снарте **7**5

Component Assessment

This chapter discusses the function of each component and how it helps to address HIPAA compliance requirements. Each component was assessed by Verizon Business, and the full reference architecture report is available in Appendix C, "Reference Architecture Assessment Report—Cisco Healthcare 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
- Assessment summary
- Primary function
- Design considerations
- Assessment detail

Description

A high level overview of the products, features, and capabilities with relevance to compliance.

Assessment Summary

For each component, the Assessment Summary table lists each of the HIPAA safeguards that were addressed or failed.

Table 5-1 shows an example.

Models Assessed	
-----------------	--

CISCO891W version c890-universalk9-mz.151-3.T.bin

CISCO1941W-A/K9 version c1900-universalk9-mz.SPA.151-3.T.bin

CISCO2921/K9 version c2900-universalk9-mz.SPA.151-3.T.bin

CISCO2951/K9 version c2951-universalk9-mz.SPA.151-3.T.bin

CISCO3945-SPE150/K9 version c3900-universalk9-mz.SPA.151-3.T.bin

HIPAA Safeguards	s Addressed
Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Response and Reporting
Technical	Standards/Implementation Specifications
164.312	(a)(1) Access Control
	(b) Audit Controls
	(e)(2)(ii) Encryption
HIPAA Standards	Failed
No HIPAA standa	rds were failed.
HIPAA Implement	ation Specifications Failed
· · · · · · · · · · · · · · · · · · ·	

No HIPAA implementation specifications were failed.

Primary Function

A HIPAA-relevant description of how this device is useful in an enterprise for addressing HIPAA compliance.

Design Considerations

This section provides compliance principles as well as best practices for each technology deployed within a clinic or hospital environment.

Assessment Details

A comprehensive list of the HIPAA safeguard citations addressed including sample device configurations.

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.

Models Assess	ed
Cisco Unified C	Communication Manager 8.5.1
HIPAA Safegua	ds Addressed
Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(6)(i) Response and Reporting
	(a)(6)(ii) Security Incident Procedures
Technical	Standards/Implementation Specifications
164.312	(a)(i) Access Control
	(b) Audit Controls
	(c)(1) Data Integrity
HIPAA Standard	ls Failed
No HIPAA stan	dards were failed.
HIPAA Impleme	ntation Specifications Failed
No HIPAA imp	lementation specifications were failed.

Table 5-2 PHI HIPAA Assessment Summary – Cisco IP Voice Control

Primary PHI Function

The primary function of the Cisco Unified Communications Manager in a healthcare network environment is to securely manage IP phones and communications flows, as well as securing publicly accessible network jacks in clinics and hospitals.

Design Considerations

The Cisco Unified Communication Manager is used to configure all of the communications infrastructure within the enterprise including ip phones, video endpoints, recording devices and conferencing bridges. Additionally it can also configure the flow of communications throughout the network.

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:

- Disable the gratuitous ARP setting on the Cisco Unified IP Phones.
- 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

HIPAA Assessment Detail—HIPAA Safeguards Addressed

Here is a brief on communications from the HIPAA final rule:

Treatment sessions provided via video and audio conferencing software are not covered by the Security Rule. The HIPAA Final Rule specifically states "because 'paper-to-paper' faxes, person-to-person telephone calls, video teleconferencing, or messages left on voice-mail were not in electronic form before the transmission, those activities are not covered by this rule" (page 8342). If, however, the provider records the session and saves a copy, the saved version would be subject to Security Rule provisions for data at rest. Regardless, the treatment session and all related information and documentation from it are subject to the Privacy Rule provisions. To ensure the patient's privacy during treatment sessions, clinicians should consider the use of private networks or encrypted videoconferencing software.

The HIPAA definition of electronic media is as follows:

Subpart A – General Provisions

§160-103

Electronic Media means:

(1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

This solution validation did not include storage or recording of voice or video communications, therefore no implementation steps are shown on how to secure recorded ePHI.

All of the sample configurations shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
 - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - \$164.308(a)(6)(i) Security Incident Procedures. Implement policies and procedures to address security incidents.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.

L

- §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.

Sample Configuration

Cisco Unified Communication Manager is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. They were met using the Cisco Unified Communication Manager's internal user database, because it has extensive features for administering users. 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 and roles are based on group membership.

End users and administrators are added to the system by creating user IDs and passwords in the User Management section of the Cisco Unified Communication manager web interface, as shown in Figure 5-1.

