager - D	C-UCSFabric		
ault Summary	🗄 🤤 🏐 🗈 New 🗸 🏹 Option	ns 🕜 🕕 🔟 Exit	-ijoj cisci
0 15 9 4	>> 🛱 All + 🔑 Key Manageme	nt + 🥕 KeyRing default	🔑 KeyRing default
quipment Servers LAN SAN VM Admin	General Events		N
Filter: Al	Actions	Properties	
	+ Create Certificate Reg	Name: default	
Authorization	Delete Certificate Regu		
LDAP		Request	8
RADIUS		Certificate	8
		Certificate	•
Locales			
🖨 🚟 Locally Authenticated Users			
- A admin			
bmcgloth chjanoff			
Remotely Authenticated Users			
bmcgloth			
😥 🏭 Roles			
- P Key Management			
KeyRing default			
Communication Management Communication Management Communication Management			
Communication Services			

Figure 5-41 1024-Bit Mod Key Default Keyring

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

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT, see the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

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				
Fault Summary	🗄 🕒 💷 New 👻 🏹 Optio	ns 😢 🕕 🔟 Exit		
	>> 🛱 All 🕨 🔒 User Managem	ent 🕨 🔒 TACACS+		TACACS+
Equipment Servers LAN SAN VM Admin	General Events FSM			
Filter: Al	Actions	Properties		
± =	Create TACACS+ Provi			
Faults, Events and Audit Log		TACACS+ Providers		
🛛 👩 Core Files		🔍 Filter 👄 Export 🗞	Print	
Events		Hostname	Order Port	
		192.168.42.131	1 49	^ ^
Syslog				
Authorization				
ADIUS				
E TACACS+				
□ 192.168.42.131 (1) □ 24 User Services				
- A Locales				-
Locally Authenticated Users Remotely Authenticated Users				
Roles				
Key Management KeyRing default				
Communication Management				
Call Home				
Communication Services				
Management IP Pool (ext-mgmt)				
Management Interfaces				
🖃 🖳 Stats Policies				
Collection Policy adapter				
🔟 Collection Policy host				
Collection Policy port			Save	Changes Reset Values
Logged in as bmcgloth@ucsmanager.cisco-irn			Syste	m Time: 2011-06-03T15:50

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

290990

🛕 Cisco Unified Computing System Manager - DC	-UCSFabric	
Fault Summary	🗄 😋 🏐 🖽 New 🕞 🛃 Options 🧭 🚯 🗿 Exit	ajiaji. Cisco
0 15 9 4	>> 🛱 All > 🔒 User Management > 🔒 Authorization	🔒 Authorization
Equipment Servers LAN SAN VM Admin	General Events FSM	
Filter: All	Console: tacacs	

Figure 5-43 Authorization – Selecting Console and Default Settings

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		
cisco	Jump To Access Restricti	ions 💌
User Setup Shared Profile Components Network Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Control Control Control Network Access Posture Validation Control Control <th> Shell (exec) Access control list Auto command Callback line Callback rotary Idle time No callback verify No escape No hangup Privilege level Timeout Custom attributes shell:Admin*Admin default-domain cisco-av-pair*shell:roles="network-admin admin shell:PCL*Admin default-domain </th> <th></th>	 Shell (exec) Access control list Auto command Callback line Callback rotary Idle time No callback verify No escape No hangup Privilege level Timeout Custom attributes shell:Admin*Admin default-domain cisco-av-pair*shell:roles="network-admin admin shell:PCL*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 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.



Image: Source Control Image: Source Contr	🛕 Cisco Unified Computing System Manager - DC-UCSFabric			
Start Comment Servers LAU SAAL ON Rome Intern Autorstore	Fault Summary			المملو
	🛛 🔍 🔨 🛆			
Regeneral Servers LAN SAN Month Ritter Al	0 15 9 4	>> 🛱 All 🕨 📺 Timezone Manag	ement	📺 Timezone
Filter: Alignet Control Control A Events Control A Settrage Control A Settrage Control A Address Control A Robing		General Events		
Image: Add MP Server Image: Dents Image: Dents <	Equipment Servers LAN SAN VM Aumin	Antinan	Burgensting	
Interaction (Add Angleses (Pacific, Links) Formation Format	Filter: All		roperues	
A chuis A	± =	Add NTP Server	Timezone: America/Los_Angeles (Pacific Time)	
A chuis A	Events		NTP Servers	
As years A uthorston A strends/value Communication Management A strends/value Communication Services A strends/value Collection Policy dapter Collection Policy dapter Statis Management Statis Policies Statis Policies Statis Policies Statis Policies Statis Policies Collection Policy dapter Statis Policies Statis Policies A shapters A shapters A shapters A coblosis				
User Management User Management DAP ADUS TACACS+ Stoolers Balas Communication Management Communication Management Communication Management Communication Management Communication Management Context Polo (extrogont) Collection Policy value State Management the Polo Collection Policy value State Management State Management State Management State Management State Management State Management State Management Management Market State Management State Management State Management Management Market State Management Management Market Management Marke			el Filter ⇒ Export © Print	
Authorization Authori			Name	T
Charter Services Collector Policy adapter Solector Policy default Collector Policy policy Solector Policy policy Solector Policy policy Solector Policy default Solector Policy Berley Solector Policy Default Solect			INTP Server 192.168.62.161	
Colors Services Colors Services Colors Reases Reast Values Colors Nanagement Saw Change Colors Colors Nanagement Colors Colors Colo			MTP Server 192.168.62.162	
Collector Policy adapter Collector Policy adapter Collector Policy server Collector Policy Policy San Could Collector Policy Policy San Could Collector Policy Policy Collector Policy Policy San Could Collector Policy San Could Sa				
Localy Authenticated Users Reiter Re				
Remotely Authenticated Users Roles				
Remotely Authenticated Users Roles	Locales			
KeyRing default Communication Management Communication Management Communication Services Dis Management IP Pool (extramnt) Management ID refraces Stats Management Stats Management Solution Policy datapter Solution Policy datapter Solution Policy adapter Solution Policy post Solution Policy post Solution Policy server Solution Policy adapter Solution Policy server Solution Policy adapter Solution Policy post Solution Policy adapter Solution Policy post Solution Policy adapter Solution Policy adapt	Remotely Authenticated Users			
Key Management Key Management Cal Home Cal Home Communication Management Pool (ext-mgmt) Management Pool (ext-mgmt) Management Therfaces Stats Polices Stats Polices Scalection Poly adapter Scalection Poly of basis Memory Unit				
Communication Nanagement Communication Services Communication Services DNS Management Pool (ext-mgmt) Management Interfaces Sate Management Interfaces Sate Management Interfaces Sate Management Interfaces Sate Collection Policy datapter So Collection Policy prott So Collection Policy port So Collection Policy port So Collection Policy port So Collection Policy port So Collection Policy server Cate Internal LAN Cate Collection Policy adapter Cate Collection Poli	🚊 🔑 Key Management			
Call Home Communication Services Communication Services Communication Services Communication Services State Management Therfaces State Management State Management Collection Policy dapter Collection Policy dapter Collection Policy pott Collection Policy pott Collection Policy pott Collection Policy pott Collection Policy pott Collection Policy pott Collection Policy default A sub-Organizations Communications Consumer Consumer Collection Policy default A sub-Organizations Consumer Consumer Consumer Consumer Consumer Collection Policy default Collection Policy default Consumer Con				
Communication Services Not Management Proof (ext-mgmt) Management Interfaces Stats Management Collection Policy adapter Collection Policy post Collection Policy post C				
ONS Management Imagement Iberfaces Stats Management Interfaces Stats Paloices Stats Paloices Scalecton Policy adapter Scalecton Policy host Scalecton Policy port Scalecton Policy port Scalecton Policy port Scalecton Policy default Imagement Imagement Stats Paloices Scalecton Policy host Scalecton Policy port Scalecton Policy default Stats Polices Imagement Stats Polices Stat				-
Management IP Pool (ext-mgmt) Management Interfaces Stats Poloies Stats Poloies Stats Poloies Stats Poloies Stats Poloies Soluction Policy adapter Soluction Policy nost Soluction Policy port Soluction Policy server Soluction Policy server Soluction Policy server Soluction Policy of aut Soluction Policy default Soluctions Soluctions Soluctions Soluctions Soluctions Soluctions Soluction Soluctions Soluction				
Stats Management Image: Stats Policies Stats Policies Scalection Policy adapter Scalection Policy parts Scalection Policy port Scalection Policy Policy Actions Scalection Policy Policy Adapters Actions Applie Scalection Policy Policy Adapters Actional Policy Scane Changes R	Management IP Pool (ext-mgmt)			
Image: State Policies Image: State Policies Image: State Policies Image: State Policy adapter Image: Scalection Policy post Image: Scalection Policy post				
Scalection Poley adapter Scalection Poley hosts Collection Poley port Scalection Poley port Scalection Poley server Thread LAN Could SAN Cloud SAN Cloud SA				
Collection Policy chassis Collection Policy post Collection Policy post Collection Policy post Collection Policy server Collection Policy server Collection Policy server Collection Policy server Collection Policy default Colle				
Collection Policy host Collection Policy port Collection Policy server Fabric Fabric Collection Policy server Fabric Collection Policy server Fabric Fabr				
Collection Policy server ☐ fabric ☐ Internal LN ☐ LAN foud ☐ SAN Cloud ☐ SAN Cloud ☐ San Could ☐ San Could ☐ San Could ☐ Sub-Organizations ☐ Capability Catalog ☐ Ca				
Internal LAN Internal LAN LAN Cloud Save Organizations Internal LAN Sthr-policy-default Save Organizations Internal LAN Capability Catalog Adapters Servers Volution Servers				
Internal LAN LAN Cloud Canolity Catalog Adopters				
Save Changes Reset Values				
A rot Sub-Organizations Adopters Adopter				
Asub-Organizations Immezone Management Compatibility Catalog Adapters Adapters Adapters Adapters Achassis Acha	- et root			
Capability Catalog Capability Catalog Cata				
Capability Catalog X Adapters X Adapters X CPUs X Fan Modules X Fan Modules X Local Disks X Memory Units X Servers				
-X. Adapters -X. CPUs -X. Chassis -X. Chassis -X. To Modules -X. Io Adolules -X. Local Disks -X. PSUs X. Servers				
- X CPUS - X Chassis - X Fan Modules - X IO Modules - X IO Modules - X Local Disks - X PSUs - X Servers - X Server				
- X Chassis - X Fan Modules - X I D Modules - X Local Disks - X Memory Units - X Servers -				
- X IO Modules - X Local Disks - X PSUs - X Servers -				
- X Local Disks - X Memory Units - X PSUs - X Servers - X Servers - X				
A Memory Units 				
A PSUs Save Changes Reset Values				
				Save Changes Reset Values
B Logged in as bmcgloth@ucsmanager.cisco-irn System Time: 2011-06-03T15:54				Neact values
	A 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

🚖 Cisco Unified Computing System Manager - DC-UCSFabric			
Fault Summary			
	😧 🍥 🗉 New 🖌 🏹 Options 🔞 🚺 🔯 Exit		
0 15 9 4	>> 🛱 All 🕨 📉 Faults, Events and Audit Log 🕨 📉 Syslog	Syslog	
0 12 9 4			
Equipment Servers LAN SAN VM Admin	Syslog		
	Local Destinations	Remote Destinations	
Filter: All			
÷ =	Console	Server 1	
	Admin State: O enabled O disabled	Admin State: enabled disabled	
Faults, Events and Audit Log			
		Level: information	
🙆 Core Files	Monitor	Hostname (or IP Address): 192.168.42.124	
	Admin State: • enabled • disabled	Facility: local7	
	Aumin State: O enabled O disabled		
<mark></mark> X Settings X Syslog	Level: information	Server 2	
Systog Systog User Management			
Authorization	File	Admin State: O enabled O disabled	
	Admin State: • enabled disabled		
TACACS+	Level: information		
🖻 🤮 User Services	Name: messages	Server 3	
Locales		Admin State: O enabled O disabled	
E- Remotely Authenticated Users	Size (KB): 4194304	Admin State: O enabled O disabled	
E			
Erent Key Management			
KeyRing default			
🖃 🖥 Communication Management			
Call Home 😑			
Management IP Pool (ext-mgmt)			
Anagement Interfaces			
Stats Policies			
Scollection Policy adapter			
S Collection Policy chassis			
S Collection Policy host			
S Collection Policy port			
S Collection Policy server			
i fabric			
Internal LAN			
E-C LAN Cloud			
⊡s root			
Sub-Organizations			
Timezone Management			
Adapters			
CPUs	· · · · · · · · · · · · · · · · · · ·	•	
		Save Changes Reset Values	
TO Modules			
A Logged in as bmcgloth@ucsmanager.cisco-irn		System Time: 2011-06-03T15:53	

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 (UCS) Express and Services Ready Engine (SRE) allows organizations to securely deploy sensitive applications directly within the routing platform. By using the UCS E-series, organizations can remove legacy compute resources in the branch, saving space, energy, and operational costs.

Cisco UCS E-series is a converged networking, computing, and virtualization platform for hosting essential business applications in the branch 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 branch 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 As	sessed		
Cisco UCS	S Express version 1.1 on SRE900		
PCI Sub-Re	equirements 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, 8.5.5, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14		
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-Re	equirements Requiring Compensating Controls		
No sub-requirements were failed.			
PCI Sub-Re	equirements Failed		
No sub-requirements were failed.			

Primary PCI Function

The main function of the 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 an organization to separate its payment systems (in-scope) from other non-sensitive data (out-of-scope).

Table 5-17 lists the component assessment details for the Cisco UCS Express and Cisco SRE.

PRIMARY FUN Securely ho REQUIREMENT	st payment applications	
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	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)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.
+	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)
╋	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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)
1	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 5-17 Component Capability Assessment-Cisco UCS Express and Cisco SRE

Design Considerations

The major consideration when using Cisco UCS Expresss 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 1.5 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.

<u>Note</u>

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.



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 branch, 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.

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT, see the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

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

The relevant sub-requirements of Requirement 7 were met using the vCenter 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 the ESX hypervisor as part of the vSphere and vCenter infrastructure.

• **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.

- 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.

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 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 E-Series NTP Servers

Resource Allocation Performa	ance Configuration Local Users & Groups Events Permissions	
Time Configuration		
General		
Date & Time	21:28 6/23/2011	
NTP Client	Running	
NTP Servers	192.168.62.161, 192.168.62.162	291526

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

No sub-requirements were failed.

PCI Assessment Detail—PCI Sub-Requirements Failed

No sub-requirements were failed.

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

Г

Models As	sessed	
Cisco Secu	ure Access Control Server Release 4.2(1) Build 15 Patch 3	
PCI Sub-Re	equirements 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-Re	equirements Requiring Compensating Controls	
No compe	nsating controls were required to satisfy any sub-requirements.	
PCI Sub-Re	equirements Failed	
No sub-rea	quirements were failed.	

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

Primary PCI Function

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

Table 5-19 lists the component assessment details for Cisco Secure ACS.

PRIMARY FUNCTION Securely authenticate users to systems in the cardholder environment REQUIREMENT: 7, 8 (7.1, 7.2, 8.2)			
ASSESSMENT	CAPABILITY		
	SECURITY SERVICES		
\checkmark	Disable Any Unnecessary Services	"Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove a unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)	
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)	
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)	
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)	
	AUTHENTICATION		
\checkmark	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.	
\checkmark	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)	
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)	
	LOGS/ALERTS		
+	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)	
1	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 5-19 Component Capability Assessment—Cisco Secure ACS

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



<u>Note</u>

Server hardening, including appropriate security settings for all system components, is the responsibility of the organization/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

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

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.

L

Firefox 🔻		
CiscoSecure ACS	+	*
() 🔶 🜔 🚺 cisco-irri	.com https://tacacs.cisco-irn.com:2005/index2.htm	🚖 🕶 🕑 🛃 = Google 👂 🍙 Feedback •
Most Visited 🐝 Cisc	o UCS Manager 📄 UIM 📄 NCM 📄 WCS 👩 TACACS 🧭 RSA enVision 📄 HyTrust 🚟 CM-2 📄 RSA-	AM 號 VSOM 📴 RSA-KMA 🚾 RSA Access Manager:
	Administration Control	X
cisco		n
User Setup	Administrator Password Policy Setup	Password Validation Options Password Justime Dations Password Instrume Options Password Instrume Atomatic Options Instrume L Password Atomatic Options
Shared Profile Components	Password Validation Options	Use this page to configure the Administrator password policy.
- Net work	Password may not contain the username	Password Validation Options
Configuration		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
Configuration	Minimum length 7 characters	length is 4. • Password must contain: - Use these options to determine the password complexity constraints.
-99 L Administration	Password must contain:	 Uppercase alphabetic characters - If enabled, the password must contain uppercase alphabetic characters.
Control	🗹 lower case alphabetic characters	 Lowercase alphabetic characters - If enabled, the password must contain lowercase alphabetic characters.
Databases	🗹 upper case alphabetic characters	 Numeric characters - If enabled, the password must contain numeric characters.
Posture Validation	numeric characters	 Non alphanumeric characters - If enabled, the password must contain non alphanumeric characters.
Network Access Profiles	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).
Reports and		[Back to Top]
Activity	Password must be different from the previous:	Password Lifetime Options
Documentation	4 versions	 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.
	Password Lifetime Options	 The password will require change after (s) 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.
	Following a change of password:	• The Administrator will be locked out after (x) days - Following a change of
	The password will require change after 90 days	password, if enabled, x specifies the number of days before ACS locks out the associated administrator account due to password age (default = 60,
	The Administrator will be locked out after 60 days	range = 1 to 365). [Back to Top]
		Password Inactivity Options
	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
	Following last account activity:	since the activity (administrator login).
	The password will require change after 30 days	 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
	The Administrator will be locked out after 90 days	change of password due to password age (default = 30). The range is 1 to 365.
	Incorrect Password Attempt Options	 The Administrator will be locked out after (X) days - Following a change of password, if anablad, x specifies the number of days before ACS locks out the associated administrator account due to password age (default = 60, range = 1 to 365).
	Lock out Administrator after 6 successive failed attempts	[Back to Top]
		Incorrect Password Attempt Options
	💡 Back to Help	Lack 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.
	Submit Cancel	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.