System 👻 Call Routing 👻 Me	edia Resources 👻 🖌	Advanced Features 👻	Device 👻	Application 👻	Use	er Management 👻	Bulk Administration 👻	• Help 🗸	
End User Configuration						Credential Policy I Credential Policy	Default	Related Links: Back to Find List Users 👻 Go	
Save						Application User			
Status]	End User			•
(i) Status: Ready						Role			1
U Status: Keday						User Group			1
User Information						User/Phone Add			1
User ID*						Application User	CAPF Profile		1
Password						End User CAPF P	rofile		1
Confirm Password						SIP Realm			1
PIN					_				ē.
Confirm PIN									1
Last name*									1
Middle name									1
First name									1
Telephone Number									1
Mail ID									
Manager User ID									
Department									
User Locale	< None >			-					
Associated PC									
Digest Credentials									
Confirm Digest Credentials									

Figure 5-1 End User Configuration

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 5-2.)

le Configuration		Related Links: Back To Find/Lis	st 🔻 Go
Copy 🛟 Add New			
ole Information			
Application * Cisco Call Manager Administration			1
lame* Standard CCM Service Management			-
Description Standard CCM Service Management			
esource Access Information	Description	Privilege	
AAR Group web pages	Description	read update	
Access List		read update	
Add Unity User		read update	
Announcement		read update	
Annunciator web pages		✓ read ✓ update	
Application Dial Rules web pages		read update	
Application Server		🗖 read 🔲 update	
Application User CAPF		read update	
Application User Web Pages		🔲 read 🔲 update	
BLF Directed Call Park		🗖 read 🔲 update	
BLF Speeddial		🗖 read 🔲 update	
Blocked Learned Pattern		🗖 read 🔲 update	
Blocked Learned Patterns		🗖 read 🗖 update	
Bulk Add/Update Lines		🔲 read 🔲 update	
Bulk Add/Update Phones		🗖 read 🗖 update	
Bulk CUPS User Page		🔲 read 🔲 update	
Bulk Config Tool Export		🗖 read 🗖 update	
Bulk Config Tool Import		🔲 read 🔲 update	
Bulk Config Tool Import Validation		🗖 read 🔲 update	
Bulk Delete Access List		🗖 read 🔲 update	
Bulk Delete Call Pickup Group		🗖 read 🔲 update	
Bulk Delete Client Matter Codes		🗖 read 🔲 update	
Bulk Delete Fallback Profile		🗖 read 🔲 update	
Bulk Delete Forced Authorization Codes		🗖 read 🔲 update	
Pulli Dalata Catallaria			

Figure 5-2 Role Configuration

Cisco Unified Communication Manager supports configuring a credential policy for user management and applying that policy to a designated group. Figure 5-3 shows a modified default credential policy.

Figure 5-3 User Credential Policy Configuration

System - Call Routing - Media Resources - Advanced Featu	res • Device • Application • User Management • B	ulk Administration 👻 Help 👻
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.		

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	Check this check box to require the system to disallow credential that are easily hacked, such as common words, repeated character patterns, and so on. The default setting checks the check box.	III 290984
-----------	---	---------------

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)

The Cisco Unified Communication Manager uses various role definitions for permitting access to various application components on the server. (See Figure 5-4.)

Figure 5-4 Find and List Roles

ystem 👻 Call Routing 👻 Media Resources 👻 Advanced Features 👻 Device	▼ Application ▼ User Management ▼ Bulk Adr	ninistration 👻 Help 👻	
nd 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	ß
Standard Admin Rep Tool Admin		Administer CAR	ß
Standard Audit Log Administration	Cisco Call Manager Serviceability	Serviceability Audit Log Administration	r <u>b</u>
Standard CCM Admin Users		All users with access to CCM web site	ß
Standard CCM End Users		Access to CCM User Option Pages	6
Standard CCM Feature Management	Cisco Call Manager Administration	Standard CCM Feature Management	Di la
Standard CCM Gateway Management	Cisco Call Manager Administration	Standard CCM Gateway Management	0
Standard CCM Phone Management	Cisco Call Manager Administration	Standard CCM Phone Management	ß
Standard CCM Route Plan Management	Cisco Call Manager Administration	Standard CCM Route Plan Management	D.
Standard CCM Service Management	Cisco Call Manager Administration	Standard CCM Service Management	0
Standard CCM System Management	Cisco Call Manager Administration	Standard CCM System Management	ß
Standard CCM User Management	Cisco Call Manager Administration	Standard CCM User Management	D.
Standard CCM User Privilege Management	Cisco Call Manager Administration	Standard CCM User Privilege Management	0
Standard CCMADMIN Administration	Cisco Call Manager Administration	Administer all aspects of CCMAdmin system	ľb –
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	Ū.
Standard CCMADMIN Read Only	Cisco Call Manager Dialed Number Analyser	Read access to all CCMAdmin resources	ß
Standard CCMUSER Administration	Cisco Call Manager End User	Administer all aspects of CCMUser system	0
Standard CTI Allow Call Monitoring	Cisco Computer Telephone Interface (CTI)	Allow monitoring of calls	ß
Standard CTI Allow Call Park Monitoring	Cisco Computer Telephone Interface (CTI)	Allow monitoring of call park DNs	ß
Standard CTI Allow Call Recording	Cisco Computer Telephone Interface (CTI)	Allow recording of calls	6
Standard CTI Allow Calling Number Modification	Cisco Computer Telephone Interface (CTI)	Allow calling number modification	6
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 a conf	(CTI)	Standard CTI Allow Control of Phones supporting Connected Xfer and conf	6
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	6
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	r M 🕹 🕻

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco Unified Communications Manager enforces this as 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.

To address the Incident Response and Auditing HIPAA Safeguards identified above, 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 5-5 and Figure 5-6 show the configurations necessary for log forwarding.

cisco	Cisco Unified CM A For Cisco Unified Communi			bmcglo			Unified CM A Imentation			
System 👻	Call Routing 👻 Media Resources 👻	Advanced Features 👻	Device 👻	Application 👻	User Ma	nagement 👻	Bulk Admini:	stration 👻	Help 👻	
Enterprise	Parameters Configuration									
Save	🧀 Set to Default	🧷 Apply Config								
Remote S	yslog Agent Tyslog Server Name	192.168.42.124								
<u>Syslog Se</u> <u>messages</u>	<u>s *</u>	Informational				🖵 Error				291558

Figure 5-5 Enterprise Parameters Configuration

Figure 5-6 shows the necessary configuration under Cisco Unified Serviceability.

Figure 5-6 Adult Log Configuration	
CISCO Unified Serviceability For Cisco Unified Communications Solutions	Navigation Cisco Unified Serviceability GO
<u>A</u> larm → <u>T</u> race → To <u>o</u> ls → <u>S</u> nmp → <u>H</u> elp →	
Audit Log Configuration	
🔚 Save 🤣 Set to Default	
Status () Status : Ready	
Select Server	
Apply to All Nodes	
Application Audit Log Settings Filter S	Remote Syslog Audit Event Level Informational 💌
Output Settings Maximum No. of Files* 366 Maximum File Size (MB)* 10	
−Database Audit Log Filter Settings ✓ Enable Audit Log De	bug Audit Level Schema Only
Output Settings ✓ Enable Audit Log Rotation Maximum No. of Files* 40 No. of Files Deleted on Log Rotation* 20	
SaveSet to Default	

Within the Cisco Unified Communications Manager appliance operating system, root access to the OS is disabled and this prevents any unwanted services from being implemented. To secure authentication information and management of the server, addressing safeguard 164.308(a)(1)(i) Security Management, Telnet and HTTP access to the server for administration is disabled. The communication between phones and server over HTTP can be secured using SSL. (See Figure 5-7.)

Figure 5-6 Audit Log Configuration

CISCO For Cisco Unified Com	munications Solutions bmcgloth Search Documentation Abo	ut Logou
stern 👻 Call Routing 👻 Media Resourc	ces ▼ Advanced Features ▼ Device ▼ Application ▼ User Management ▼ Bulk Administration ▼ Help ▼	
terprise Parameters Configurati	tion	
] Save 🧀 Set to Default 🌳 Res	set 🥜 Apply Config	
		1
	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		
Secured Authentication URL Secured Directory URL Secured Idle 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	
Secured Phone URL Parameters Secured Authentication URL Secured Directory URL Secured Idle URL Secured Information URL Secured Messages URL	https://cm-2.cisco-irn.com:8443/ccmcip/authenticate.jsp https://cm-2.cisco-irn.com:8443/ccmcip/xmldirectory.jsp	

Figure 5-7 Enterprise Parameters Configuration

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.

As a best practice, it is recommended to restrict physical and or logical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized. As Cisco IP phones include a pass-through port on them allowing a device to be connected to the network on which an IP phone resides, it is recommended to disable these ports or have them connect to a guest network segment when not intended for use on the ePHI network. Disabling the PC port can be accomplished in the phone configuration window for ports that are not in use, as shown in Figure 5-8.

Inclusion Cisco Unified CM Admir Isco For Cisco Unified Communications			-	d CM Administration 👻
em 👻 Call Routing 👻 Media Resources 👻 Advar	nced Features • Device • Application • User Management •	Bulk Administration 👻 Help 👻		
ne Configuration		Related Links: Back To F	ind/List	•
Save 🗶 Delete 🗋 Copy 嗋 Reset 🥖	Apply Config 🖧 Add New			
	C 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			
	route specific comparation cayour	🦻 Parat	m	Override Common Settings
	Disable Speakerphone	a		Settings
	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	Enabled	•	
	Advertise G 722 Codec*	Une Contras Defeats		

Figure 5-8 Phone Configuration

As a best practice, 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 Unified Communications Manager uses NTP by configuring the NTP server, as shown in Figure 5-9.