Figure 5-51 Administrator Password Requirements

• **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

Firefox *				
CiscoSecure ACS	+	÷		
(cisco-irn	.com https://tacacs.cisco-irn.com:2005/index2.htm	🚖 - C 🚼 - Google 🔎 🍙 Feedback -		
Most Visited	o UCS Manager 📄 UIM 📄 NCM 📄 WCS 👩 TACACS 🏈 RSA enVision	HyTrust 號 CM-2 📄 RSA-AM 號 VSOM 🛛 🔹 Bookmarks		
cisco	Administration Control			
User Setup Group Setup (49. Shared Profile	Session Policy Setup	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.		
Components	Session Configuration ?	[Back to Top]		
Network Configuration	Session idle timeout (minutes)	Session idle timeout (minutes)		
System Configuration	□ Allow automatic local login	Type the number of minutes of inactivity after which the browser terminates the remote administration connection. The default is 60 minutes.		
Configuration	Respond to invalid IP address	[Back to Top] Allow automatic local login		
Administration Control		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.		
Doon Posture Doon Validation		[Back to Top]		
Network Access Profiles Reports and Activity Online Documentation	💡 Back to Help	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 connaction attempt is made. Administrators can disable this option to prevent unauthorized identification of ACS. This option is checked by default.		
	Submit Cancel	[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 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.

Firefox 🔻		
CiscoSecure ACS	+	· · · · · · · · · · · · · · · · · · ·
(la cisco-irn.	com https://tacacs.cisco-irn.com:2005/index2.htm	🟫 - C 🚱 - Google 🔎 🍙 Feedback -
A Most Visited	o UCS Manager 📄 UIM 📄 NCM 📄 WCS 👩 TACACS 🍼 RSA enVision 📄 HyTrust 端 CM-2 📄	RSA-AM 🗯 VSOM 👷 RSA-KMA 🕵 RSA Access Manager:
	Administration Control	X
cisco		
cisco		
User Setup	Administrator Password Policy Setup	Password Validation Options Password Infettine Options Password Infettive Options Incorrect Password Attempt Options
Shared Profile	Password Validation Options ?	Use this page to configure the Administrator password policy.
Network	Password may not contain the username	Password Validation Options
System Configuration	Minimum length 7 characters	 Password may not contain the username - If enabled, the password cannot contain the username or the reverse username. Minimum Length - there 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
Configuration	Password must contain;	constraints. • Uppercase alphabetic characters - If enabled, the password must contain
Administration Control	✓ lower case alphabetic characters	uppercase alphabetic characters - If enabled, the password must contain
= External User	✓ upper case alphabetic characters	lowercase alphabetic characters. • Numeric characters - If enabled, the password must contain numeric
JU Databases	✓ upper case aphaoetic characters	characters. • Non alphanumeric characters - If enabled, the password must contain non
Conn Posture Validation	non alphanumeric characters	alphanumeric characters.
Network Access Profiles		 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]
Reports and Activity	Password must be different from the previous;	Password Lifetime Options
Online Documentation	4 versions	 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 vas changed.
	Password Lifetime Options	 The password will equine change after (x) days - Following a change of password, if enabled, is specifies the number of days before ACS requires a password but for password day to password age (darault = 03). The range is 1 to 265, if an arrive and the specific days are also be able to be able
	Following a change of password:	The Administrator will be locked out after (x) days - Folloving a change of
	The password will require change after 90 days The Administrator will be locked out after 60 days	password, if enabled, × specifies the number of days before ACS locks out the associated administrator account due to password age (default = 60, range = 1 to 363).
		[Back to Top]
	Password Inactivity Options ?	Password Inactivity Options
	Following last account activity.	 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 30 days	• The password will require change after (x) days - Following a change of
	The Administrator will be locked out after 90 days	password, if enabled, × specifies the number of days before ACS requires a change of password due to password age (default = 30). The range is 1 to 365.
	Incorrect Password Attempt Options	 The Administrator will be locked out after (X) days - Following a change of password, if enabled, x specifies the number of days before ACS lock out the associated administrator account due to password age (default = 60, range = 1.6 365).
	Lock out Administrator after 6 successive failed attempts	[Back to Top]
		Incorrect Password Attempt Options
		Lock out Administrator after (x) successive failed attempts - Enable this option to
	Back to Help	 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.
	Submit Cancel	 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]

Figure 5-53 Syslog for Passed Authentications

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.

Models As	sessed
RSA Auth	entication Manager 7.1 Service Pack 2
PCI Sub-Re	equirements 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-Re	equirements Requiring Compensating Controls
No compe	nsating controls were required to satisfy any sub-requirements.
PCI Sub-Re	equirements Failed
No sub-rec	uirements were failed.

 Table 5-20
 PCI Assessment Summary—RSA Authentication Manager

Primary PCI Function

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

Table 5-21 lists the component assessment details for RSA Authentication Manager.

PRIMARY FUN Securely au REQUIREMEN	thenticate remote users using two	o-factor authentication
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	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)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
\checkmark	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.
\checkmark	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)
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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)
1	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 5-21 Component Capability Assessment—RSA Authentication Manager

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.

	arch 👷 Favorites 🤣 😥 - 😓 🕞					
e 🍘 https://rsa-am.cisco-irn.com:70	004/console-ims/ListUser.do					💌 🄁 Go 🛛 I
Security Cons	sole		Logged o	n as: bmcglo		<u>My Preferences</u> <u>Log C</u> nDomain <u>Configurati</u>
Identity - Authentication -	Access V Reporting V RADIUS Ad	ministration 👻 Setup 💌	Help 🔻			
Users V					1	Help on this page *
User Groups	▶ ▶					Theip off this page
A Identity Attribute Definitions	stem with a unique account within this realm.					
Count	4 found. Showing 1-4.					
Search	0 selected: Add to User Groups	Go 🔁				Show 250 💌 per page
Security Domain:	User ID	Last, First Name	Disabled	Locked	Security Domain	Identity Source
Identity Source:	□ 🕞 bart 👻	mcglothin, bart			[ং] ন্: SystemDomain	Internal Database
Internal Database 💌	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	McGlothin, Bart			°্≓ু SystemDomain	Internal Database
For:	🗖 🙀 chjanoff 🗸	janoff, Christian			°ন্∵ SystemDomain	Internal Database
Where:	SelfServiceAdmin_zw44oqry -	Administrator, Self-Service	~		°ন্∷ SystemDomain	Internal Database
User ID 🔹	User ID	Last, First Name	Disabled	Locked	Security Domain	Identity Source
starts with	0 selected: Add to User Groups	Go 🔁	1			Show 250 💌 per page
More criteria	4 found. Showing 1-4.					
Search >	-					
Advanced Search						
Auvanceu bearch						
	Copyright ©2007 - 200	8 RSA Security Inc. All rights I	reserved.			

Figure 5-54 Users and Groups

- 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.

ress	https://rsa-am.cisco-irn.com:700)4/console-ims/AddUser.do?action=r	nvPreAdd&ptoken=UVS702ZDZKECDD06
	Last Name:	*	
	User ID:	*	
	Email:		
	i Certificate DN:		
	Notes:		
	Password		
	i Password:	*	What's a valid password?
	Confirm Password:	*	Your password must contain:
	i Force Password Change:	Require user to change pas	 7 to 32 characters At least 3 alphabetic characters At least 1 numeric characters
	Account Information		 At least 1 special characters At least 1 special characters Not allowed: @~
	I Account Starts:	June 💽 17 💌 2011	You may not re-use one of your last 5
	i Account Expires:	No expiration date June 17	passwords. Note: Any leading or trailing <space> characters will be automatically</space>
	i Account Status:	Account is disabled	removed.
	1 Locked Status:	☐ Account is locked by lockout ☐ Account is locked out of emo	• •

Figure 5-55 User Password Requirements Based on Policy

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

ck 💌 🕘 👻 📓 🐔 🔎 Search 👷 Favorit														4	
🕫 截 https://rsa-am.cisco-irn.com:7004/console-am/L	istAssign	edToken.do?pageaction=nv	PreSearchAll	BitokenCatego	ory—assigned8	3ptoken=EKK	J6OA4E835CIBC)						- 2	Go Lin
SA Security Console										Loi	gged in as: I	bmcgloth <u>My Pe</u> Rea		<u>My Preferences</u> nDomain <u>Co</u>	
me Identity Authentication Access	Reportin	g ▼ RADIUS ▼ Admin	istration 🔻	Setup 🔻	Help 🔻										
SecurID Tokens Import Se	curID T	okens 🔁											1	Help on this page	
Assigned Unassigned															
Hardware or software-based security tokens that	ave beer	assigned to users manage	d in this realr	π.											
	2 fc	und. Showing 1-2.													
Security Domain: SystemDomain •	_	elected: Unassign			Go Go	2								Show 250 -	ner nane
For:		Serial Number	Token	Algorithm	_	Disabled	Enabled For	Requires	Pending	will	ст-кір	Last Used To	Expires	Security	Notes
All Assigned Tokens			Туре		To		Emergency Online	Passcode	Replacement By Token	Replace Token	Capable		<u>On</u>	Domain	
Serial Number	-	000115335607 -	Gandard	AES-TIME	bricgloth		Access					3/9/11 1:18:58	12/31/11	SystemDomain	
starts with		11111 000115355607 ¥	Card	ALS-TIME	billogical			~				PM PST	12:00:00 AM PST	Systembolilari	
More criteria		000115400388 •	Software	AES-TIME	bart			*			~		12/31/11 12:00:00 AM PST	SystemDomain	
Search D		<u>Serial Number</u>	<u>Token</u> Type	<u>Algorithm</u>	<u>Assiqned</u> <u>To</u>	<u>Disabled</u>	Enabled For Emergency Online Access	<u>Requires</u> Passcode	<u>Pending</u> <u>Replacement</u> <u>By Token</u>	<u>Will</u> Replace Token	<u>CT-KIP</u> Capable	<u>Last Used To</u> <u>Authenticate</u>	<u>Expires</u> On	<u>Security</u> Domain	<u>Notes</u>
	0 sel	ected: Unassign			• G0	Σ								Show 250 -	per page
	2 fo	und. Showing 1–2.													
				Copyright ©	2007 - 2008 F	RSA Security	Inc. All rights res	erved.							

Figure 5-56 Assigned Tokens

- 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.

RSA Security Console: - Add New User - Microsoft Internet Explorer		_ 🗆 ×
ile <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp		
) Back 🔹 🕥 👻 😰 🏠 🔎 Search 👷 Favorites 🛛 🧀 😓 🗔		
ldress 🙋 https://rsa-am.cisco-irn.com:7004/console-ims/AddUser.do?action=nvPreAdd&ptoken=36NZIRX52121GMWQ	💌 🄁 Go	Links »
Password		
Password: * What's a valid password?		
Confirm Password:		
I Force Password Change:		
Account Information		
👔 Account Starts: June 💌 17 💌 2011 11 AM 🔍 09 💌 PDT		
Account Expires: O No expiration date O <u>Aucoust</u> 17 • 2012 11 AM • 09 • PDT		
🔝 Account Status:		
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.		
one	🔒 🕢 Trusted sites	

Figure 5-57 User Account Expiration

• 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.



🚰 RSA Security Console: - Edit Password Policy - Microsoft Internet Explorer	
Ele Edit View Favorites Iools Help	<u></u>
3 Back ▼ 3 ▼ E 2 5 Psearch ☆ Favorites Ø 3 ▼ 3 E	
Address 🗿 https://rsa-am.cisco-irn.com:7004/console-ims/AddPasswordPolicy.do	Links »
Format	
Minimum Length:	
Maximum Length: 32	
Excluded Characters: @~-	
Excluded Words Dictionary: * None 🖳	
Character Requirements: Require at least alphabetic characters	
Require at least 0 uppercase characters	
Require at least O lowercase characters	
Require at least 1 numeric characters	
Require at least methods are characters	
Cancel 🔀 Reset 🗿 Save 🔰	
Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.	•
😰 Done	11.

• 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 Locko	out Policy - Microsoft Internet Explorer	
$\underline{F} ile \underline{E} dit \underline{V} iew F \underline{a} vorites \underline{T} ools$	Help	20
• • • • • • • • •	Search 👷 Favorites 🛛 🖉 - 😓 🗁	
Address 💩 https://rsa-am.cisco-irn.com	r:7004/console-ims/AddLockoutPolicy.do?action=nvPreEdit&guid=ims.000000000000000000000000000000000000	3000&ptoken=TR0YIL354L3LO91F 💽 🋃 Go Links »
RSA Security Co	nsole	mcgloth <u>My Permissions</u> <u>My Preferences</u> <u>Log Off</u> Realm: SystemDomain <u>Configuration</u>
Home Identity Authentication	Access V Reporting V RADIUS Administration V Setup V Help V	
🖉 Lockout Policy: In	itial Lockout Policy 👻	i Help on this page ▼
▶ Edit		
Lockout policies specify the cor	nditions under which user accounts are locked or unlocked by the system after failed authentication attem	pts.
Cancel X Res	et 🖸 Save 🔰	
	* Required field	
Lockout Policy Basics		
Lockout Policy Name:	* İnitial Lockout Policy	
Default Policy:	I 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:	$^{\rm C}$ Allow unlimited failed authentications $^{\rm C}$ Lock accounts after 6 consecutive failed authentications within 1 days	•
I Unlock:	C Administrators unlock user accounts System automatically unlocks accounts after 3 minutes •	
Cancel X Res	iet 😼 Save 🔰	
	Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.	×
🝯 Done		Trusted sites

• **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.

<u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help	4
ack 🕶 🕤 👻 🖹 😭 🔎 :	iearch 👷 Favorites 🛛 😥 🍡 🚍	
ss 🙋 https://rsa-am.cisco-irn.con	:7004/console-ims/AddSessionManagement.do?action=nvPreEdit&guid=ims.000000000000	000000001000c0027099&ptoken=AMR 🔽 🛃 Go 🛛 Links
SA Security Co	nsole	bmcgloth My Permissions My Preferences Log Off Realm: SystemDomain Configuration
ome Identity - Authentication	Access V Reporting V RADIUS Administration V Setup V Help V	
Session Lifetime:	Console/Command API Session Li 👻	i Help on this page ▼
Edit		
Session lifetimes define session	durations. They are assigned to resources to limit sessions times for users who access thos	se resources.
Cancel 🔀 Re:	et 🖸 Save 🔰	
	* Required field	
Session Lifetime Basi	rs.	
	·····	
Session Lifetime Name:	* Console/Command API Session Lifetime	
i Time-out:	☑ Time out idle sessions	
	Close idle sessions after 15 minutes 💌 of inactivity	
Maximum Lifetime:	✓ Limit session lifetime	
	Close sessions after 8 hours	
System Default:	\square Set as the default session lifetime for all resources	
Notes:	The authenticated session lifetime.	
Cancel 🔀 🛛 Re:	et 🖸 Save 💫	
	Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.	

Figure 5-60 Session Lifetime for Console

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 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.





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 Identity Services Engine

Cisco Identity Services Engine (ISE), a security component of the Cisco Borderless Network architecture, provides visibility and control into who and what is connected to the network. Cisco ISE 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 ISE allows businesses to gain complete control over the access points into their networks. This includes all wired, wireless, and VPN network entry points.

Cisco ISE 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—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 ISE 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, and web authentication. In addition, this same infrastructure is what enforces the appropriate access into parts of the network via VLANs, downloadable or named ACLs and security group ACLs.

• Client—Cisco Anyconnect 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 ISE architecture also supports native O/S supplicants.

The Cisco Identity Services Engine 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 LAN deployment.

Figure 5-62 Cisco ISE-Based LAN Deployment



Table 5-22 PCI Assessment Summary – Cisco Identity Services Engine

Models As	sessed
Cisco Iden	tity Service Engine version 1.2
PCI Sub-Re	equirements 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, 10.5.4
PCI 11	11.1.b, 11.1.d
PCI Sub-Re	equirements Requiring Compensating Controls

Γ

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

No compensating controls were required to satisfy any sub-requirements. PCI Sub-Requirements Failed

No sub-requirements were failed.

Primary PCI Function

Cisco ISE 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 5-23 lists the component assessment details for the Cisco ISE Solution.

Table 5-23 Component Capability Assessment—Cisco ISE

PRIMARY FUN Authenticat	ICTION te and authorize users and endpoi	nts via wired, wireless, and VPN
REQUIREMEN	T: 7, 11 (7.1, 7.2, 11.1)	
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	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)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.
\checkmark	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)
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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)
1	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 ISE configuration best practices for PCI compliance:

- The solution tested used the virtual machine appliance version of Cisco ISE running on an ESX platform.
- The default accounts for administration are removed.
- ISE only supports HTTPS and SSH access
- 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.

Main	enance Backup & Restore A	admin Access Settings		
	entication Method Password	Policy		
	itication Type			
۲	Password Based		* Identity Source AD:AD1	*
0	Client Certificate Based			688806

Figure 5-63 Admin Access Using Active Directory for Authentication

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 can be upgraded and patched 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

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

ISE is used for ensuring network-wide compliance with PCI 6.1 for all Windows and Mac OSX systems. Systems are posture-assessed for compliance upon connection to the network. If found not to be compliant, remediation and access restrictions can be put in place on the network.

Cisco ISE is able to check all hosts connecting to the network to make sure they are compliant with requirement 6.1. Cisco ISE has several auto-update configuration options you can use to keep its posture assessment database current. 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. In addition to OS updates, ISE can also ensure anti-virus software is installed, running and up to date.

cisco Ide	entity Services Engine		A Home Ope	erations 🛛 🔻 Pol	icy 🛛 🔻 Administratio	n ▼			
💄 Authenti	ication 🧕 Authorization 🛛	A Profiling	Posture	Client Provi	sioning 🚊 Securit	y Group Access	🔒 Policy Elements		
-town Dat									
sture Poli	ю								
ine the Post	ure Policy by configuring rules based	on operating	system and/or oth	er conditions.					
Status	Rule Name		Identity Groups	Opera	ting Systems	Other Conditions			Requirements
Status	Rule Name		Identity Groups	Opera	ting Systems	Other Conditions			Requirements
		late If				Other Conditions		then	
Status	Rule Name Windows AV Installed and Up-to-d	late If	Identity Groups Employee		ting Systems	Other Conditions		then	Requirements Any_AV_Installation_ n &

Figure 5-64 ISE Endpoint Posture Policy for Checking AV and OS 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 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.

ISE ensures 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 5-65 shows the Authorization Profiles screen.

Results	Authorization Pro	ofiles > PCI_in_Scope		
<u>م</u>	* Name	PCI_in_Scope		
¢- ≡ Щ ŵ-	Description	For Hosts That Need	Access To PCI CDE	_
Authentication Allowed Protocols	* Access Type	ACCESS_ACCEPT		
a Default Network Access				
Authorization				
Authorization Profiles	▼ Common Task			
Cisco_IP_Phones	Common Task	(5		
Q DenyAccess	DACL Name		PERMIT_ALL_TRAFFIC	
PCI_in_Scope	DAGE Name		PERMIT_ALL_INAPPIO	
PermitAccess	VLAN		1:POS	
Downloadable ACLs	Voice Domain	Dormicolon		
Inline Posture Node Profiles	U Voice Domain	remission		
Profiling	Posture Disco	overy		
Posture		Ich Authentication		
Client Provisioning	Centralized W	Veb Authentication		
Security Group Access	Auto Smart Po	ort	dot1x	

Figure 5-65 Authorization Profiles

- 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 5-66 shows the Authorization Policy screen.



A Home	Monitor Policy	Administration	V			
2 Authentic	ation 💽 Authorization	Refiling	Posture	Client Provisioning	Security Group Acc	cess 🦂 Policy Elements
Define the Au	thorization Policy by config	uring rules base	d on identity gro	oups and/or other condition	S	
First Matche	ed Rule Applies	-				
Exception	S					
	15					
	Rule Name	Ider	ntity Groups	Other Conditions		Permissions
• Standard			ntity Groups sco-IP 🔶	Other Conditions and Condition(s)	the	
	Rule Name		sco-IP 💠			Cisco_IP_Pho 🔶

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.

ISE supports a robust administrator password policy and account lockout duration settings.

Figure 5-67 ISE Admin Password Policy Settings
Maintenance Backup & Restore Admin Access Settings
Authentication Method Password Policy
GUI and CLI Password Policy
* Minimum Length: 10 characters
Password should not contain the adminname or its characters in reversed order
Password should not contain "cisco" or its characters in reversed order
Password should not contain password or its characters in reversed order ^
Password should not contain repeated characters four or more times consecutively
Password must contain at least one character of each of the selected types:
✓ Lowercase alphabetic characters
✓ Uppercase alphabetic characters
V Numeric characters
V Non-alphanumeric characters
Password History
Password must be different from the previous 5 [When enabled CLI remembers only last 1 password irrespective of value configured]
Password change delta 3 characters (Valid Range 3 to 10)
Password Lifetime
Admins can be required to periodically change password
Disable admin account after 45 days if password was not changed
Send an email notification / warning message prior to password expiry after 30 days
✓ Lock/Suspend Account with Incorrect Login Attempts
* # 5 (Valid Range 5 to 20)
Suspend account for 60 minutes (Valid Range 15 to 1440) ^ O Disable account
Email remediation message ^
This account has been locked. For this account to become unlocked, please contact your IT helpdesk.
Save 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 ISE is configured to re-authenticate both admin users and RADIUS users every 15 minutes.

🔆 System 🛛 💆 Identity Management	Net	work Resources	🛃 Web Portal Ma	anagement 🛛	Feed Service
Deployment Licensing Certificates	Logging	Maintenance	Backup & Restore	Admin Access	Settings
Admin Access		Session Timeou	It Session Info)	
④ • 	م شہ	* Session Idle T	imeout 10	minutes (Valid I	Range 6 to 100)
Authentication	Lot V				
Authorization					
 Administrators Esttings 					
Access					
i i Session					

Figure 5-68 Admin Access

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.

Cisco ISE can assist with this requirement by ensuring that all network jacks require AAA, posture assessment, and profiling. ISE can then determine the type of access to grant to that switchport based on the results of the above and/or based on the switchport's location. This type of authorization to the network would prohibit a non-authorized endpoint/user from access PCI data through publicly accessible network jacks.

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 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
```

CISCO Identity Services Engine	🙆 Hor	ne Operations v Polic	y 🔻 Administration 🔻		
Authentications 📑 Reports 🔯 En	dpoint Protection Ser	vice 💊 Troubleshoot			
Report Selector	Administrate	or Summary			
Favorites					
ISE Reports	From 01/19/20	13 12:00:00.000 AM to 01/19	9/2013 10:02:10.024 PM		
Auth Services Status 4 reports	Administrator	Resources and Privileges	Configuration Changes	Logins	Roles
▼ Deployment Status	Jamey.Heary	0	Q	0	Super Admin, System Admin
Administrator Logins	admin	0	<u>_</u>	0	Super Admin
Administrator Summary					
Run					
Change Configuration Audit					
Secure Communications Audit					
Operations Audit					

Figure 5-69 Administrator Summary

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 10.5.4—Write logs for external-facing technologies onto a log server on the internal LAN.

Figure 5-70 Remote Logging Targets

🔆 System 🖉 Identity Management	Network Resources 🛛 🛃 Web Portal Mana	gement 🔄 Feed Service		
Deployment Licensing Certificates Log	ing Maintenance Backup & Restore	Admin Access Settings		
Logging	Remote Logging Targets			
il Local Log Settings				
Remote Logging Targets	/ Edit - Add Duplicate 🗙	Delete		
Logging Categories	Name 🔺	IP Address Type	Description	Status
Message Catalog	O LogCollector	10.1.103.4 UDP SysLog	Syslog Target for Log Collector	Enabled
Debug Log Configuration	O ProfilerRadiusProbe	127.0.0.1 Profiler SysLog	Syslog Target for Profiler RADIUS Probe	Enabled
	O RSA EnVision	10.2.3.12 Secure SysLog	external log server	Enabled
	O TCPLogCollector	127.0.0.1 TCP SysLog	TCP SysLog collector	Ø Disable

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 ISE 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 ISE authentication services in the data center, add the following configurations to all switch and switch interface ports where ISE network access control is required. In most cases, every access switch port in your network should be protected using ISE. However, as a minimum, any switchport that could potentially let a host find its way to the PCI security domain should be protected by Cisco ISE.

Pre-requirements for ISE 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 ----
I
aaa new-model
1
!
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>
1
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
1
authentication mac-move permit
!
1
ip device tracking
ip admission name ise proxy http inactivity-time 60
1
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-----
    1
   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
```

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

Cisco ISE 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 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 Prime LAN Management Solution (LMS)

Cisco Prime LAN Management Solution (LMS), a part of Cisco Prime Infrastructure, delivers powerful network lifecycle management by simplifying the configuration, compliance, monitoring, troubleshooting, and administration of Cisco networks. Cisco Prime LMS offers end-to-end management for Cisco's latest business-critical technologies and services such as Medianet, Cisco ISE, and Cisco EnergyWise while ensuring compliance with corporate and regulatory requirements.

Models As	sessed
Cisco Prin	ne LMS version 4.2.2
PCI Sub-Re	equirements 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 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, 10.5.4, 10.5.5
PCI Sub-Re	equirements Requiring Compensating Controls
No compe	nsating controls were required to satisfy any sub-requirements.
PCI Sub-Re	equirements Failed
No sub-rec	quirements were failed.

Table 5-24 PCI Assessment Summary—Cisco Prime LMS

Primary PCI Function

LMS simplifies compliance by ensuring that all of the devices across the network adhere to the security policy of the company. In addition, it will verify that device configurations; match templates, are synchronized, and includes a customized PCI compliance dashboard to simplify the ongoing management for administrators (1.2.2).

Table 5-25 lists the component assessment details for the Cisco Prime LMS.

PRIMARY FUNCTION Manage network device configuration and verify configuration against policy templates REQUIREMENT: 1 SECURITY SERVICES V CaPABILITY SECURITY SERVICES V 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) V Secure Administrative Access Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3) V Uses SNMP Version 3—SNMP Versions 1 and 2 are considered insecure. (Verizon Recommended) V Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3) V Uses SNMP Version 3—SNMP Versions 1 and 2 are considered insecure. (Verizon Recommended) V Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1) AUTHENTICATION			
ASSESSMENT	CAPABILITY		
	SECURITY SERVICES		
\checkmark		unnecessary functionality, such as scripts, drivers, features, subsystems, file systems,	
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)	
\checkmark	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)	
\checkmark	Vendor Supported		
	AUTHENTICATION		
\checkmark	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.	
+	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)	
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)	
	LOGS/ALERTS		
╉	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)	
\checkmark	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 5-25
 Component Capability Assessment – Cisco Prime LMS

Design Considerations

- Provide sufficient licenses to cover all devices in your network.
- Provide proper host system sizing including CPUs, memory, and storage for the selected operating system.
- Restrict access behind a firewall or access list to only those administrative clients that need access.
- Activate the NMC capability license for compliance audits.

Compliance and Audit

The compliance and audit reports provide the compliance status of the network, lifecycle, and contract information about network devices, security advisory, and service reports based on device and software capabilities, and the services that are enabled.

The compliance reports provide information about the compliance state of the network for specific compliance requirements and can be found in LMS by navigating to Reports > Compliance and Audit.

Licensed/Unlicensed Compliance and Audit Reports

The following compliance and audit reports require a regulatory compliance management license:

• HIPAA Compliance Reports

- SOX (COBIT) Compliance Reports
- ISO/IEC 27002 Compliance Reports
- NSA Compliance Reports
- PCI DSS Compliance Reports
- DHS Checklist Reports
- DISA Checklists Report
- CIS Benchmarks

The following compliance and audit reports are supported by the LMS license alone and do not require a regulatory compliance management license:

- Service Reports
- Lifecycle Management Reports
- Vendor Advisory Reports
- Change Audit Reports

For compliance and audit license information, see the topic "Regulatory Compliance Management License in Administration with Cisco Prime LAN Management Solution 4.2.2".

The Compliance and Audit Report module uses the stored configurations within the LMS database and evaluates them against specifically defined criteria of the selected devices. The PCI DSS Compliance Summary Report shows Payment Card Industry Data Security Standard (PCI DSS) security compliance audit results against either the entire network or selected network devices to verify how compliant the selected devices are against this regulation. (See Figure 5-71.)

IR.com	Policy Title						
irn.com ASA-WAN-1.cisco-		Rule Title	Message	Severity	Result	Info	
	HTTP Server	Check state of HTTP server			Not Applicable	0	
	Terminal Access	Check Authentication parameters on terminal lines			Not Applicable	0	
ASA-WAN-1.cisco-	Terminal Access	Check for allowed incoming connections			Not Applicable	0	
ASA-WAN-1.cisco-	Terminal Access	Check for allowed outgoing connections			Not Applicable	0	
ASA-WAN-1.cisco- (irn.com	User Passwords	Passwords should not be shown in clear text in configuration			Not Applicable	0	
ASA-WAN-1.cisco- irn.com	User Passwords	All users must have passwords configured			Not Applicable	0	
ASA-WAN-1.cisco- (irn.com	User Passwords	Passwords must be MD5 encrypted			Not Applicable	0	
ASA-WAN-1.cisco-	User Passwords	Check minimum length for user/enable/line passwords			Not Applicable	0	
ASA-WAN-1.cisco- irn.com	User Passwords	Check maximum authentication failure rate			Not Applicable	0	
ASA-WAN-1.cisco- irn.com	Console Access	Check console connection		۵	Not Applicable	0	
ASA-WAN-1.cisco-	Console Access	Check auxiliary connection			Not Applicable	0	
ASA-WAN-1.cisco-	SNMP	Check the state of SNMP server			Not Applicable	0	
ASA-WAN-1.cisco- 1 irn.com \$	Miscellaneous Services	Disable TCP small servers			Not Applicable	0	
ASA-WAN-1.cisco- 1 irn.com	Miscellaneous Services	Disable UDP small servers			Not Applicable	0	
ASA-WAN-1.cisco- I irn.com	Miscellaneous Services	Disable Finger server			Not Applicable	0	
ASA-WAN-1.cisco- I irn.com S	Miscellaneous Services	Disable BOOTP server			Not Applicable	0	
ASA-WAN-1.cisco- I irn.com \$	Miscellaneous Services	Disable configuration auto- loading from TFTP server			Not Applicable	0	

Figure 5-71 PCI DSS Compliance Summary

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.

Firewall, router, and switch configuration files are backed up centrally using Cisco Prime LMS. LMS automatically verifies that running and startup configurations of firewalls, routers, and switches are synchronized for the devices managed.

The Out-Of-Sync Summary report can be used to view which systems configurations need to be synchronized and provides the ability to select and synchronize the devices. (See Figure 5-72.)

bmcgloth | Log Out | About | Cisco Prime CISCO LAN Management Solution 🔹 My Menu 💌 Monitor Inventory * Configu Configuration > Compliance > Out-of-Sync Summary Startup and Running Out-Of-Sync Summary Showing 5 records Device Name Diff Startup Running 1. R-A2-Med-2 Dec 13 2012 09:45:15 Q Oct 17 2012 14:57:28 2. 🔲 R-A2-Lrg-2 Nov 20 2012 09:45:15 D, Nov 20 2012 08:00:09 Q 3. 🔲 R-A2-Mini-1 Dec 13 2012 09:45:09 Oct 17 2012 14:57:13 Q 4. 🔲 R-A2-Med-1 Dec 13 2012 09:45:15 Oct 17 2012 14:57:00 Q 5. 🔲 R-A2-Conv-1 Dec 13 2012 09:45:09 Nov 09 2012 15:06:18 Sync on Device 203311

Figure 5-72 Out-of-Sync Summary Report

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, and so on.

Cisco Prime LMS supports several protocols for securely managing devices. Device management preferences are configured in Admin > Collection Settings > Config > Config Transport Settings. Add secure protocols to the list in order of preference and remove insecure protocols for each Application Named function. Figure 5-73 shows the preferred protocol selections for Archive Management.

isco LANI	Prime Management Solution	🔺 My Menu 🔻 🛛 M	onitor 🔻 Inventory 🔻	Configuration 🔻
Admin >Collectio nsport S€	on Settings > Config > Config [·] ettings	Transport Settings		
onfig Transpor pplication Name:	r t Settings Archive Mgmt V			
	Available Protocols		Selected Protocol Order	
Config Fetch :	HTTPS SSH SCP TFTP TELNET RCP	Add >> << Remove	HTTPS SSH SCP	Up Down
	Available Protocols		Selected Protocol Order	
Config Deploy :	HTTPS SSH SCP TFTP TELNET RCP	Add >> << Remove	HTTPS SSH SCP	Up Down

Figure 5-73 Device Management Transport Settings

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

The Cisco Prime LMS soft appliance does not have any unnecessary services enabled by default.

Cisco Prime deployed on other server platforms such as Windows or Solaris should first be hardened using industry best practices for those systems before installing the LMS application. Server hardening best practices guidelines can be found at a variety of Internet resources provided by the vendor or sites such as the NSA, NIST, and SANS.

• 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 Prime LMS supports encrypted administrative access via SSH and HTTPS. SSH is enabled by default after installation. HTTPS can be enabled with a self-signed certificate or public certificate. To enforce the use of only SSL for the web interface of LMS, perform the following configurations, as shown in Figure 5-74). These configuration steps can also be found in the LMS 4.2 Administration Guide, page 53.

Cisco Prime LAN Management Solution	My Menu 🔻 Monitor 🔻 Inventory 🔻 Configuration 🔻 Reports 🔻	Admin 🔻
Admin > Trust Management > Local Server >	Browser-Server Security Mode Setup	
Navigator	Browser-Server Security Mode Setup	
Current Settings		
Browser-Server Security Mode Setup	Browser-Server Security Mode Setup Current Setting: Enabled	
Certificate Setup	Change Setting To: 🔘 Enable 🔘 Disable	
Single-Server Management	Apply	

Figure 5-74 Enable Cisco Prime LMS Browser Security

To enable browser-server security, complete the following steps.

Procedure

Step 1 Select Admin > Trust Management(4.2.2 patch) > Local Server > Browser-Server Security Mode Setup. The Browser-Server Security Mode Setup dialog box appears. Step 2 Select the **Enable** option to enable SSL. Step 3 Click Apply. Step 4 Log out from your Cisco Prime session and close all browser sessions. Step 5 Restart the Daemon Manager from the LMS Server CLI. On Windows: a. Enter net stop crmdmgtd **b.** Enter net start crmdmgtd On Solaris/Soft Appliance: a. Enter /etc/init.d/dmgtd stop b. Enter /etc/init.d/dmgtd start Step 6 Restart the browser and the Cisco Prime session. When accessing the LMS CLI, you need to enter the SHELL by using the "shell" command. Then you can execute the stop/start commands for the soft appliance.

If you have issues logging in to LMS (lsuch as long delays), try disabling the launch of the LMS Getting Started page by default (as the first page after log in) by completing the following steps:

a. Open the properties file name "gs.properties" under the following path:

Windows:

/<<NMS-ROOT>>/MDC/tomcat/webapps/cwlms/WEB-INF/classes/com/Cisco/nm/gs/ui/gs.proper ties

Soft appliance:

./opt/CSCOpx/MDC/tomcat/webapps/cwlms/WEB-INF/classes/com/cisco/nm/gs/ui/gs.properties

- **b.** Update the field IS_DEFAULT_PAGE as "false".
- c. Clear the browser cache and login-in (Daemon restart not required).

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.