Figure 5-9 NTP Server List



Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications 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 clinic, hospital, and data center environment. Video surveillance for loss prevention can now be extended into the area of protecting the ePHI data environment.

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

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

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

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

Table 5-3 PHI HIPAA Assessment Summary – Cisco Video Surveillance

Models Assessed

Cisco Video Surveillance Manager version 6.3.1

HIPAA Safeguards Addressed	
Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(6)(i) Response and Reporting
	(a)(6)(ii) Security Incident Procedures
Physical	Standards/Implementation Specifications
164.310	(a)(1) Facility Access Controls
HIPAA Standards Fai	iled
No HIPAA standa	rds were failed.
HIPAA Implementa	tion Specifications Failed

No HIPAA implementation specifications were failed.

Primary PHI Function

The primary function of video surveillance is to monitor physical access to sensitive areas within the ePHI data environment.

Design Considerations

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

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

A best practices guide is available for *Securing Cisco Video Surveillance Manager* at the following URL: http://www.cisco.com/en/US/docs/security/physical_security/video_surveillance/network/design/bestp rac.html#wp62691

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of Cisco Video Surveillance shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict Access to ePHI Data as required by HIPAA Administrative and Technical Safeguards
 - \$164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
 - §164.310(a)(1) Facility Access Control: Implement policies and procedures to limit physical
 access to its electronic information systems and the facility or facilities in which they are
 housed, while ensuring that properly authorized access is allowed.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.

- \$164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
- §164.308(a)(6)(i) Response and Reporting. Implement policies and procedures to address security incidents. Requirements addressed include: Incident Response and Auditing.
- §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.

Cisco VSOM is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership. The role configuration menu in the VSOM 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

L

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

Firefox *			_ 0 ×
Kideo Surveillance Operations Manage	er 📉 🗋 Video Surveillance Management	a second s	
+> P http://msp-dc-1/v	smc.html	🏫 - C 🚼 - Google	P 👚 Feedback *
Annual Cisco UCS Manager	UIM NON WES TACAES	RSA enlision 🗋 HyTrust 🗋 CH-2 🗋 RSA-AM 🚢 VSOM	Dookmarks
cisco		Video Surveillan	ce Management Console
Overview	On ensting a Manager C	anfiguration	
installed Packages	Operations Manager C	onnguration	-
Status Console	Log Level	and the second	
Monitoring	Log Level	Notice (Default)	
Archives	Database Connection		
Archive Backup	Database Type:	MySQL 5.0 💌	
System Log	Database Server	localhost	
Mediaout Server Status	Database Username.	cisco	
	Database Password	•••••	
Configuration	Database Name.	baa	
SNMP Trap Destinations	Database Version	6.3.1-12	
44 Media Server	Database Configuration Validatio	a	
🚳 Media Server Backup	Database Status	Validate DB	
Operations Manager		(Unsaved configurations can not be validated)	
Operations Manager Backup	SMTP Parameters		
Virtual Matrix	SMTP Parameters SMTP Server		_
Console Password Camera Firmware Upgrade			
Server Upgrade	SMTP "From." Address:	(Only affects to newly created or updated event setups)	
Restart Server			
Reboot Server	User Login Authentication		
-	Authentication Type:	LDAP Server	
Other Utilities	LDAP Configuration		
BWT Pages		171.68.38.106	
Media Server User Guide	Host Port	389	
Support Report		CN=\userneme00=Employees,00=Cisco Users	-
	Domain Controllers (DC)	dc=cisco.dc=com	-
	Delimiter		
	Select Homepage		_
	Change default homepage to VSOM	6	
	Change default homepage to VSMC		
		Update Reset	

Figure 5-11 VSOM LDAP Configuration

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco VSOM can be configured to enable session timeout and has a minimum session timeout of 30 minutes in the configuration for the version validated. To configure session timeouts navigate to Settings in the Administrator pages and select the Settings Tab.

291604

To secure the authentication information and management of the server, addressing Safeguard 164.308(a)(1)(i) Security Management, 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.

To address the Incident Response and Auditing HIPAA Safeguards identified above, Cisco VSOM can be configured to send its log data to the RSA enVision log management platform. The following configuration script was implemented to send the local log files to the RSA enVision server to be secured and the integrity established:

```
Directory: /etc/cron.daily
Filename: ftp-backup-files.cron
#!/bin/sh
FTP_USER=anonymous
FTP_PASS='vsom@cisco.com'
    localDIR="/usr/BWhttpd/bas/db/backups"
serverDIR="/vsom_backup/"
```

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

As a best practice, 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.

Step 1 In the YaST Control Center window, click **Network Services**, then click **NTP Configuration** in the right panel, as shown in Figure 5-12.



Figure 5-12 Accessing NTP Options

The Advanced NTP Configuration area appears, as shown in Figure 5-13.