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

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

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 within LMS 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 Prime LMS supports role-based user access. Users can be assigned to role groups and, based on privilege levels, have access to only the tasks they require for their job function. By default in Cisco Prime LMS, authenticated users are allowed help desk level access unless specifically configured and assigned to appropriate roles. To restrict access to only configured users, clear the default role option under Admin > System > User Management > Role Management Setup (see Figure 5-75).

ululu Cisco Prime		bmcgloth	Log Out I About I Sitemap I
CISCO LAN Management Solution	My Menu 🔻 Monitor 🔻 Inventory 🔻	Configuration 🔻 Reports 🔻 Admin 🕈	Work Centers 🔻
Admin > System > User Management > Role Mana	agement Setup		
Navigator	Role Management Setup		
Local User Policy Setup			denie constr
Local User Setup	Roles	Description	Showing 6 records Default Roles
Notify Users	1. Approver	Approver Role	
Role Management Setup			
	2. 🖳 Help Desk	Help Desk Role	
	3. 🔲 Network Administrator	Network Administrator Role	
	4. 🔲 Network Operator	Network Operator Role	
	5. 🔲 Super Admin	Super Admin Role	
	6. 🔲 System Administrator	System Administrator Role	
	Add Edit Delete Copy I	Export Import I Set as default Clo	ear default

Figure 5-75 Role Management Setup

Local user accounts are configured to authorize role privileges and can also be used as fallback if the central 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. (See Figure 5-76.)

User Login Detai Jsername:	s	bmcgloth				
Password:		•••••		Verify Pa	ssword:	
imail:		bmcgloth@ci	sco-irn.com			
Authorization Ty	/pe		,			
-	-	ation 💿 Ena	ble Task Aut	horization	Enable Device Authoriza	ation
Roles					norization	_
🔽 Help Desk			Not App	licable		
🔽 Network O	perator					
Approver						
Network A	dministrator					
System Ad						
Super Adm	iin					
L						
Network Level Lo This pane allows you			redentials fo	r LMS to a	ommunicate with the network	
levices.						
Jsername:	bmcgloth					
Password:	•••••		Verify Pa	ssword:	•••••	
	•••••		Verify Pa	ssword:	•••••	
Enable Password:						

203316

Several AAA services are available to externally authenticate users assigned to administer the system. Roles for these individuals are created and managed within the LMS system (see Figure 5-77). As of version 4, LMS no longer supports external authorization.

Figure 5-77 Authentication Mode Setup

	Cisco Prime									
cisco	LAN Management Solution	My Menu	•	Monitor	•	Inventory	•	Configuration	•	F
Admin	> System > Authentication Mode Setup									
uthen	tication Mode Setup									
Authen	tication Mode Setup									
Current Lo	ogin Mode: TACACS+									
Availab	le Login Modules									
10	Local Authentication									
2O	Local UNIX System									
20 30	Local UNIX System MS Active Directory									
	·									

In the TACACS server configuration, either all accounts or only specified accounts can be allowed for authenticaiton in the event that the ACS server cannot be reached. (See Figure 5-78.)

Login Module Options	710100
Selected Login Module: Description:	TACACS+ Cisco Prime TACACS+ login module
Server:	192.168.42.131
Port:	49
SecondaryServer:	
SecondaryPort:	49
TertiaryServer:	
TertiaryPort:	49
Key:	•••••
Debug:	🔘 True 🔘 False
	 Allow all Local Authentication users to fallback to the Local Authentication login.
Login fallback options:	Only allow the following user(s) to fallback to the Local Authentication login if preceding login fails:
	bmcgloth, chjanoff (comma separated)
	$\hfill \bigcirc$ Allow no fallbacks to the Local Authentication login.
	OK Cancel

Figure 5-78 Login Module Options

Cisco LMS does not include the capability to restrict access to its CLI and HTTPS interfaces from only authorized systems. This server should be implemented in a network segment that includes firewalling or access list restriction capabilities to ensure proper access is limited as necessary.

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 Prime LMS 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 Prime LMS supports the creation of local user accounts with unique IDs through the use of the **username** command in the CLI and via the web interface Admin > System > User Management > Local User Setup. (See Figure 5-79.) These users are necessary to role assignment and can be used for local fallback user accounts.

username chjanoff password hash \$1\$3Af9qCBs\$GCZoSBOqvTIkYMLxXOeZf1 role admin username bart password hash \$1\$zJe0WwVd\$jHUzM9cNQxpy./D9uHCYM1 role admin

assword:				
	•••••	Verify Pa	assword:	
mail:	bmcgloth@cis	co-irn.com		
Authorization Type				
	uthorization 💿 Enab		Enable Device Authorization	
Roles		Device level Aut Not Applicable	horization	
📝 Help Desk		NOT Applicable		
Network Operator				
Approver				
Network Administr				
🗵 System Administrat	or			
🗵 Super Admin				
letwork Level Login Cre	dentials			
his pane allows you to prov evices,	de the network login cr	edentials for LMS to c	communicate with the network	
	th			
sername: bmcolo				
sername: bmcglo				
, Dinegie	••••	Verify Password: Verify Password:	•••••	

Figure 5-79 LMS Local User Accounts

- **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 Prime LMS require setting of a password.

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

Cisco Prime LMS uses MD5-encrypted hashing of locally stored passwords.

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

Cisco Prime LMS does 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.

• PCI 8.5.9—Change user passwords at least every 90 days.
Cisco Prime LMS 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 Prime LMS supports the ability to specify a minimum password length for local accounts in the Admin > System > User Management > Local User Policy Setup. The default minimum password length must be changed from 6 to 7 characters, as shown in Figure 5-80.

Cisco Prime	My Menu 🔻 Monitor 🗶 Inventory 🗶 Configuration 🗶 Reports Y Admin Y Work Centers Y
Admin > System > User Management > Local Use	r Policy Setup
Navigator	Local User Policy Setup
Local User Policy Setup	
Local User Setup	Local User Policy Setup
Notify Users	□ Allow Special Characters (~ @ # _ ' - \ / . space) in Username
Role Management Setup	Allow Username to Start with Numbers
	Password should have at least characters from three groups of lowercase, uppercase, digits and special characters
	Password should not be the same as the username, or the username in reverse
	Password should not have the same character repeated three times, in sequence
	Password should not contain a variant of the word Cisco
	Username Length between 5 and 256 Characters
	Password Length between 7 and 256 Characters
	Apply

Figure 5-80 LMS Local User Policy Setup

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

Cisco Prime LMS supports the ability to specify the necessary password complexity for local accounts in the Admin > System > User Management >Local User Policy Setup.

• **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 Prime LMS does not support an automated capability to perform this function at this time; user account creation 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 Prime LMS does not support an automated capability to perform this function at this time. 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.

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 Prime LMS management interface timeout must be properly configured to meet this requirement:

Change the Session TimeOut to 15 minutes from the default 120 minutes, as shown in Figure 5-81 on the Admin > System > System Preferences menu.

ew / Edit System Preferences E mail Settings	
SMTP Server:	msexchange.cisco-irn.co
SMTP Server TimeOut:	6000 in Milliseconds
Administrator E-mail ID:	administrators@cisco-irn
Enable E-mail Attachment:	
Maximum Attachment Size:	2 MB
Other Settings	
RCP User:	cwuser
5CP User:	cwuser
5CP Password:	•••••
5CP Verify Password:	
Disable Idle Timeout Settings:	
idle Timeout:	15 🗾 in Minutes
	Apply Cancel

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

Cisco Prime LMS 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.*

233220

- **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.

The majority of LMS system activities on the server are accomplished through jobs. Each of these jobs tracks the requestor, the success or failure, the type of event, and the systems against which they are executed. The Job Browser shows status of scheduled, current and past jobs. The jobs browser is located at Admin > Jobs > Browser.

Additional audit trail information for system configuration changes (for example, changing the authentication mode of the LMS Server from local to TACACS and back to local) require enabling debug mode logging for the Tomcat service. With debug mode enabled, the server is able to capture sufficient information for logging this configuration change and other similar system changes.

To enable debug mode for the Tomcat console, navigate to Admin > System > Debug Settings > Common Services Log Configurations (see Figure 5-82). Select "Console logs from Tomcat" in the component dropdown. Click the **Enable** radio button and then click **Apply**.

Figure 5-82 Common Services Log Configurations

alialia Cisco Prime	t Calution	bmcgloth	Log Out I At	oout I Sitemap I	I Feedback I H
cisco LAN Managemer	My Mi	enu 🔻 Monitor 🔻	Inventory 🔻	Configuration	 Reports
Admin > System > Debug Settings > Common Services Log Configurations					
Navigator	Common Services Log Configurations				
Discovery Logging Configuration	Common Services Lo	og Configurations			
Layer2 Configuration and	Component: Console logs from Tomcat Log File(s) Location: C:/PROGRA~2/CSCOpx/MDC/tomcat/logs/stdout.log Description: Enables/Disables debug for direct console logs from web applications in tomcat				
Reports					
Common Services Log Configurations					
Data Collection	Debug Mode:	⊙ _{Enable} ⊂ Disable			
Dynamic User Tracking				Reset All	Apply
Dynamic User Tracking				(tosott1m	

Note

Enabling debugging may have a significant performance impact on the LMS system, depending on the number of users who are simultaneously accessing and managing the system. All web front end activity is logged in detail.

The "accesslogfilter.log" captures source IP address, date, time, and username for logged-in users as well as failed logins. Failed logins in this log have a "null" username. The attempted usernames of the failed logins appear in the Audit-Log-{date}.CSV report. These reports do not include the user's source IP address, so some manual correlation must be done between the two logs. These

reports are generated at Reports > System Audit Reports > System, or available in \CSCOpx\MDC\log\audit. Informkation about currently logged-in users is available in Reports > System > Users > Who is logged On.

The "stdout.log" and "accesslogfilter.log" files should be added to the Log Rotation under Admin > System > Log Rotation.

To add these logs to the rotation, click Add at the bottom of the page. (See Figure 5-83.)

Figure 5-83 Adding Logs to the Rotation

[↑] Select an item then take an action>				Edit Delete	
	Rows per page: 100 💌	I	Go to page	1 of 1 pa	ages Go >>1
59. O	C:\PROGRA~2\CSCOpx\log\Cmapps.log	600	gz	2	
58. C	C:\PROGRA~2\CSCOpx\log\Campus.log	600	gz	2	
57. O	C:\PROGRA~2\CSCOpx\log\CMFOGSServer.log	307200	gz	5	
56. C	C:\PROGRA~2\CSCOpx\log\CMFOGSClient.log	307200	gz	5	
55. O	C:\PROGRA~2\CSCOpx\log\syslog.log	1048576	gz	3	
54. O	C:\PROGRA~2\CSCOpx\MDC\tomcat\logs\stdout.log	102400	gz	99	

In the popup window, set the max file size needed to capture about a days' worth of information for your environment and usage. Set the number of backups to the maximum of 99. (See Figure 5-84.)

Figure 5-84 Configure Logrot

	Configure Logrot		
	Logrot		
	Select Log File*:	C:/PROGRA~2/CSCOp> Browse	
	Maximum Logrot Size*:	102400 KB	
	Compression Format:	GNU Zip 💌	
	No.of Backups:	99	
		Apply Cancel Help	3
No	te: * - Required Field	50 50 50	3
		,	ĩ

Click **Browse** and navigate to the file location as appropriate for the operating system; for example, C:/PROGRA~2/CSCOpx/MDC/tomcat/logs/stdout.log. (See Figure 5-85.)

File:	C:/PROGRA~2/CSCOpx/N	1DC/tomcat/logs/
	stderr.log-OLD-3	
Directory Content:	stdout.log stdout.log-OLD-1	
Directory Content.	stdout.log-OLD-2	
	stdout.log-OLD-3	•
Drive:	C:\ 💌	

Figure 5-85 Server Side File Selector

Click **OK** to complete the file section, and then **Apply** to complete the addition of the log rotation file.

Cisco Prime LMS 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 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 Cisco Prime LMS appliance uses NTP to meet these requirements by implementing the following configuration statements:

ntp server 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 10.5.4—Write logs for external-facing technologies onto a log server on the internal LAN.
- **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 Prime LMS GUI and console scripts support periodic log rotation based on file size and can be configured for the maximum size of the file and number of files to maintain. A script must be created to copy these log files off the system to an external secure repository (for example, a directory on the RSA enVision server) because LMS is not natively capable of sending system events to a centralized repository or ensuring the integrity of the logs to the standards required for PCI. This script file should be automated and scheduled to run periodically at least daily (for example, every 1, 2, or 24 hours) via the operating system (Linus, Solaris, Windows) based on the deployment OS. Logs stored locally are buffered and require operator level privileges on the system to be viewed.

L

Logging enabled by implementing the following configuration statements in the CLI is only for system events such as software updates via the cars application utility:

logging 192.168.42.124 logging loglevel 6

RSA enVision supports the periodic collection of log files from Cisco LMS versions 3.2 and 4.0. The old method required the daily running of a .VBS script on the server (Windows only) where a file is created in the directory/files/rme/archive directory. It then required the installation of an RSA enVision NIC SFTP Agent, which is used to transfer the log files to the RSA enVision appliance. RSA recently added support for ODBC collection of change audit information from Cisco LMS. It is highly recommended to update to the latest RSA enVision ESU and move to this ODBC method as log collection occurs more frequently. ODBC importing was not validated for LMS at the time of this publication.

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 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 5-26	PCI Assessment Summary—Cisco Security Manager
------------	---

Models As	Models Assessed		
Cisco Security Manager version 4.0.1			
PCI Sub-R	equirements 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-R	equirements Requiring Compensating Controls		
No compe	nsating controls were required to satisfy any sub-requirements.		
PCI Sub-R	equirements Failed		
No sub-ree	quirements 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 5-27 lists the component assessment details for Cisco Security Manager.

PRIMARY FUNCTION Implement security configuration based on policy templates to secure the cardholder data environment REQUIREMENT: 1 (1.2)				
ASSESSMENT	CAPABILITY			
	SECURITY SERVICES			
\checkmark	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)		
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)		
\checkmark	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)		
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.		
+	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)		
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)		
	LOGS/ALERTS			
+	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)		
\checkmark	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 5-27 Component Capability Assessment—Cisco Security Manager

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 5-86 shows how the Cisco Security Manager is configured in Common Services for ensuring that only encrypted communications for administration are used.

Figure 5-86 CSM Secure Administration and AAA Policy

Firefox 🔻		
Cisco Security Management Suite	CSManager - AAA Mode Setup × +	-
Cisco-irn.com https://csmanag	rer.cisco-irn.com/cwhp/loginModule.do	Feedback •
Most Visited We Circo LICS Manager	IIM NCM WCS 10 TACACS IN RSA enVision HyTrust 🗰 CM-2 RSA-AM 🗰 VSOM	» 🔝 Bookmarks
Most visited and cisco oco manager _ c		s Help About
	mon Services	
CIECO	Server Software Center Device and Credentials Groups	
· · · · · · · · · · · · · · · · · · ·	server sortware center betree and creatinears croops	
You Are Here + Server > Security > AAA Mode :		
TOC	de Setup	
Single-Server Management		
Browser-Server Security Mode Setup	AAA Mode Setup	
Local User Policy Setup	Select a Type: ACS Non-ACS	
Local User Setup Certificate Setup	Current Login Module: TACACS+	
Multi-Server Trust	-	
Management	Server Details	
Peer Server Account Setup	Primary IP Address/Hostname: 192.168.42.131 ACS TACACS+ Port: 49	
- System Identity Setup	Secondary IP Address/Hostname: ACS TACACS+ Port: 49	
Peer Server Certificate Setup	Tertiary IP Address/Hostname: ACS TACACS+ Port: 49	
Single Sign-On Setup	Login	
AAA Mode Setup Cisco.com Connection	ACS Admin Name: csm-acs-admin	
Management	ACS Admin Password:	
Cisco.com User Account Setup	ACS Shared Secret Key:	
Proxy Server Setup	Acts shared sed a key.	
	Application Registration	
	Register all installed applications with ACS	
	Current ACS Administrative Access Protocol	
	C HTTP C HTTPS	
	Appl	V

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

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

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 5-86 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 5-87 shows the configuration setting in the client for setting the idle timeout.

Figure 5-87 Customize Desktop

🎉 Cisco Security Manager - Administration	
AutoLink Grifiguration Archive Grifiguration Archive Grifiguration Archive Grifiguration Archive GetAverse VestArg Debug Options Debug Options Device Communication Device On Management Device On Management Discovery Event Management Discovery Event Management Discovery Device Options Debug Options Servers Status	
	Close Help

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 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 5-88, Figure 5-89, and Figure 5-90 shows the Logs, Audit Report, and View Settings screens.

Figure 5-88 Logs

Logs							
		1.					
Keep Audit Log For:*	30	days	Purge Now				
Purge Audit Log After:*	10000	entries					
Keep Operation Log For:*	30	days					
Log Level:	INFO -]					
				Save	Reset	Restore Defaults	468
							Poc

ch by any or all of the criteria below:	Message Level	Date	Source	Action	Object	User Name	Activity
earch by action:	Success	07-Jun-2011 14:08:48	Devices	Add	1811	admin	None
e- 🔜 🏭 🔺	Success	07-Jun-2011 14:08:48	PolicyManager	Assign	None	admin	None
PolicyManager	Success	07-Jun-2011 14:08:48	PolicyManager	Create	None	admin	None
🖲 🔲 🏭 Topology	Success	07-Jun-2011 10:53:12	-	Assign	None	admin	admin_31.May.2011_1
Devices Devices Devices	Success	07-Jun-2011 10:53:12		Create	None	admin	admin_31.May.2011_1
	Success	07-Jun-2011 10:53:12		Create	None	admin	admin_31.May.2011_1
🕀 🗍 🛄 Admin 📃 🔻	Information	07-Jun-2011 10:42:46	Objects	Create	myeDirectory_server	admin	admin_31.May.2011_1
earch by date:	Information	07-Jun-2011 10:42:16	Objects	Create	LDAPserver 1	admin	admin 31.May.2011 1
From:	E Success	07-Jun-2011 02:00:00	Deployment	Purge	None	System	None
Jun 06 2011	Success	07-Jun-2011 02:00:00	Deployment	Purge	None	System	None
To:	Success	07-Jun-2011 02:00:00	Deployment	Purge	None	System	None
Jun 07 2011	Success	06-Jun-2011 02:00:00	Deployment	Purge	None	System	None
earch for activity by state:	Success	06-Jun-2011 02:00:00	Deployment	Purge	None	System	None
Filter: No Activity 👻	Success	06-Jun-2011 02:00:00		Purge	None	System	None
	Success	00 301 2011 02100100	beployment	, orge		oyotem	
earch by message warning level:							
Information A Warning							
C							
SUCCESS v	Showing page 1 of 1	# of rows per page:	50 👻				
Search Reset							< >

Figure 5-89 Audit Report



Views ÷	Event Monit	toring												
🕈 New 📓 Edit 🏢 Delete	🛃 AI D	evice Events	Firewall Ti	affic Events >	🗧 🔙 Firewa	II Denied Events	AAA Eve	nts 🛛 🙀 IPSe	: VPN Events					4 ▷ ⊞
Predefined Views	Siew Se	ettinas												*
All Device Events											1			
Firewall Traffic Events	Search within	n results: Q+ Typ	e here to sear	ch	last 1	0 min 👻 All Ever	nts (Default) 🔹	Save •	Start S	top Clear				12,86
Firewall Denied Events	Receive Tim	e Severity 🗸	Ƴ Ev ▼	Event Name	Device 👻	Source 👻	Sourc +	Destin +	Destin	Direction +	Protocol 👻	Action 👻	Conne +	Policy
NAT Events	6/7/11 2:27.	🔥 Informa	302013	Built TCP	🔗 ny-asa	172.16	tcp/14633	208.72	tcp/5636	autbound 🥵	10 top	🖌 built	63555433	-
Botnet Events	6/7/11 2:27.	. 🔥 Informa	302014	Teardown TCP	🔗 ny-asa	208.72	tcp/5636	10.10.1	tcp/20998		tcp	☐ ⁴ teardown	63555021	
	6/7/11 2:27.	🔥 Informa	302013	Built TCP	🔗 ny-asa	172.16	tcp/16825	208.72	tcp/5636	autbound 🧖	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	Steardown	63555020	
Failover Events	6/7/11 2:27.	🔥 Informa	302013	Built TCP	🔗 ny-asa	172.16	tcp/17284	66.98.1	tcp/80	ref outbound	tcp	🖌 built	63555430	
All IPS Events	6/7/11 2:27.	. 🔥 Informa	302014	Teardown TCP	🔗 ny-asa	216.188	tcp/443	10.10.1	tcp/16019		tcp	☐ ^d teardown	63555019	
	6/7/11 2:27.	🔥 Informa	302014	Teardown TCP	🔗 ny-asa	75.125	tcp/22	10.10.1	tcp/23005		tcp	☐ ⁴ teardown	63555018	
IPS Status Events	6/7/11 2:27.	. 🔥 Informa	302021	Teardown I	🔗 ny-asa	4.69.15	0	172.16	34457		Kee icmp	☐ ^d teardown		
IPS Error Events	6/7/11 2:27.	. 🔥 Informa	302020	Built ICMP	🔗 ny-asa	4.69.15	0	172.16	34457	🐴 inbound	Ket icmp	🖌 built		
- I My Views	6/7/11 2:27.	- 🔥 Informa	302013	Built TCP	🔗 ny-asa	172.16	tcp/30537	216.188	tcp/443	ref outbound	tcp	🖌 built	63555428	
All Device Events -Admin	6/7/11 2:27.	🔥 Informa	302013	Built TCP	🔗 ny-asa	172.16	tcp/34457	75.125	tcp/22	autbound 🦉	tcp	🖌 built	63555427	
Firewall Traffic Events last 1	6/7/11 2:27.	. 🔥 Informa	302014	Teardown TCP	🔗 ny-asa	208.72	tcp/5636	10.10.1	tcp/17225		tcp	☐ ⁴ teardown	63555017	
	6/7/11 2:27.	🔥 Informa	302013	Built TCP	🔗 ny-asa	172.16	tcp/27866	208.72	tcp/5636	ref 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	☐ ⁴ teardown	63555015	
	6/7/11 2:27.	🔥 Informa	302013	Built TCP	🔗 ny-asa	172.16	tcp/10323	208.72	tcp/5636	autbound	tcp	🖌 built	63555424	
	6/7/11 2:27.	🔥 Informa	302014	Teardown TCP	🔗 ny-asa	216.188	. tcp/443	10.10.1	tcp/29199		tcp	☐ ^d teardown	63555014	
	6/7/11 2:27.	. 🔥 Informa	302014	Teardown TCP	🔗 ny-asa	75.125	tcp/22	10.10.1	tcp/31612		tcp	☐ ⁴ teardown	63555013	
	6/7/11 2:27.	🔥 Informa	302013	Built TCP	🔗 ny-asa	172.16	tcp/30704	216.188	tcp/443	ref outbound	tcp	🖌 built	63555423	
	6/7/11 2:27.	🔥 Informa	302013	Built TCP	🔗 ny-asa	172.16	tcp/33061	75.125	tcp/22	autbound 🦉	tcp	🖌 built	63555422	
	6/7/11 2:27.	. 🔥 Informa	302021	Teardown I	🔗 ny-asa	38.104	0	172.16	24790		ket icmp	Steardown		
	6/7/11 2:27.	🔥 Informa	302020	Built ICMP	🔗 ny-asa	38.104	0	172.16	24790	🐴 inbound	Ket icmp	🖌 built		
	6/7/11 2:27.	🔥 Informa	302014	Teardown TCP	🔗 ny-asa	208.72	tcp/5636	192.168	tcp/13551		top	☐ ⁴ teardown	63555011	
	6/7/11 2:27.	🔥 Informa	302013	Built TCP	🔗 ny-asa	172.16	tcp/24790	208.72	tcp/5636	autbound 🥵	tcp	🖌 built	63555419	
	6/7/11 2.27	· *-£	202014	Tandaua TCD	Ø	200 70	ton /22.72	100.100	ton/16000				620000	
														-
	50									-				
													2:27	و و 📜

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 5-91.)





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 5-92.



Figure 5-92 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

L

Publication is a 324-page, three-part document. Organizations, 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 an organization 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.

Models As	sessed
RSA Data	Protection Manager version KM-3.1 / AM-6.1.SP3
PCI Sub-Re	equirements 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-Re	equirements Requiring Compensating Controls
No compe	nsating controls were required to satisfy any sub-requirements.
PCI Sub-Re	equirements Failed
No sub-rec	juirements were failed.

Table 5-28 PCI Assessment Summary—RSA Data Protection Manager

Primary PCI Function

The main function of RSA Data Protection Manager is to securely manage the keys that protect cardholder data. (3.5)

Table 5-29 lists the component assessment details for RSA Data Protection Manager.

PRIMARY FUN	anage the keys that protect cardho	
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	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)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
\checkmark	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.
\checkmark	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)
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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)
\checkmark	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 5-29 Component Capability Assessment—RSA Data Protection Manager

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 5-93.)



Figure 5-93 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 5-94 shows an appropriate password policy for PCI compliance.

Figure 5-94 F	Password Policy Settings		
RSA Access Manager: Edit	Password Policy +		
(Contemporal Contemporal Conte] https://rsa-kma.cisco-irn.com/admingui/ListPolicies.jsp?id=1&edit= 🏫 * 🕑 🚼 * Google	2	Feedback
Anost Visited	:S Manager 📄 UIM 📄 NCM 📄 WCS 👩 TACACS 🧭 RSA enVision 📄 HyTrust 端 CM-2 📄 RS	A-AM »	3 Bookma
°	admin: Default Administrative Group/[efault Administra	itive Role
RSA Access M	anager He	lp Options	Log Out
Home Define R	esources Authorize Access Manage Users Delegate Administration		
	ministration > Password Policies	How To	
	ets of requirements for user passwords, such as minimum and maximum password length. Password policies roups and govern password requirements for all users within that administrative group.	Onderstand Password P	3
* is a required field		Add Passw Policies	ord
Password Policy Basics			
i Policy Name	Default Password Policy		
Description	This is the default password policy.		
i Lifetime	90 Days 💌		
i History	Users cannot re-use their previous 4 Passwords		
i Minimum Lifetime	0 Seconds 💌		
Default Policy	Make this the default password policy		
Password Characters			
Minimum length			
Maximum length	32		
i Excluded Characters	^&*(
i Excluded Words File	words.txt		
i Non-alpha Required	Require at least one non-alphabetic character		
Policy Lockout			
i Lock Out	$^{ m O}$ Users can enter an unlimited number of incorrect passwords without being locked out.		
	Cock out a user after 6 incorrect password entries in 1 Days		
i Unlock	C Require an administrator to unlock users who have been locked out. C Automatically unlock users after 30 Minutes		
1 Notification E-mail			
Update <mark>></mark> Cancel	3		

291.571

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 5-94.

• 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 5-94.

• 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 5-94.

• **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 5-94.

• 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 5-94.

• **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 5-94.

• **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 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, organizations 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.

Models Asse	ssed
EMC CLAR	iiON CX-240
EMC Unified	Infrastructure Manager version 2.0.1.1.160
PCI Sub-Requ	uirements 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-Re	quirements Requiring Compensating Controls
No compen	sating controls were required to satisfy any sub-requirements.
PCI Sub-Re	quirements Failed
No sub-req	uirements were failed.

Table 5-30 PCI Assessment Summary – EMC SAN Disk Array (continued)

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 5-31 lists the component assessment details for the EMC SAN disk array.

 Table 5-31
 Component Capability Assessment – EMC SAN Disk Array

PRIMARY FUN Securely ma REQUIREMEN	anage the keys that protect cardho	older data
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	Disable Any Unnecessary Services	*Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system; Remove a unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (Sub-Requirements 2.2.2, 2.2.4)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.
_	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)
+	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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)
1	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 1To 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 5-95.
 - Figure 5-95 Adding LDAP Service

ervice Connection(s):	Rankin	
92.168.42.130	primar	У
dd a new LDAP service conne	ction	<u>A</u> dd
odify selected connection sett	ing	Modify
emove selected connection se	etting(s)	Remove
unchronize accounts with curr	ent service	Synchronize
Synchronization Rate		hour(s) 🔘 day(s)

Step 3 Configure the LDAP server for Active Directory as shown in Figure 5-96.

erver Role	Mapping	Advanced		
IP Address	192	. 168 . 42 . 130	Port Number	636
Server Type	Active Di	rectory 🗸	Protocol	LDAPS
BindDN	CN=Bart M	:Glothin, CN=Users, DC=cisco	-irn,DC=com	
(Example: cr		cation,ou=applications,c	-	om)
Bind Passwor	d	****		
Confirm Bind	Password	****		
Jser Search F				
CN=Users,DC=0 (Example: o		=com ==bigcorp.dc=com)		
Group Search				
N=Users,DC=0				
Add Certifi	cate			

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 5-97.



Add Role Map	ng	
Gro 🛩 <in< th=""><th>sert Name> Monitor</th><th>bbA 💌</th></in<>	sert Name> Monitor	bbA 💌
Туре	Name	Role
Group Group Group	Storage-Admin Storage-Security Storage-Monitor	Administrator Security Administrator Monitor
	Remove	

Figure 5-96 Configuring the LDAP Server for Active Directory

Step 5 The Advanced features were left at their default settings, as shown in Figure 5-98.

oup Object Class group	anced Fields	
oup Name Attribute cn oup Member Attribute member er Object Class (optional) oup Object Class group	er ID Attribute	sAMAccountName
oup Member Attribute member er Object Class (optional) oup Object Class group	er Name Attribute	m
er Object Class (optional)	oup Name Attribute	m
oup Object Class group	oup Member Attribute	member
litional Functions	er Object Class (optional)	
	oup Object Class	group
		settings Duplicate

Figure 5-98 Advanced Settings

Step 6 You can then log out, and log back in, selecting the **Use LDAP** option for centralized authentication, as shown in Figure 5-99.

Figure 5-99 Selecting Use LDAP Function

	emc. ² where information lives.
V1.0.50	
System	192.168.42.51 bmcgloth
Password Scope	Use LDAP
	Login Cancel Help 10 EMC Corporation. All Rights Reserved

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 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 5-100.

Figure 5-100 NTP Configuration for Domain: Local

EMC Unisphere 👔 All Systems ¥ 🔠 Dashboard 🐼 Domains < System List 🛕 Alerts All Systems > Domains NTP Configuration for Domain: Local _ 🗆 × Multi-Domain NTP Control Manage Multi-Domain Configuration Time Sync Interval 🔽 Enable NTP 1 Hour ~ NTP Servers Local Domain ~ × Key ID Key Value Server Select Domain Master Configure NTP 192 . 168 . 62 . 161 Add/Remove Systems Scan for CLARiiON Systems 192 . 162 . 168 . 62 Users ~ . . Manage Global Users Configure LDAP for CLARiiON Systems ¥ 291460 OK Apply Cancel Help

- 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 5-101.)

licas	💼 Monitoring 🗳	😂 Settings 🛛 🧿 Si	
	Reports		
	SP Event Logs		
	Event Notification		
	Analyzer		
	Quality of Service M	anager G	
EMC Un	nisphere	Pool LUN 🔍 Search System 🗊 Storage 👔 Hosts 😨 Replicas 📓 Monitoring 🚿 Settings 🕥 Support	2 👰 🎙 🗷.
EMC-SA	<u>N-1</u> > <u>Monitoring</u> > <u>Event Notific</u>	cation > Notification Templates	
	otification for CLARiiON Storage Syst		
Config	gure Centralized Monitors Distribute	d Monitors Notification Templates	
	fication Templates		2 7 ° 10 30 0
	Filter for		
Nam			
E b	oart RSAenVision	Template Properties	
	SAenvision	General E-Mail Paging SNMP EMC E-Mail Home ConnectEMC	
		Template Name: RSAenWision	
		Events	
		General Event Severity Event Category	
		✓ Information ✓ Basic Array Feature Events	
		Explicit Events Warning Warning SnapView Events (if applicable)	
		✓ Warning ✓ SnapView Events (if applicable) ✓ SAN Copy Events (if applicable)	
		✓ Error ✓ NQM Events (if applicable)	
		Critical Critical	
		Advanced	
		Actions for events	
		Log to System Log Combine Events for Storage System	
		Combine Events for Storage System	
		Add Response	
		OK Apply Capcel Help	
1 Sel	lected Create Delete Pri	operties	2 items
			2 items Last Refreshed: 2011-03-25 14:46:26
			§

Figure 5-101 Using Log to System Log Option

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.

Models As	sessed				
RSA enVi	sion version 4.0, Revision 5				
PCI Sub-R	equirements 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 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-Re	equirements Requiring Compensating Controls				
No compe	nsating controls were required to satisfy any sub-requirements.				
PCI Sub-R	equirements Failed				
No sub-ree	quirements were failed.				

Table 5-32 PCI Assessment Summary—RSA enVision

Primary PCI Function

The main function of RSA enVision is to securely store and correlate the system logs that is receives. (10.5)

Table 5-33 lists the component assessment details for RSA enVision.

PRIMARY FUN Securely sto REQUIREMEN	ore and correlate the system logs t	hat it receives
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	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)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 6.1)
	AUTHENTICATION	
\checkmark	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.
\checkmark	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)
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
\checkmark	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)
1	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 5-33 Component Capability Assessment—RSA enVision

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 5-102.

🕴 System Configuration - RSA enVisio	on - Microsoft Interne	t Explorer				
Overview Alerts Analysis Reports	_+⊐ 📕 🚱					
Dashboard System Performance	Use this wire the services		processing status	of the NIC services and to sta	rt and stop	RSA enVision
Best Practices	Manage Services					
		Site: RSAenVisi	ion 💌			
System Configuration					Logging	
Devices	Start/Stop Service	Service Name	Node	Status	Enabled	Logging Level
 Manage Monitored Devices Manage Device Group Filters 		NIC Alerter	RSAenVision-ES	🔘 Running		6
- Manage Device Attribute Definitions		NIC FVV-1 Lea Client	RSAenVision-ES	Running		6
- Import/Export Device Attributes Manage Device Types		NIC Collector	RSAenVision-ES	Running		6
+ Messages		NIC File Reader	RSAenVision-ES	Running		6
+ Directories		NIC SDEE Collection Service	RSAenVision-ES	🔘 Running		6
+ Users Services		NIC Trapd Service	RSAenVision-ES	🔘 Running		6
- Manage Services		NIC Locator	RSAenVision-ES	🔴 Running		6
 Manage Collector Service Set Up DNS Resolver Service 		NIC Logger	RSAenVision-ES	😁 Running		6
- Set Up DHCP Polling Service	п	NIC Server	RSAenVision-ES	😁 Running	•	6
Set Up Site Communication		NIC DHCP Polling Service	RSAenVision-ES	😝 Stopped	~	6
 Scheduler Service Device Services 		NIC ODBC Service	RSAenVision-ES	e Stopped	•	6
Asset Services		NIC Packager	RSAenVision-ES	Running	•	6
+ Universal Device Collection		NIC Scheduler	RSAenVision-ES	Running		6
 Dashboard Items Watchlists 		NIC Asset Collector Service	RSAenVision-ES	Running		6
Set Up System Performance		NIC Asset Processor Service	RSAenVision-ES	Running	~	6
		NIC Windows Service	RSAenVision-ES	😝 Stopped		6
∢► Vulnerabilities		NIC App Server	RSAenVision-ES	Running		6
Assets		NIC WinSSHD	RSAenVision-ES	Running		
nasets Task Viewer			Apply	Refresh		
lser: bart mcglothin (bmcgloth) Log Out	Connected to:NIC / RS/	AenVision / RSAenVision-ES	Logged in since	: Mon Jun 20 12:57:57 PDT 2011	Server Time: Mon J	un 20 13:11:27 PDT <u>2011</u>
Done						Local intranet

Figure 5-102 RSA enVision Managed Services

• **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 5-103.