Ivanced NTP Configuration	
-Automatically Start NTP Daemon	
O Never	
During Boot	
🔀 Run NTP Daemon in Chroot Jail	
Configure NTP Daemon via DHCP	
Firewall Settings	
Open Port in Firewall Firewall Details	
Firewall is disabled	
Syndromization Type Address	
Add Edjt Deleje	Display Log

Figure 5-13 Advanced NTP Configuration Area

Step 2 Make sure that the During Boot radio button is selected, as shown in Figure 5-14.

Figure 5-14 Choosing the During Boot Radio Button

-Automatically Start NTP Daemon-----Never During Boot

Step 3 Uncheck the Configure NTP Daemon via DHCP check box, as shown in Figure 5-15.

Figure 5-15 Unchecking the Configure NTP Daemon via DHCP Check Box

Run NTP Daemon in Chroot Jail

Step 4 Then click the **Add** button. The New Synchronization area appears, as shown in Figure 5-16.

New Synchroni	zation	
new Synemonia		
	-	
	Туре	
	Server	
	O Peer	
	0.01	
	Radio Clock	
	O Outgoing Broadcast	
	Incoming Broadcast	

Figure 5-16 New Synchronization Area

Step 5 In the New Synchronization area, make sure that the Server radio button is selected, and click Next. The NTP Server panel appears, as shown in Figure 5-17.

Figure 5-17 NTP Server Area

NTP Server		
	Address	
	Address	Salart
		Select.
		Select •
	[Select.
	[Select. •
	[I	Selec -

Step 6

- In the NTP Server area, take these actions:
 - a. In the Address field, enter the IP address or host name of your NTP server.
 - **b.** (Optional) Click **Test** to make sure that the Multi Services Platform can access the NTP server.
 - c. Check the Use for Initial Synchronization check box.
 - d. Click OK.
 - e. When complete, in the Advanced NTP Configuration screen, click Finish.

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications 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 HIPAA safeguards 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 5-18). 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.

Table 5-4 PHI HIPAA Assessment Summary – Cisco Physical Access Control

Models Assessed

Cisco Physical Access Manager version 1.2.0

HIPAA Safeguards Addressed

Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(6)(i) Response and Reporting
	(a)(6)(ii) Security Incident Procedures
Physical	Standards/Implementation Specifications
164.310	(a)(1) Facility Access Controls
HIPAA Standar	ds Failed
No HIPAA star	ndards were failed.
HIPAA Impleme	entation Specifications Failed
No HIPAA imp	plementation specifications were failed.

Table 5-4 PHI HIPAA Assessment Summary—Cisco Physical Access Control (continued)

Primary PHI 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 healthcare ePHI data environment.

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

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the CPAM shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.

- §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
- §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
- §164.310(a)(1) Facility Access Control: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(6)(i) Response and Reporting. Implement policies and procedures to address security incidents. Requirements addressed include: Incident Response and Auditing.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.

Sample Configuration

Cisco PAM is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

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.



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 5-19.)

Figure 5-19 Profiles Module Main Window

Events & Alarms Users Doors Admin Reports	Options Help		
🛿 Edit 📑 Add 📄 Duplicate 🔟 Disabl	e 👘 📄 Repo	ort 🐙 Column:	s 🚔 Filter 🔻
Name	Enabled	Site	1
Administrators	Yes	SanJose	
Administrators Door Monitors System Config Users	Yes	SanJose	
le System Config Users	Yes	SanJose	

<u>Note</u>

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 5-20:
 - Default—A basic set of privileges is set.
 - Most Restrictive—No privileges are set.
 - Least Restrictive—All privileges are set.

Figure 5-20 Profile Templates

🖥 New Profile 🛛 🗙		\mathbf{X}	
Template:	Least restrictive		~
	ОК	Cancel	



Enter the basic profile settings, as shown in Figure 5-21.

-	
🔞 Edit - Profile	
📄 Save and Close 🛛 🔒 Report	
Profile name: Administrators	
Enabled	
Site: SanJose	
General Modules Device Commands Data Types	Allow access to the application
General	Allow issuing device commands
Events/Alarms	Allow access to external hyperlinks
Help	Require device commands to be commented
	Allow editing from right-click menus
	Allow logoff without password

Figure 5-21 Profile—General Tab

- 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 5-5.

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

Field	Description
General	
Allow access to the application	Allows access to the application.
Allow issuing device commands	Allows user to issue device commands directly to hardware.
Allow access to external hyperlinks	Allows access to external hyperlinks.
Require device commands to be commented	Requires the user to enter a comment with each device command issued in the system.
Allow editing from right-click menus	Allows access to the right-click the Edit menu.
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 variou	is 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 5-5 General Settings—Profile Module (continued)

- Step 6 Click the Modules tab to define the modules accessible to the profile, as shown in Figure 5-22.
 - a. Select a Cisco PAM module.
 - **b.** Select **Allow access to module** to enable access to the module.