🗿 System Configuration - RSA enVisi	on - Microsoft Internet Explorer	_ 🗆 ×
Overview Alerts Analysis Reports		
Dashboard	Use this window to add or modify a user. RSA en	/ision*
System Performance	Manage Users - Add/Modify User	
Best Practices	Manage 03013 - Haa/Mouny 0301	
System Configuration	User information	۲
Devices Manage Monitored Devices Manage Device Group Filters Manage Device Attribute Definition ImportExport Device Attributes Manage Device Types	User ID: bmcgloth Enabled: First name: bat Last name: mcglothin Password: Confirm	
+ Messages + Directories	Description:	
Users	Groups membership	۲
 Manage Users Manage User Sessions Manage Authentication Servers 	Module/Tool permissions	۲
– Manage Groups – Manage Site Log In Permissions	Report permissions	۲
 Manage Device Access Filters Manage Module and Tool Permission 	Report folder permissions	۲
 Manage Event Explorer Permission Set Up Access Denied 	Device access permissions	۲
Display License Information	Site login permissions	۲
 Manage Services Manage Collector Service 	Alert view permissions	۲
Set Up DNS Resolver Service Set Up DHCP Polling Service	Dashboard permissions	۲
Vulnerabilities	Event Explorer permissions	۲
Assets		
Task Viewer	Apply Cancel Delete	
User: bart mcglothin (bmcgloth) Log Out	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
🗐 Done	🕒 📔 🔤 Local intranet	t /

Figure 5-103 RSA enVision User Profile

- 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 5-104.
🎒 System Configuration - RSA en¥isio	n - Microsoft Internet E	plorer		
Overview Alerts Analysis Reports	_ ↓ 🚽 🚱			
Dashboard	A Lise this windo	w to display the Authentication Server c	onfigurations	RSA enVision
System Performance			eningeratione.	Rox christon
Best Practices	Manage Authenticatio	n Servers		
System Configuration 🛛 📿	Delete	Fully Qualified Hostname	IP Address	
system conliguration		RSAenVision-ES.RSAenVision.nic	127.0.0.1	
Devices Manage Monitored Devices Manage Device Group Filters Manage Device Attribute Definition Import/Export Device Attributes Manage Device Types Messages e = = = = = = = = = = = = = = = = =		activedirectory cisco-irn.com	192.168.42.130	
Directories Users Manage Users Manage User Sessions Manage Authentication Servers			tivedirectory.cisco-irn.com er logon name	
 Manage Groups Manage Site Log In Permissions Manage Device Access Filters Manage Module and Tool Permiss 		Port number:	LDAP protocol over TLS/SSL on port 636 LDAP on port 389	
 Manage Event Explorer Permissio Set Up Access Denied Display License Information 		Δρρίγ	Cancel Help	
Services Manage Services Manage Collector Service Set Up DNS Resolver Service Set Up DHCP Polling Service Vulnerabilities				
Assets		Delete	Add	
Task Viewer		Delete	Add	
Jser: bart mcglothin (bmcgloth) Log Out	Connected to:NIC / RSAen'	vision / RSAen Vision-ES Logged in si	nce: Mon Jun 2012:57:57 PDT 2011 Server Time: I	Mon Jun 20 13:23:50 PDT 2011
🗳 Done				🔓 🔍 Local intranet 💦 🍃

Figure 5-104 RSA enVision Authentication 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 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 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 organizations 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.

Models As	sessed	
HyTrust ve	ersion 2.2.1.14064	
PCI Sub-Re	equirements 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	0 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-Re	equirements Requiring Compensating Controls	
No compe	nsating controls were required to satisfy any sub-requirements.	
PCI Sub-Re	equirements Failed	
No sub-rec	quirements 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 5-35 lists the component assessment details for the HyTrust Appliance.

Table 5-35	Component Capability Assessment—HyTrust Appliance
------------	---

	t Appliance	ultult. ^{QSA} cisco Validated
Monitor and		structure by proxying administrative sessions to VMware vCenter
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	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)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.
+	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)
+	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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)
\checkmark	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

L

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.

1 Edi	t Rule			
		Name	PCINetworkAdminOnly	
		Domain User Group	support - HT_PCINetworkAdmin	
		Role	HT_NetworkAdmin	
		Propagate	X	
		Description		
		Assign to Policy Resource	Assign	
C Sele	ct Al 🗌 View	Al		
Add	Delete			
Showin	g 1 to 2 of 2			<< <1>>>>
	Edit	Constraint Type	Description	
	Edit	Client IP Match	172.16.2.10	
Г	Edit	Client Protocol	vSphere (SOAP)	
				Ok Cancel

Figure 5-105 Edit Rule Screen

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 8.5.9—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 5-106). 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.

L



🗷 Administrator: Windows PowerShell	1
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\kcranda]]\Desktop\RecoverPassword-1.0> _	
-	290951

- 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 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 5-107.)

Firefox 🔨		_ 🗆 ×
HE HyTrust - Network Configuration		~
< > 🕅 192.163.42.135 https://192.166.42.135:8443/hytrust/network-config 👷 😴 🚱 - Google	۹	Feedback •
🖉 Most Visited 🕮 UCS-M 📄 UIM 📄 NCM 📄 WCS 🔯 TACACS 🏈 RSA enVision 🖷 HyTrust 🍀 CM-2 📄 RSA-AM 🍀 VSOM 🚾 RSA-KMA 🛈 IronPort	>>	🔝 Bookmarks
H y T r u s t Network Configuration	Ģ	Log Out
General 🔻 Compliance 👻 Policy 👻 Configuration 👻 Maintenance 👻 Help 👻		
📲 Network Configuration		
Router Interface		
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 255.255.2		
Connection 2: IP Address 192.168.41.1		
Connection 2: Mask 255.255.0		
*Gateway 192.168.42.1		
*List of DNS Server IP Addresses 192.168.42.130		
▼ NTP Servers		
Enable NTP Servers 🔽		
*NTP Servers 192.168.62.161,192.168.62.162		
		Apply
Copyright (2) 2009-2011 HyTrust Inc. All rights reserved.		

Figure 5-107 Specifying the NTP Server

290962

- **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—Branch

The Cisco Integrated Services Router (ISR) is the component that is used as the primary routing and security platform of the branches. 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 branches 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.

Models As	ssessed		
CISCO89	1W version c890-universalk9-mz.151-3.T.bin		
CISCO194	41W-A/K9 version c1900-universalk9-mz.SPA.151-3.T.bin		
CISCO292	21/K9 version c2900-universalk9-mz.SPA.151-3.T.bin		
CISCO29	51/K9 version c2951-universalk9-mz.SPA.151-3.T.bin		
CISCO39	45-SPE150/K9 version c3900-universalk9-mz.SPA.151-3.T.bin		
PCI Sub-R	equirements 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-R	equirements Requiring Compensating Controls		
No compe	ensating controls were required to satisfy any sub-requirements.		
PCI Sub-R	equirements Failed		
No sub-re	quirements were failed.		

Table 5-36 PCI Assessment Summary – Cisco ISR

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, an organization 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 branch, 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 organization. They may not be used to filter untrusted networks. For example, many organizations have a central chokepoint in their data center that is the connection to the Internet (an untrusted network). As long as the organization has only untrusted network

connections outside of the branch, (the data center, in this case), then an organization may use router access lists to protect its scope from its own private internal networks. As soon as the branch connects to untrusted networks directly, items 3 and 4 below become relevant. (See Figure 5-108.)



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 branch 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 branch level, firewalling and IDS/IPS must be deployed. (See Figure 5-109.)

Figure 5-109 Using Firewall and IDS/IPS



The Cisco ISR can be used to address segmentation challenges and enforce scope boundaries depending on the levels required by the organization. Each of these features can be enabled by using a license key. This feature is particularly useful for organizations because it does not require a visit to every branch 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 branch 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 5-37 lists the component assessment details for the Cisco ISR.

 Table 5-37
 Component Capability Assessment – Cisco ISR

Cisco I	SR	ciji i ji u ji voji osa cisco Validated
		vorks with ACLs or firewall/IDS/IPS
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	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)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
\checkmark	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.
+	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)
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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)
\checkmark	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 branch 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 branch architectures are maintained with Cisco Prime LMS.

- 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 branch router from the WAN needs to be protected by a branch-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 PCI Solution lab, a private MPLS WAN is simulated, and filtering of the branch 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 branch 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 Cisco Prime LMS. 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
      ip 172.16.0.0 0.15.255.255 any log
denv
      ip 192.168.0.0 0.0.255.255 any log
denv
 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 branch 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:

L

- 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 branch and the enterprise network.

Cisco Virtual Office provides reference designs for building a VPN solution to connect branches 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 branch and the data center headend router. The branch router is referred to as the spoke router, and the data center router as the hub. Figure 5-110 shows a simplified Cisco VPN topology.





Cisco VPN technology connects the branches 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 branches' 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 branch 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, branch 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 Branch 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>

L

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>
```

Cisco Compliance Solution for PCI DSS 2.0 Design and Implementation Guide

```
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 Cisco Prime LMS.

• 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 Cisco Prime LMS.

• 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
```



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 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.shtm

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 branch 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
```

L

```
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 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 branch, security functions are typically separated physically into distinct appliances. The Cisco ASR1002 routers were used for the Internet edge and branch 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, an organization 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 organization. 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, an organization may use router access lists to protect its scope. As soon as the branch 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.

Models As	sessed
ASR-1002	(RP1) version asr1000rp1-adventerprisek9.03.02.01.S.151-1.S1.bin
PCI Sub-Re	equirements 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-Re	quirements Requiring Compensating Controls
No compe	nsating controls were required to satisfy any sub-requirements.
PCI Sub-Re	equirements Failed
No sub-rec	uirements 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 5-39 lists the component assessment details for the Cisco data center routers.

Data C	enter Routers	ululu (sa cisco Validated
PRIMARY FUNCTION Protect trusted networks from untrusted networks with ACLs or firewall/IDS IOS REQUIREMENT: 1, 11 (1.2, 1.3, 11.4)		
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	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)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
\checkmark	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.
+	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, 8.5.13, 8.5.14)
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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)
\checkmark	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 5-39 Component Capability Assessment—Data Center Routers

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 Cisco Prime LMS (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 Cisco ASR1002 was 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.

```
L
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
1
```

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 Cisco Prime LMS. 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.

L

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

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

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 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.

L

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 Cisco Prime LMS.

• 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 Cisco Prime LMS.

• 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
```

L

```
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.shtm



The Cisco 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—Branch

Cisco branch 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.

Branch switches are broken into three categories to provide scale and feature relevance;

- Compact switches—Quiet, small form factor switches that can be used on branch 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 branch 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 branch. 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—Branch Switches

Models Asses	sed	
WS-C2960PD	D-8TT-Lc2960-lanbasek9-mz.122-55.SE1.bin	
WS-C2960G-	8TC-Lc2960-lanbasek9-mz.122-50.SE4.bin	
WS-C2960-87	TC-Lc2960-lanbasek9-mz.122-50.SE4.bin	
WS-C2960S-4	48FPS-Lc2960s-universalk9-mz.122-53.SE1.bin	
WS-C3750X-	48PF-Sc3750e-universalk9-mz.122-53.SE2.bin	
	PD-8PT-Lc2960c405-universalk9-mz.122-55.0.43.SK.bin	
WS-4507+R \$	SUP-7cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin	
WS-C3560X-	48PF-Sc3560e-universalk9-mz.122-53.SE2.bin	
WS-C3560CF	PD-8PT-Lc3560c405ex-universalk9-mz.122-55.0.44.SK.bin	
PCI Sub-Requ	irements 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	
PCI 9	9.1.2	
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-Requ	irements Requiring Compensating Controls	
No compensa	ting controls were required to satisfy any sub-requirements.	
PCI Sub-Requ	irements Failed	
No sub-requir	rements were failed.	

Primary PCI Function

The primary PCI compliance feature of branch switches is to provide secure wired port access. (9.1.2, 11.1)

Branch 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 branch switches allow organizations to put their payment networks into separate VLANs (scopes) from other non-sensitive data (out-of-scope).

Figure 5-111 shows an example of switch segmentation.



Figure 5-111 Cisco Branch 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 branch floor.

Table 5-41 lists the component assessment details for the Cisco branch switches.

Branch Switches PRIMARY FUNCTION Provide secure access to payment devices in the branches REQUIREMENT: 9, 11 (9.1.2, 11.1.b)		
ASSESSMENT	CAPABII ITY	PATTICIPATING ORGANIZATION
155E55MENT		
✓	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)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
\checkmark	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
√	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.
+	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)
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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)
\checkmark	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 5-41 Component Capability Assessment—Branch Switches

Design Considerations

- The configurations of the Cisco Catalyst switches in the branch architectures are maintained within Cisco Prime LMS (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 organization 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.

<u>Note</u>

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

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

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

To meet all of the requirements listed below, the PCI solution 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 Cisco Prime LMS.

• 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 Cisco Prime LMS.

• **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.

L

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 ${\tt attempts}~{\tt 6}$ 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
```



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/a sp_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
```

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.

hidekevs

• **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.shtm

Note

The Cisco 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 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 branch 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
1
! ----Configurations to add for NAC ----
aaa new-model
1
1
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
1
aaa server radius dynamic-author
client 192.168.42.111
server-key 7 <removed>
I.
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
```

L

```
authentication mac-move permit
ip device tracking
ip admission name ise proxy http inactivity-time 60
1
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
T.
! ----Auto Smart Ports Macro method for port configurations-----
1
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

Catalyst65	09-Sup720-3BXL version s72033-adventerprisek9_wan-mz.122-33.SXJ.bin
•	-48P version c3750-ipbasek9-mz.122-55.SE1.bin
PCI Sub-Re	quirements 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-Re	quirements Requiring Compensating Controls
No compe	nsating controls were required to satisfy any sub-requirements.
PCI Sub-Re	quirements Failed
No sub-rec	uirements 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 5-112.)

Figure 5-112 Cisco Catalyst Data Center Switches

 Catalyst Switches with Services Modules VLAN Routing Firewall Segmentation	
Load Balancing Content Inspection and Filtering	
Intrusion Detection and Prevention	2
Wireless Services Control	290977

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 an organization 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, an organization 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 organization. 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 5-43 lists the component assessment details for the Cisco Catalyst data center switches.

		Ire and servers using VLANs, ACLs, and firewall/IPS
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	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)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
\checkmark	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.
+	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)
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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.

Table 5-43 Component Capability Assessment – Cisco Catalyst Data Center Switches

Design Considerations

- The configurations of the Cisco Catalyst switches in the data center and Internet edge architectures are maintained within Cisco Prime LMS (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 organization 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 Cisco Prime LMS. 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

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

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 Cisco Prime LMS.

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 Cisco Prime LMS.

• 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 branch.

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.shtm

Note

The Cisco 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 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 VM ware 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 As	sessed
Cisco Nexus 1000V version 4.2(1)SV1(4)	
PCI Sub-Re	equirements 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-Re	equirements Requiring Compensating Controls
No compe	nsating controls were required to satisfy any sub-requirements.
PCI Sub-Re	equirements Failed
No sub-rec	quirements 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 an organization 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, an organization 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 organization. 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 5-45 lists the component assessment details for the Cisco Nexus 1000V Series Switch.

	CTION regation and access layer connect T: 1	
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	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)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
\checkmark	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.
+	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)
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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)
\checkmark	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 5-45 Component Capability Assessment – Cisco Nexus 1000V Series Switch

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

L

site. The Cisco 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.shtm 1

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 Asse	essed
	5020 Chassis ("40x10GE/Supervisor") version n5000-uk9.5.0.3.N1.1b.bin Chassis ("Supervisor module-1X") version n7000-s1-dk9.5.1.2.bin
PCI Sub-Req	uirements 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 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-Re	equirements Requiring Compensating Controls
No compe	nsating controls were required to satisfy any sub-requirements.
PCI Sub-Re	equirements Failed
No sub-rec	juirements were failed.

Table 5-46	PCI Assessment Summary—Cisco Nexus Data Center Switches (continued)
------------	---

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 an organization 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, an organization 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 organization. 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 5-47 lists the component assessment details for the Cisco Nexus data center switches.

PRIMARY FUNCTION Secure access to payment infrastructure and servers using segmentation of trusted networks (VLANs, ACLs) REQUIREMENT: 1 (1.3.5)			
ASSESSMENT	CAPABILITY		
	SECURITY SERVICES		
\checkmark	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)	
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)	
\checkmark	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)	
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.	
+	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)	
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)	
	LOGS/ALERTS		
+	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 5-47 Component Capability Assessment – Cisco Nexus Data Center Switches

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 Cisco Prime LMS (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 Cisco Prime LMS. 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.



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.

L

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 Cisco Prime LMS.

• 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 Cisco Prime LMS.

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.

L

• **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 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.shtm l

L

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 branch. 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 As	essed	
AIR-CT55	08-12-K9 version 7.0.114.112	
MSE3550	version 7.0.200.125	
Cisco WC	Manager version 7.0.171.107	
AIR-CAP	042N	
AIR-CAP	502i	
AIR-CAP	502E	
AIR-LAP	262N	
PCI Sub-R	quirements Passed	
PCI 2	2.1.1, 2.2, 2.2.2, 2.2.4, 2.3	

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-Red	uirements Requiring Compensating Controls
No compen	sating controls were required to satisfy any sub-requirements.
PCI Sub-Rea	quirements Failed
No sub-requ	irements were failed.

Table 5-48	PCI Assessment Summary—Cisco Wireless Products (continued)

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 5-49 lists the component assessment details for Cisco wireless products.

 Table 5-49
 Component Capability Assessment - Cisco Wireless Products

PRIMARY FUN		eilitilit. OSA cisco Validated					
Secure access to payment infrastructure and servers using segmentation of trusted networks (VLANs, ACLs) REQUIREMENT: 4, 11 (4.1, 11.1)							
ASSESSMENT	CAPABILITY						
	SECURITY SERVICES						
\checkmark	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)					
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)					
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)					
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.					
+	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)					
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)					
	LOGS/ALERTS						
+	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)					
\checkmark	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 branch is required at a minimum of once a quarter, whether or not the organization has wireless deployed. A hacker might infiltrate a branch 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 branch (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 branch 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.



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.

Wireless Deployment	Risk	Required Measure
No wireless deployed	Hacker deploys wireless into branch	Rogue detection
Wireless deployed, no wireless POS/CDE	Hacker deploys unknown wireless into branch, or hacks into existing wireless	Rogue detection Stateful firewall separating wired from wireless LAN Intrusion Detection System
Wireless deployed, includes wireless POS/CDE	Hacker deploys unknown wireless into branch, or hacks into existing wireless	Rogue detection Stateful firewall separating wired from wireless LAN Intrusion Detection System Strong wireless encryption for CDE (e.g., WPA2) Wireless CDE must be protected from other wireless and wired segments using a stateful firewall (Req. 1,2,3)

Table 5-50Wireless Compliance Stages

Cisco recommends using the Unified Wireless (controller-based) architecture for enterprise 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 5-113 and Figure 5-114). 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.

սիսիս	Sa <u>v</u> e Co	nfiguration <u>P</u> ing Lo <u>q</u> out <u>R</u> efresh
CISCO MONITOR	WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT	C <u>O</u> MMANDS HE <u>L</u> P <u>F</u> EEDBACK
WLANs	WLANs > Edit 'jian-ma'	< Back Apply
WLANs	General Security QoS Advanced	
Advanced	Layer 2 Layer 3 AAA Servers	32
	Layer 2 Security WPA+WPA2 MODE To MAC Filtering WPA+WPA2 Parameters	
	WPA Policy WPA2 Policy	
	WPA2 Policy V WPA2 Encryption V AES TKIP	
	Auth Key Mgmt 802.1X V	

Figure 5-113 WLANs Security Screen

ter de te						
ahaha					ve Configuration	<u>P</u> ing Lo <u>g</u> out <u>R</u> efres
cisco	MONITOR WLANS COM	ITROLLER WIRELESS	<u>S</u> ECURITY	MANAGEMENT COM	MANDS HELP	<u>F</u> EEDBACK
Wireless	Global Configuration					Apply
 Access Points All APs Radios	CDP			High Availabil	ity	
802.11b/g/n Global Configuration	CDP State	V		AP Heartbeat Timeout(1-30)	30	
 Advanced Load Balancing 	Ethernet Interface#	CDP State		Local Mode AP Fast Heartbeat Timer State		
Band Select Preferred Calls	1	v		H-REAP Mode / Fast Heartbeat Timer State		
Mesh HREAP Groups	3			AP Primary Discovery Timeout(30 to	120	
802.11a/n Network	Radio Slot# 0	CDP State		3600) Back-up Prima		
✓ RRM RF Grouping TPC	1			Controller IP Address		
DCA Coverage	3			Back-up Prima Controller nan		
General Client Roaming Media EDCA Parameters	Login Credentials			Back-up Secondary Controller IP Address		
DFS (802.11h) High Throughput (802.11n)	Password Enable Password			Back-up Secondary Controller nan	me	
CleanAir 802.11b/g/n	802.1x Supplicant Cre	edentials		TCP MSS		
 Media Stream General Streams 	802.1x Authentication			Global TCP Adj MSS		

Figure 5-114 Wireless Global Configuration Screen

- **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 5-115, Figure 5-116, Figure 5-117, and Figure 5-118 show where to disable non-encrypted management interfaces (for example, Telnet and HTTP).

sco WCS - Server Settings - 192.168.	43.135 +	
) 192.168.43.135 https://	192.168.43.135/webacs/ServerSettingsAction.do?command=init&subMenuBitMa 🏫 👻 😋 🚱 👻 Google	P 🔒 Feedback 🖲
ost Visited 📄 Cisco UCS Manager	UIM 📄 NCM 📄 WCS 📄 TACACS 📄 R5A enVision 📄 HyTrust 📄 CM-2 📄 R5A-AM 👑 V5O	M 🔝 Bookmarl
Alarm Summary 🄍	🔺 40 🔻 3 🔾 8 🗸 Wireless Control System	<ip,name,ssid,mac> Search Advanced Search Saved Search</ip,name,ssid,mac>
sco	User: hm	Advanced Search Saved Search
<u>M</u> onitor ▼ <u>R</u> eports ▼ <u>C</u> onf	igure ▼ Services ▼ Administration ▼ Tools ▼ Help ▼	😧 🕂 불 Logout
Alarms	Server Settings	
Audit	Administration > Settings > Server Settings	
Client	O Changes will take affect on next restart.	
CLI Session	FTP	
Controller Upgrade Settings	C Enable © Disable	
Data Management	Port 21 Default: 21	
Guest Account Settings	Root C:/wcs-ftp	
Login Disclaimer	Rock Joweship	
Mail Server Configuration	TFTP	
Notification Receivers	C Enable © Disable	
Report	Port 69 Default: 69	
Server Settings	Root C:hwcs-fftp	
Severity Configuration		
SNMP Credentials	НТТР	
SNMP Settings	C Enable @ Disable	
Switch Port Trace	Port 80 Default: 80	
	HTTPS	
	Port 443 Default: 443	
	Save	

Figure 5-115 WCS Server Secure Management

Figure 5-116 CLI Session Secure Management



ost Visited 📄 Cisco UCS Manag	r UIM NCM WCS TACACS RSA enVision HyTrust CM-2 RSA-AM 🗰 VSOM	Bookmark
Alarm Summary () SCO Monitor • Reports • C	▲ 40 ▼ 3 0 8 Wireless Control System Advanced Search Saved : Advanced Search Saved : User: <u>bmcqloth</u> @ Virtual Domain: n Infigure ▼ Services ▼ Administration ▼ Tools ▼ Help ▼ ?	root 🔻
<u>monitar e Reports e c</u> Properties System		
VLANs	Telnet SSH Configuration	
I-REAP Security	Template Applied (None)	
ccess Points	Session Timeout 15 (mins) Maximum Sessions 1 3	
02.11	Allow New Telnet Sessions No Allow New SSH Sessions Yes	
02.11a/n 02.11b/g/n	O Allow New SSH Sessions Yes ▼ O Save Audit	
lesh	© Footnotes:	
orts Ianagement	 1. Setting 0 value for 'Maximum Sessions' parameter will cause the CLI session to terminate immediately if logging in using SSH. 	1
Trap Receivers Trap Control Telenet SSH Multiple Syslog Web Admin Local Management Users Authentication Priority		
ocation	lacksquare	_

Figure 5-117 Controller Secure Management for SSH

Figure 5-118 Controller Secure Management for HTTPS

) 192.168.43.135 htt	2.168 +	ebConfinGeneralAction do?	command=detail&controlk ☆ - C	🛃 🕶 Google	P 🏦 Feedback
			enVision HyTrust CM-2		Bookmark
III Alarm Summary	<u>▲ 40</u> ▼		Wireless Control Sys		e,SSID,MAC> Search
ISCO	<u> </u>	2 2			earch <u>Saved Search</u>
Monitor 🔻 Reports 🔻 (6		ools 🔻 Help 🔻	User: <u>bmcgloth</u> @ Virt	tual Domain: root 🔻
<u>M</u> onitor ▼ <u>R</u> eports ▼ <u>(</u> Properties	figure ▼ <u>S</u> ervices ▼ ○ Web Admin :		oois • <u>H</u> eip •		O & E Logour
	Configure > Control		anagement > Web Admin		
System	Ð				
WLANs	WEB Admin		_		
H-REAP	▶ WEB Mode	Disable 💌			
Security	Secure WEB Mode	Enable 💌			
Access Points	Certificate Type				
802.11		b Admin Certificate			
802.11a/n	Save Audit Res	penerate Cert			
802.11b/g/n	• •				
Mesh	Footnotes:				
Ports	 Controller mu certificate to tak 	ist be rebooted for the i e effect	new Web Admin		
Management	•				
Trap Receivers	9				
Trap Control					
Telnet SSH					
Multiple Syslog					
🗎 🛛 Web Admin					
📄 Local Management Users					
Authentication Priority					

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 5-119). 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 5-119 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 5-120.)

Figure 5-120	WLAN Information
--------------	------------------

						ntries 1 - 4 of 4
WLAN ID	Profile_Name	SSID	WLAN/Guest/Remote LAN	Security Policies	<u>Status</u>	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
						ntries 1 - 4 of

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

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT: http://www.cisco.com/en/US/products/products security vulnerability policy.html#cpsirp

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 5-121 and Figure 5-122.

290931

،،ا،،،ا،، cısco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT
Management Summary SNMP HTTP-HTTPS Telnet-SSH Serial Port Local Management Users User Sessions Logs Mgmt Via Wireless	Local Ma User Nam Password Confirm F User Acce	Password	nt Users > Nev	Only V Only		

Figure 5-121 Local Management Users Screen

Figure 5-122 Management Via Wireless Screen

ဂျ၊ဂျ၊ င၊sco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>s</u> ecurity	MANAGEMENT
Management	Managen	nent Via	Wireless			
Summary SNMP HTTP-HTTPS Telnet-SSH Serial Port Local Management Users	Enable Co	ontroller Ma	anagement to be a	accessible from	Wireless Clier	nts 🗌
User Sessions Logs Mgmt Via Wireless						

Cisco WCS is configured to use TACACS+ for authentication of administrators, as shown in Figure 5-123.



Figure 5-123 WCS Manager AAA Authentication Mode

The authentication servers for TACACS+ in WCS Manager are configured as shown in Figure 5-124.

Figure 5-124 WCS Manager TACACS+ Server Configuration

Firefox Gisco WCS - TACACS Server - 192.168	143.1 +
	//192.168.43.135/webacs/tACACSServerGeneralAction.do?command=detailssubl 😭 - C 🕃 - Google 🔎 🍙 Feedback - UIM NCM WCS TACACS RSA enVision HyTrust CM-2 RSA-AM 🕮 VSOM 💽 Boolmarks
CISCO	
Change Fossword Policy AAA Mode Users Groups Active Sessions TACACS+ RADIUS	Administration > AAA > <u>TACACS+</u> > TACACS+ Server Detail TACACS+ Server Port 49 Shared Secret Format ASCII • Shared Secret •••••• Retransmit Timeout 5 (secs) Retries 1 Authentication Type PAP • Local Interface IP 192.168.43.135 •

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 5-125 shows the local password policy that has been modified to meet the minimum requirements as specified by the preceding requirements.

isco WCS - Password Policy - 192.168.	43.1 + 192.168.43.135/webacs/passwordPolicyAction.do?command=forward8subMen. 💮 v C 🕅 🛐 v Google 🔊	Feedback •
lost Visited 📋 Cisco UCS Manager	UIIM NCM WCS TACACS RSA enVision HyTrust CH-2 RSA-AM ## VSOM	Bookmari
Alarm Summary 🄍	▲ 40 ▼ 3 O 8 Wireless Control System Advanced Search	
sco	User: <u>bmcqloth</u> @ Virtual D	omain: root 🔻
<u>M</u> onitor ▼ <u>R</u> eports ▼ <u>C</u> onf	ïgure ▼ <u>S</u> ervices ▼ <u>A</u> dministration ▼ <u>T</u> ools ▼ <u>H</u> elp ▼	🗞 📑 Logout
Change Password	Local Password Policy Administration > AAA > Local Password Policy	
Local Password Policy		
AAA Mode	Password minimum length is 7	
Users	Password cannot contain username or reverse of username.	
Groups	Password cannot be cisco or ocsic (cisco reversed) or any special characters replaced for the same.	
Active Sessions	Root password cannot be the word public.	
TACACS+	No character can be repeated more than three time	
RADIUS	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.	
	Save	

Figure 5-125 WCS Manager Local Password Policy

• **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 5-117 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 5-126 shows the configuration of local logging settings, and Figure 5-127 shows the syslog server configuration used to send logs to RSA enVision.

Figure 5-126 Local Logging Configuration

Firefox 🔻						
Cisco WCS - Logging General - 192.168.4	13.1 +					-
← → 192.168.43.135 https://1	92.168.43.135/webacs/Loggin;	gGenera	Action.do?command=init&subMen	JBIEM 🏫 = 🕑 🚼 = Googi	le 🔎 .	Feedback •
Most Visited Cisco UCS Manager	UIM 🗋 NCM 📄 WCS 🛛		ACS 📄 RSA enVision 📄 HyTru:	st 📄 CM-2 📄 R5A-AM 🗱	VSOM	Bookmark
Alarm Summary 🏵	<u>▲ 40</u> ▼ <u>3</u>	_	O 8 Wireless	Control System	<ip,name,ssid,ma< td=""><td>C> Search</td></ip,name,ssid,ma<>	C> Search
IIIIII Alarm Summary 🕀	A 10 V 2		<u> </u>		Advanced Search	
				User:	: <u>bmcgloth</u> @ Virtual Dor	
			ation ▼ <u>T</u> ools ▼ <u>H</u> elp ▼		U t	🕒 📑 Logout
General Logging Options	General Logging Administration > Logg	j Opti jing Op	ons > General			
SNMP Logging Options						
SysLog Options	General Log Setti Message level	_	rmation 💌	Log File Settings Maximum file size	4 (MB)	
	Enable Log Modules			Number of files		
	chable boy modules		Log Modules		5	
		•	Configuration	File prefix	wcs-%g-%u.log (Use %g to indicate file	number,
			Monitor		96u is the unique numbe will be assigned by loca	
			Fault Analysis		system, eg. wcs-1-0.lo	0
		•	General	Download Log File		
		•	Navigator	Download the log file h	ere. Download	
		7	Reports	Email Log File		
		•	Database Administration	То	Send	
			Communication Protocols	Use comma-separate		
		•	UI General			
		•	Administration			
		•	Tools			
		হ হ	Mobility Services Engine			
			SOAP Communication			
	Save					
						_

Firefox 🔻	
Cisco WCS - Syslog Configuration -	92.168 +
() 192.168.43.135 http	s://192.168.43.135/webacs/Logging5yslogAction.do?command=init&subMenuBitMa 😭 🗸 🕑 🔀 🛛 Google 🛛 👂 🎓 Feedback
Most Visited Cisco UCS Manag	r UIM NCM WCS TACACS RSA enVision HyTrust CM-2 RSA-AM 🗰 VSOM
Image: state sta	
CISCO	Advanced Search Saved Search
	User: <u>bmcqloth</u> @ Virtual Domain: root * onfigure * Services * Administration * Tools * <u>H</u> elp * 🛛 🖓 🕁 Logout
General Logging Options	SysLog Options
SNMP Logging Options	Administration > Logging Options > SysLog
SysLog Options	SysLog Settings
	Enable SysLog 🔽 Enable
	SysLog Host 192.168.42.124
	SysLog Facility USER 💌
	Save
1	

Figure 5-127 WCS Manager Syslog Configuration

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 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 5-128.

Cisco WCS - Configure Controllers - :	192.168 +	F			
)> 192.168.43.135 http:	s://192.168.43	3.135	i/webacs/ntpServerGeneralAction.do?command=list&contro	llerIc 🚖 = 🕑 🚼 = G	ioogle 🔎 🏫 Feedback
Most Visited 📄 Cisco UCS Manage	r 🗋 UIM 🛛	N	CM 📄 WCS 📄 TACACS 📄 RSA enVision 📄 HyTrus	t 📄 CM-2 📄 RSA-AM	utility VSOM Sookma
Alarm Summary 🕀	<u> </u>	10	Vireless	Control System	<ip,name,ssid,mac> Search</ip,name,ssid,mac>
ISCO	<u> </u>				Advanced Search Saved Search
1300				U	Iser: <u>bmcgloth</u> @ Virtual Domain: root 🔻
<u>M</u> onitor - <u>R</u> eports - <u>C</u> o	onfigure 🔻	<u>S</u> er	rvices ▼ <u>A</u> dministration ▼ <u>T</u> ools ▼ <u>H</u> elp ▼		💡 🤣 🖺 Logout
Properties	0		rork Time Protocol		Select a command 💌 Go
System	•	ntigu	re > <u>Controllers</u> > <u>192.168.43.21</u> > System > Network	Time Protocol	
General					Entries 1 - 2 of 2
Commands					
Interfaces			Server Index	Server Address	
Interface Groups			1	192.168.62.161	
Network Route				192.168.62.162	
Mobility Groups		-	2	192.168.62.162	Entries 1 - D - E D
Network Time Protocol					Entries 1 - 2 of 2
QoS Profiles					
DHCP Scopes					
User Roles AP Username Password					
Global CDP Configuration					
AP 802.1X Supplicant Cr					
DHCP					
Multicast					
AP Timers					
WLANs	۲				
H-REAP	۲				
Security	•				
	•				
Access Points					

Figure 5-128 NTP Servers Screen for Controllers

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 5-129 and Figure 5-130.)



սիսիս							Sa <u>v</u> e Confi
cisco	<u>M</u> ONITOR <u>W</u> L	ANs <u>C</u> O	ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS
Security AAA General RADIUS Authentication Accounting Fallback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	AP Policies Policy Configu Accept Self Sig Accept Manufa Accept Local S Authorize MIC Authorize LSC	ned Certif ctured Ins ignificant (APs again	talled Certific Certificate (LS st auth-list or	SC)			
Password Policies Local EAP	AP Authorizatio	on List				Entr	ies 0 - 0 of 0
 Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth Advanced 	Search by MAC	Certific Type		Search ey Hash	1		

Figure 5-130 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.

290945

290944

290946

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 5-131.)

Figure 5-131	Notification	Receiver Screen
--------------	--------------	------------------------

Notification Receiver		
Administration > Settings > Not	fication Receivers > Notification Receiver	
IP Address		
Name		
Receiver Type	 North Bound Guest Access 	
Notification Type 🔍	O UDP ○ TCP	
Port Number	162	
Community	public	
Criteria	Category (1)	
	🗆 All	
	Access Points	Adhoc Rogue
	Clients	Controllers
	Coverage Hole	SE Detected Interference
	Context Aware Notifications	Mesh Links
	Mobility Service	Performance
	Rogue AP	RRM
	Security	□ NCS
	Switches	
	Severity (1) 1	
	🖂 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.

Models As	sessed
	5 ("Supervisor/Fabric-2") version m9500-sf2ek9-mzg.5.0.1a.bin.S4 5 ("Supervisor/Fabric-2") version m9500-sf2ek9-mz.5.0.4.bin
PCI Sub-Re	equirements 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-Re	equirements Requiring Compensating Controls
No compe	nsating controls were required to satisfy any sub-requirements.
PCI Sub-Re	equirements Failed
No sub-red	quirements were failed.

Table 5-51 PCI Assessment Summary – Cisco MDS Storage Switches

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 5-52 lists the component assessment details for Cisco MDS storage switches.

PRIMARY FUN Securely en REQUIREMEN ⁻	crypt cardholder data at rest	
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	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)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
\checkmark	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.
+	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)
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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)
1	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 5-52 Component Capability Assessment – Cisco MDS Storage Switches

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

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

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 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—Branch

The Cisco ASA 5500 Series Adaptive Security Appliances provide secure segmentation within the branch. Their stateful firewall and modular intrusion detection modules enable the branch 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, 5512-X, 5515-X, 5520, 5525-X, 5540, 5545-X, 5550, 5555-X, 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) and virtual modules. 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.

Models As	sessed			
Cisco ASA5515-X w/vIPS Module version asa900-129-smp-k8.bin and IDS version 7.1(6) PCI Sub-Requirements Passed				
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, 10.5.4			
PCI 11	11.4			
PCI Sub-Re	quirements Requiring Compensating Controls			
No compen	sating controls were required to satisfy any sub-requirements.			
PCI Sub-Re	quirements Failed			
No sub-req	uirements were failed.			

Table 5-53 PCI Assessment Summary – Cisco ASA 5500 Series (Branch)

Primary PCI Function

The main function of the branch Cisco ASA firewall is to securely segment public and cardholder data environment branch networks, and provide intrusion detection capabilities. (1.2, 1.3, 11.4)

Table 5-54 lists the component assessment details for the Cisco ASA 5500 Series.

PRIMARY FUNCTION Segment public and cardholder data environment networks within the branch REQUIREMENT: 1, 11 (1.2, 1.3, 11.4)				
ASSESSMENT	CAPABILITY			
	SECURITY SERVICES			
\checkmark	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)		
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)		
\checkmark	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)		
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.		
+	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)		
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)		
	LOGS/ALERTS			
+	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)		
\checkmark	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 5-54 Component Capability Assessment – Cisco ASA 5500 Series (Branch)

Design Considerations

- Select the appropriate Cisco ASA model and IPS module for the traffic needs in the branch.
- For ASAs with SSM modules, connect the external Ethernet interface of the module to the secure management segment of the branch network.
- 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 Cisco Prime LMS. These tools also verify 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
I
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
1
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
1
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
1
! ----One line of the larger access-list permitting traffic----
1
access-list OUTSIDE extended permit object-group CSM_INLINE_svc_rule_73014461184
object-group CSM_INLINE_src_rule_73014461184 object-group POS-Store-MSP
1
! ----Applying the access-list to an interface----
1
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 192.168.41.101 255.255.255.255 MSP-WAN http 192.168.41.102 255.255.255.255 MSP-WAN http 192.168.42.122 255.255.255.255 MSP-WAN http 192.168.42.124 255.255.255.255 MSP-WAN http 192.168.42.133 255.255.255.255 MSP-WAN http 192.168.42.138 255.255.255.255 MSP-WAN telnet timeout 5 ssh 192.168.41.101 255.255.255.255 MSP-WAN ssh 192.168.42.122 255.255.255 MSP-WAN ssh 192.168.42.122 255.255.255 MSP-WAN ssh 192.168.42.124 255.255.255 MSP-WAN ssh 192.168.42.124 255.255.255 MSP-WAN ssh 192.168.42.133 255.255.255 MSP-WAN

• **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-shal aes128-shal aes256-shal
!
! ---Specify strong encryption version of SSH
!
ssh version 2
!
```