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 5-22.
- 3. Select the **Device** tab, as shown in Figure 5-23.
- 4. Click Choose.

In the Choose Devices window, expand the Logical Driver device tree and select a door (Figure 5-23).

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

Figure 5-23 Default Filter: Device Settings



Step 7 Click the **Device Commands** tab to define the hardware configuration commands available to the user (see Figure 5-24).



Figure 5-24 Profile—Device Commands Tab

- **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 5-25.

Save and C	lose 👌 Report		
Profile name:	Administrators		
	Enabled		
Site:	SJC		
General Mo	odules Device Commands	Data Types	View
🖃 🧁 Da	ta Types	~	Create
÷ •	Badge		Modify
0	Badge Custom Value 0	=	Delete
•	Badge Custom Value 1		Delete
	Badge Custom Value 2		S
•	Badge Custom Value 3		
•	Badge Custom Value 4		
0	Badge Custom Value 5		
	Badge Custom Value 6		
	Badge Custom Value 7		
	Contact Information		
	 Addresses 		
	🔸 🔶 Email Addresses		
	🔸 🔶 Phone Numbers		
	Department		
	🗠 🔶 Comments		
	🗠 🔶 Name	~	

Figure 5-25 Profile – Data Types Tab

- **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 5-6.

Table 5-6 Profile – Data Types

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

- **Step 9** Click **Save and Close** to save the profile settings.
- **Step 10** Assign the profile to one or more Cisco PAM operators using the Logins module. (See the following section).

Creating User Login Accounts and Assigning Profiles

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

Step 1 Select Logins from the Users menu. The main window (Figure 5-26) lists all the usernames in the system.

vents & Alarms U	sers Doors	Admin Repo	rts Options	Help			
PEdit 📑 Add	💥 Disa	ble 👜 Report	t 🐙 Colur	nns 🐳 Filter 🔻 🔍 Search 👻			
Username	Validity	Effective	Expires	Assigned to	Comments	Site	^
CEO	Active			CEOO, Dr. CEO1		SJC	
cpamadmin	Active					SJC	
gwashington	Active					SJC	
jadams	Active					SJC	_
b tjefferson	Active					SJC	
URL_CDV	Active			URL, Mr. URL_Create_Delete_View-user		SJC	
URL_CV-user	Active			URL, Mr. URL_Create_View_user		SJC	
URL D	Active			URL, Ms. URL Delete-user?NoView		SJC	~
Alarms: 66 act	tive			13 items	cpamadm	nin - SJC	

Figure 5-26 Logins Module Main Window

- **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**.



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

Step 3 Complete fields in the General tab, as shown in Figure 5-27. Table 5-7 describes the field properties.

Figure 5-27 Logins Module – General Tab

	Report	
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



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

Table 5-7 General Tab Fields

Field	Description
Username	Required—The username of the login.
Password	Required—Password to access the system.
Confirm	Required—The value must be entered exactly as it was in the Password field.
password	

Table 5-7	General Tab Fields
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, "Configuring Personnel and Badges" of the CPAM User guide.
Validity	Active or Inactive—Only active accounts can access the system.
Effective	The beginning date the user can log in—If left blank, the user can log in immediately.
Expires	The day the login expires and access is denied—If left blank, access is allowed indefinitely.
Site	Read-only—A site is a single instance of a Cisco PAM database.
Comments	Comments or notes about the login.

- **Step 4** Assign access privileges for the login:
 - a. Select the **Profiles** tab, as shown in Figure 5-28.
 - **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.

<u>P</u> Tip

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

Figure 5-28 Assigning One or More Profiles

Add - Login Save and Close General Profiles	Report Profiles	
- Audit Records	Administrators	egran-wxp04 - Hardware (

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.

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.

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 5-8.

Table 5-8 LDAP System Configuration Settings

Field	Description	
Enable LDAP	Click the checkbox to enable or disable LDAP support.	
LDAP server URL	URL of LDAP server, must begin with ldap://	
	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 5-8	LDAP System Configuration Settings (continued)
	EDAI Oystein Conngalation Cettings (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 5-29, the user principal name is *cpsm.user@ad1.cpamlab*. The Cisco PAM user login must be the same (*cpsm.user*).

Figure 5-29 User Principal LDAP Configuration Example

System Configuration - Cisco Plant	hysical Access Manager	
Events & Alarms Users Doors Admin	Reports Options Help	
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: @ad1.cpamlab Principal prefix: Search root: DC=ad1,DC=cpamlab LDAP version: 3 JNDI authentication type: simple JNDI factory: com.sun.jndi.ldap.LdapCtxFactory	
	cpamadmin	- SanJose

LDAP Example—sAMAccountName

In the example shown in Figure 5-30, the user login is the same as the samaccount name (cpsmuser).

vents & Alarms Users Doors Admin	Reports Options Help	
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	LDAP LDAP server URL: Principal suffix: Principal prefix: Search root: LDAP version: JNDI authentication type: JNDI factory:	Enable LDAP Idap://10.10.82.14:389 CN=Users,DC=ad1,DC=cpamlab CN= CN=Users,DC=ad1,DC=cpamlab 3 simple com.sun.jndi.ldap.LdapCtxFactory

Figure 5-30 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 5-31.)