SNMP versions 1 and 2(c) transmit data between the SNMP server and the SNMP agent "in the clear". This makes your infrastructure and corresponding infrastructure devices vulnerable to attack and or misuse. SNMP v3 adds authentication and privacy options to secure its communication between SNMP servers and SNMP agents.

Cisco ASA firewalls allow secure administration using SNMP version 3 with encryption and authentication using the "priv" security model.

SNMP groups provide an access control policy to which users are added. The user inherits the security model of the group.

SNMP users are assigned a username, a group to which they belong, authentication password, encryption password, and associated algorithms to use. Authentication algorithms are MD5 and SHA. Encryption algorithms are DES, 3DES, and AES (128,192,256).

```
snmp-server enable
snmp-server group V3Group v3 priv
snmp-server user ciscolms V3Group v3 auth sha <AUTHENTICATION-PASSWORD> priv aes 256
<ENCRYPTION-KEY>
snmp-server user csmadmin V3Group v3 auth sha <AUTHENTICATION-PASSWORD> priv aes 256
<ENCRYPTION-KEY>
```

An SNMP host is the server to which SNMP notifications and traps are sent. SNMP v3 hosts require the SNMP server IP address and SNMP username. Each SNMP host can have only one username associated with it. The user credentials on the NMS (CiscoPrime, EMC NCM, and so on) must match the SNMP username credentials.

snmp-server host MSP-WAN 192.168.42.134 version 3 ciscolms snmp-server host MSP-WAN 192.168.42.139 version 3 ciscolms snmp-server host MSP-WAN 192.168.42.133 version 3 csmadmin

Enable the SNMP traps (this will change depending on environment and business requirements). The following example enables all, but this could be limited to a subset of traps.

```
snmp-server enable traps all
snmp-server location Building SJC-17-1 Aisle 1 Rack 3
snmp-server contact EmployeeA
```

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)

L

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

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT: http://www.cisco.com/en/US/products/products security vulnerability policy.html#cpsirp

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 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 10.5.4—Write logs for external-facing technologies onto a log server on the internal LAN.
- **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 timestamp logging trap informational logging asdm informational logging host MSP-WAN 192.168.42.124

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.

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 Cisco ISE
- 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 As	sessed	
Cisco ASA	5555-X w/vIPS module version asa900-129-smp-k8.bin and IPS version 7.1(6)E4	
Cisco ASA	A5585-S60-2A-K9 asa901-smp-k8.bin	
PCI Sub-Re	equirements 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, 10.5.4	
PCI 11	11.4	
PCI Sub-Re	equirements Requiring Compensating Controls	
No compe	nsating controls were required to satisfy any sub-requirements.	
PCI Sub-Re	equirements Failed	
No sub-rec	uirements 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 branch routers.

Table 5-56 lists the component assessment details for Cisco ASA 5500 Series.

Table 5-56 Component Capability Assessment – Cisco ASA 5500 Series (Data Center)

PRIMARY FUNCTION Restrict traffic between the cardholder data environment and other network areas, and as an IPS REQUIREMENT: 1, 11 (1.2, 1.3, 11.4)			
SSESSMENT	CAPABILITY		
	SECURITY SERVICES		
\checkmark	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)	
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)	
\checkmark	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)	
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.	
+	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)	
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)	
	LOGS/ALERTS		
+	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)	
1	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. For virtual modules, the Management 0 interface is used.
- 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 branch WAN, Internet edge, and data center aggregation block.

PCI Assessment Detail—PCI Sub-Requirements Satisfied

1

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----
1
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
I.
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
I.
! ----One line of the larger access-list permitting traffic----
1
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
1
! ----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.

L

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 192.168.41.101 255.255.255.255 south http 192.168.42.102 255.255.255.255 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 192.168.41.101 255.255.255.255 south ssh 192.168.42.122 255.255.255.255 south ssh 192.168.42.122 255.255.255.255 south ssh 192.168.42.124 255.255.255.255 south ssh 192.168.42.124 255.255.255 south ssh 192.168.42.133 255.255.255 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
!
```

SNMP versions 1 and 2(c) transmit data between the SNMP server and the SNMP agent "in the clear". This makes your infrastructure and corresponding infrastructure devices vulnerable to attack and or misuse. SNMP v3 adds authentication and privacy options to secure its communication between SNMP servers and SNMP agents.

Cisco ASA firewalls allow secure administration using SNMP version 3 with encryption and authentication using the "priv" security model.

SNMP groups provide an access control policy to which users are added. The user inherits the security model of the group.

SNMP users are assigned a username, a group to which they belong, authentication password, encryption password, and associated algorithms to use. Authentication algorithms are MD5 and SHA. Encryption algorithms are DES, 3DES, and AES (128,192,256).

```
snmp-server enable
snmp-server group V3Group v3 priv
snmp-server user ciscolms V3Group v3 auth sha <AUTHENTICATION-PASSWORD> priv aes 256
<ENCRYPTION-KEY>
snmp-server user csmadmin V3Group v3 auth sha <AUTHENTICATION-PASSWORD> priv aes 256
<ENCRYPTION-KEY>
```

An SNMP host is the server to which SNMP notifications and traps are sent. SNMP v3 hosts require the SNMP server IP address and SNMP username. Each SNMP host can have only one username associated with it. The user credentials on the NMS (CiscoPrime, EMC NCM, and so on) must match the SNMP username credentials.

snmp-server host south 192.168.42.134 version 3 ciscolms
snmp-server host south 192.168.42.139 version 3 ciscolms
snmp-server host south 192.168.42.133 version 3 csmadmin
Enable the SNMP traps (this will change depending on environment and business
requirements). The following example enables all, but this could be limited to a
subset of traps.
snmp-server enable traps all
snmp-server location Building SJC-17-1 Aisle 1 Rack 3
snmp-server contact EmployeeA

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.

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

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

To meet all of the requirements listed below, the PCI solution 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
1
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 Cisco Prime LMS 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 Cisco Prime LMS 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 timestamp logging trap informational logging asdm informational logging host south 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 south
ntp server 192.168.62.161 source south 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.shtm



The Cisco 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 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

• **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.

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 Services Module (ASASM)—Data Center

The Cisco ASA Services Module (ASASM) is an integrated module installed inside a Cisco Catalyst 6500 Series Switch or Cisco 7600 Internet Router. The Cisco ASASM allows any port on the Cisco Catalyst switch to operate as a firewall port and integrates firewall security inside the network infrastructure.

The Cisco ASASM 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 ASASM to act as a Layer 2 bridging firewall, resulting in minimal changes to network topology.

Table 5-57 PCI Assessment Summary—Cisco ASA Services Module

Models Assessed

WS-SVC-ASA-SM1 version asa851-smp-k8.bin

PCI Sub-Re	equirements 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, 10.5.4
PCI Sub-Re	equirements Requiring Compensating Controls
No compe	nsating controls were required to satisfy any sub-requirements.
PCI Sub-Re	equirements Failed
No sub-rec	uirements were failed.

Table 5-57 PCI Assessment Summary – Cisco ASA Services Module

Primary PCI Function

The primary function of the Cisco ASASM is to restrict traffic between the cardholder data environment and other areas of the network (1.2, 1.3).

Table 5-58 lists the component assessment details for the Cisco ASASM.

PRIMARY FUN Restrict traf REQUIREMEN	fic between the cardholder data e	nvironment and other network areas
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	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)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
\checkmark	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.
+	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)
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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)
v	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 5-58 Component Capability Assessment – Cisco ASA Services Module

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 ASASM. 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 ASASM.
- Configure appropriate banner messages on login, incoming, and exec modes of the Cisco ASASM. The login banner warning should not reveal the identity of the company that owns or manages the Cisco ASASM. 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 ASASM 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 ASASM 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 ASASM.

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 ASASM 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 Cisco Prime LMS. These tools also verify 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 ASASM 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. ASASM 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
11
! ----Defining Objects and Object Groups----
1
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
(ASASM-DMZ-1 v1/mandatorv)
port-object eq smtp
port-object eq https
port-object eq ssh
1
object-group network CSM_INLINE_src_rule_81604379580
description Generated by CS-Manager from src of FirewallRule# 7
(ASASM-DMZ-1_v1/mandatory)
group-object DC-ALL
group-object Stores-ALL
1
! ----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----
I.
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 ASASM 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 192.168.41.101 255.255.255.255 inside http 192.168.42.102 255.255.255.255 inside http 192.168.42.122 255.255.255.255 inside http 192.168.42.124 255.255.255.255 inside http 192.168.42.133 255.255.255.255 inside http 192.168.42.138 255.255.255.255 inside ssh 192.168.41.101 255.255.255.255 inside ssh 192.168.42.122 255.255.255 inside ssh 192.168.42.122 255.255.255 inside ssh 192.168.42.124 255.255.255 inside ssh 192.168.42.124 255.255.255 inside ssh 192.168.42.124 255.255.255 inside ssh 192.168.42.124 255.255.255 inside ssh 192.168.42.133 255.255.255 inside ssh 192.168.42.138 255.255.255.255 inside

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

Cisco ASASM 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 ASASM 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
!
```

SNMP versions 1 and 2(c) transmit data between the SNMP server and the SNMP agent "in the clear". This makes your infrastructure and corresponding infrastructure devices vulnerable to attack and or misuse. SNMP v3 adds authentication and privacy options to secure its communication between SNMP servers and SNMP agents.

Cisco ASA firewalls allow secure administration using SNMP version 3 with encryption and authentication using the "priv" security model.

SNMP groups provide an access control policy to which users are added. The user inherits the security model of the group.

SNMP users are assigned a username, a group to which they belong, authentication password, encryption password, and associated algorithms to use. Authentication algorithms are MD5 and SHA. Encryption algorithms are DES, 3DES, and AES (128,192,256).

```
snmp-server enable
snmp-server group V3Group v3 priv
snmp-server user ciscolms V3Group v3 auth sha <AUTHENTICATION-PASSWORD> priv aes 256
<ENCRYPTION-KEY>
snmp-server user csmadmin V3Group v3 auth sha <AUTHENTICATION-PASSWORD> priv aes 256
<ENCRYPTION-KEY>
```

An SNMP host is the server to which SNMP notifications and traps are sent. SNMP v3 hosts require the SNMP server IP address and SNMP username. Each SNMP host can have only one username associated with it. The user credentials on the NMS (CiscoPrime, EMC NCM, and so on) must match the SNMP username credentials.

snmp-server host south 192.168.42.134 version 3 ciscolms snmp-server host south 192.168.42.139 version 3 ciscolms snmp-server host south 192.168.42.133 version 3 csmadmin

Enable the SNMP traps (this will change depending on environment and business requirements). The following example enables all, but this could be limited to a subset of traps.

```
snmp-server enable traps all
snmp-server location Building SJC-17-1 Aisle 1 Rack 3
snmp-server contact EmployeeA
```

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 ASASM 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

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

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 ASASM 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 ASASM 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 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 ASASM 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 Cisco Prime LMS or Cisco Security Manager.

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

Cisco ASASM 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 Cisco Prime LMS or Cisco Security Manager.

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

Cisco ASASM 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 ASASM 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 ASASM 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 ASASM 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 ASASM 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 ASASM firewalls are able to time-out administrative sessions using the following configuration statements:

```
!
http server idle-timeout 15
```

Cisco Compliance Solution for PCI DSS 2.0 Design and Implementation Guide

```
!
ssh timeout 15
!
console timeout 15
```

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

Cisco ASASM 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 ASASM 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 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 Cisco ASASM uses the clock of the Cisco Catalyst chassis as configured in the Supervisor Module.

To meet all of the requirements listed below, the PCI solution 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 organization'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 As	Is Assessed	
Nexus VS	G 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	

Table 5-59 PCI Assessment Summary—Cisco VSG

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 5-60 lists the component assessment details for the Cisco VSG.

Table 5-60 Component Capability Assessment – Cisco VSG

Cisco VSG PRIMARY FUNCTION Restrict traffic between the cardholder data environment and other network areas REQUIREMENT: 1 (1.2, 1.3)		
ASSESSMENT	CAPABILITY	
	SECURITY SERVICES	
\checkmark	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)
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.
+	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)
\checkmark	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)
	LOGS/ALERTS	
+	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)
V	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.



Cisco Nexus VSG System Architecture

PCI Assessment Detail—PCI Sub-Requirements Satisfied

Figure 5-132

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 Cisco Prime LMS. 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 5-133.)





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.

Г

• **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.

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

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 5-134.)

L



Figure 5-134 Configuring Roles

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 5-135.)

Figure 5-135 Configuring Locales



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 5-136.)



Figure 5-136 Configuring LDAP Server

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 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 5-137.

Figure 5-137 Configuring NTP

Add DNS Server			
Add DNS Server	🛛 Up 🚽 Down	Add NTP Server	🏫 Up 🛛 🕹 Dow
IP Addres	S	Hos	tname

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.

 Navigate to Policy Management > Device Policies > Tenant> Policies > Syslog Policies. Add a syslog policy, as shown in Figure 5-138.



Figure 5-138 Configuring Syslog

2. The severity of the logging should be at level 6 to capture the firewall policy hit in the VSG. (See Figure 5-139).

Figure 5-139 Configuring Logging Severity

Add Syslog S	erver	0
Server Type: Hostname / IP Address:	primary 10.29.172.53	
Severity:	information (6)	
Forwarding Facility: Admin State:	enabled V	
		OK Cancel

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 IDSM2 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.

Models As	sessed	
WS-SVC-I	DSM-2 version 7.0(4)	
PCI Sub-Re	equirements 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-Re	equirements Requiring Compensating Controls	
No compe	nsating controls were required to satisfy any sub-requirements.	
PCI Sub-Re	equirements Failed	
No sub-rec	uirements were failed.	

 Table 5-61
 PCI Assessment Summary – Cisco IDSM2

Primary PCI Function

The primary PCI function of the Cisco IDSM2 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 5-62 lists the component assessment details for the Cisco IDSM2.

Cisco IDSM2 PRIMARY FUNCTION Monitor all traffic at the perimeter of the CDE as well as all critical points inside the CDE REQUIREMENT: 11 (11.4)				
ASSESSMENT	CAPABILITY			
	SECURITY SERVICES			
\checkmark	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)		
\checkmark	Secure Administrative Access	Encrypt all non-console administrative access using strong cryptography. (Sub-requirement 2.3)		
	Uses SNMP Version 3—SNMP	Versions 1 and 2 are considered insecure. (Verizon Recommended)		
\checkmark	Vendor Supported	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. (Sub-Requirements 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.		
+	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)		
+	Admin Session Timeout	PCI Requires a timeout for sessions that are idle for more than 15 minutes, thereafter requiring the user to re- authenticate to renew access to the terminal or session. (Sub-Requirement 8.5.15)		
	LOGS/ALERTS			
+	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)		
1	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 5-62 Component Capability Assessment—Cisco IDSM2

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 192.168.41.101/32
access-list 192.168.42.122/32
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

The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

For more information about PSIRT: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#cpsirp

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

L

- **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 you 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	9	bart	administrator
5824		(pauljones)	viewer
9802	2	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.

Note

IPS Software version 7.1.x and newer supports a CLI activity timer addressing this desired functionality. To enable, enter the "cli-inactivity-timeout 15" command in the Service Authentication portion of the configuration.

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.shtm 1

Note

The Cisco 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 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
!
```

L

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.