Figure 5-31 Login Window: LDAP Login Type

General	General		
Profiles Login type:		LDAP	
Recent Events	Username:		
	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.

To secure authentication information and management of the server, addressing Safeguard 164.308(a)(1)(i) Security Management, SSL is enabled by default on the Cisco PAM appliance. 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. The Cisco PAM appliance should also 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:

- 1. SSH into the Cisco PAM server
- 2. sudo su
- 3. Enter the cpamadmin password
- 4. Stop the service: /etc/init.d/cpamadmin stop
- 5. 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" />
```

6. Re-start the service: /etc/init.d/cpamadmin start

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

To address the Incident Response and Auditing HIPAA Safeguards identified above, 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 5-32.)

🔞 Add - Auto	mation Rule]
🔚 Save and C	lose	
	🗹 Enabled	
Name:	Send Audit Reports	
Trigger:	Edit New Clear	
Actions:	Edit Add Move Up Move Down Delete	
	Edit New Clear Record event when rule invoked Record event when trigger fails Record event when action fails Record event when notification fails	

Figure 5-32 Creating a Global I/O with Audit Reports

Step 3 Select **Periodic** and click **OK**. (See Figure 5-33.)

Figure 5-33	Selecting Periodic
🐻 Select Trigge	r Type
Type: Periodic	•
	K Cancel

Step 4 Choose the Interval and enter the Time of Day. Click OK. (See Figure 5-34.)

ĺ	n Periodic	
	Interval: Daily	
	Time of day: 00:00	
	OK Cancel	290970

Selecting Interval and Time of Day

- Step 5 Under Actions, Click Add...

Figure 5-34

Select Report. (See Figure 5-35.) Step 6



ſ	🔞 Sel	ect Action Type	×	
ŀ	Type:	Report	-	
		Report		<u>.</u>
		Device Command		6
L		CSV Import		ାର

Step 7 Choose Audit Records-All and click OK. (See Figure 5-36.)

Figure 5-36 Audit Records-All

G Choose Report	Ŋ
Audit Records - All	
More Cisco Templates Events - All Personnel - Active Schedule(s) - Not Used Audit Records - All Badges - All Access Policy v.cred/valid_type v.cred Badges - Access Policy	
Vx_pnl vx_dev Events - All - Count V _ nviv _sciences OK Cancel	at using

Step 8 Click Save and Close. (See Figure 5-37.)

Figure 5-37 Save and Close

🔞 Add - Report		
🔚 Save :	and Close	
Report:	Audit Records - All	Choose

Under Notification section of the Global I/O, click New and Choose FTP. Click OK. (See Figure 5-38.) Step 9
Figure 5-38 Select Notification Type

FTP Notification

🐻 Sel	ect Notification Type	×	
Type:	E-mail	-	
	E-mail		7
	FTP		g
	Svsloa		ର୍ଷ

Step 10 Enter the FTP Host, Username, Password, and Path. Click OK. (See Figure 5-39.)

FTP Notif	ication
Host:	
Username:	
Password:	
Path:	
	OK Cancel

Figure 5-39

 OK
 Cancel
 K

 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.

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco PAM has a hard-coded session timeout of 30 minutes in the configuration for the version validated.

As a best practice, 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 5-40.





HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Cisco Unified Computing System

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

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

Benefits include the following:

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

Table 5-9 PHI HIPAA Assessment Summary—Cisco UCS

Models Assessed

Cisco UCS Manager version 1.3(1p)

HIPAA Safeguards Addressed

Administrative	Standards/Implementation Specifications			
164.308	(a)(1)(i) Security Management Process			
	(a)(3)(ii)(A) Authorization/Supervision			
	(a)(4)(ii)(A) Isolating Clearing House Functions			
	(a)(4)(ii)(B) Access Authorization			
	(a)(5)(ii)(C) Log-in Monitoring			
	(a)(6)(ii) Response and Reporting			
Technical	Standards/Implementation Specifications			
164.312	(a)(i) Access Control			
	(b) Audit Controls			
	(c)(1) Data Integrity			
HIPAA Standard	s Failed			
No HIPAA stan	dards were failed.			

Table 5-9 PHI HIPAA Assessment Summary – Cisco UCS (continued)

No HIPAA implementation specifications were failed.

HIPAA Implementation Specifications Failed

Primary PHI Function

The primary 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. 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 ePHI systems (in-scope) from other non-sensitive data (out-of-scope).

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.

Г

- 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 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.
- 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

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the Cisco UCS shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
 - §164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a healthcare clearinghouse
 is part of a larger organization, the clearinghouse must implement policies and procedures that
 protect the electronic protected health information of the clearinghouse from unauthorized
 access by the larger organization. Requirements addressed include: Access Control, Integrity,
 Incident Response and Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
 - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4). Requirements addressed include: Access Control and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.

- \$164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
- §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4). Requirements addressed include: Access Control and Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - \$164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(6)(i) Response and Reporting. Implement policies and procedures to address security incidents. Requirements addressed include: Incident Response and Auditing.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
 - \$164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.

Sample Configuration

Cisco UCS servers are able to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership. Cisco UCS includes extensive controls for defining user privileges and by default denies access to all individuals without a system user ID.

Add the Cisco Secure ACS server under the TACACS+ protocol option, as shown in Figure 5-41.

L

🛕 Cisco Unified Computing System Manager - DC	-UCSFabric				□ X
Fault Summary Image: Constraint of the second	Image: Second secon			Ç.	alialio cisco TACACS+
Equipment Servers LAN SAN VM Admin Filter: Al Filter: Al Filter: Al Faults, Events and Audit Log Core Files Faults Settings Syslog User Management LOAP Communication LOAP Faults Coceles Communication Management Communication Services Dis Management Communication Services Communication Services Collection Policy adapter Collection Policy adapter Collection Policy adapter Collection Policy adapter	General Events FSM	Properties Timeout: 5	 Port 49		
S Collection Policy host S Collection Policy port Collection Policy server			Save Cha	nges Reset	t Values
B Logged in as bmcgloth@ucsmanager.cisco-irn			System Tir	me: 2011-06-03T1	5:50

Figure 5-41 Adding the Cisco Secure ACS Server

Select **tacacs** from the Console and Default dropdown menus on the Authorization page, as shown in Figure 5-42.

Figure 5-42 Authorization—Selecting Console and Default Settings

ault Summary	. 1	🕒 🕘 🗳 New 👻 🖌 Options 🛛 🚱 🕕 🔯 Exit	alialia cisco
		>> ∰ All ► All ► Authorization	Authorization
quipment Servers LAN SAN VM	Admin	General Events FSM	
Filter: All	-	Console: tacacs	
		Default: tacacs	
Events	*	Role Policy For Remote Users: no-login assign-default-role States	
		Sacs	
Syslog			
Authorization			
- ADIUS			
TACACS+ Gervices			

On the TACACS+ server, create custom attributes defining the desired role for the user or group accessing the Cisco UCS Manager (see Figure 5-43):

• 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"



Local individual user accounts can be 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 established policies for passwords.

To secure authentication information and management of the UCS Manager, addressing Safeguard 164.308(a)(1)(i) Security Management, the Cisco UCS allows for the disabling of non-secure administrative interfaces. Figure 5-44 shows that the secure management protocols of SSH and HTTPS for administration. Telnet, HTTP, and other unused protocols are disabled.



Figure 5-44 Secure Management Protocols

Cisco UCS uses strong encryption for SSH and HTTPS connections. Encryption keys are created and managed under the Key Management feature. (See Figure 5-45.)

Cisco Unified Computing System Manager - DC	-UCSFabric		
ult Summary	🗄 😋 🍥 🖪 New 👻 🎴 Options		
0 15 9 4	>> 👸 All + 🔑 Key Management	heyRing default	🔑 KeyRing defau
upment Servers LAN SAN VM Admin	General Events		
Filter: All	Actions	Properties	3
	Create Certificate Request		
Authorization		Request	8
ADIUS		Certificate	8
Locales			
Eccally Authenticated Users			
🔏 bmcgloth			
Chjanoff			
Remotely Authenticated Users Brogloth			
Roles			
- P Key Management			
🖻 🖥 Communication Management			
Call Home			

Figure 5-45 1024-Bit Mod Key Default Keyring

To address the Incident Response and Auditing HIPAA Safeguards identified above, Cisco UCS can be configured to send its data to the RSA enVision log management platform using the syslog function and/or SNMP traps. In the solution, only syslog was used. (SeeFigure 5-46).

Figure 5-46 Using Syslog

Fault Summary Image: Severe S LAN SAM of Malen File: All Image: Severe S LAN SAM of Malen File: All Image: Severe S LAN SAM of Malen File: All Image: Severe S LAN SAM of Malen File: All Image: Severe S LAN SAM of Malen File: Adden State: Image: Severe S LAN Same: Severe S LA	🚖 Cisco Unified Computing System Manager - DC-U	JCSFabric	
0 15 9 4 Construction System System System Filter, A Image: A system System System 0 Image: A system Image: A system Image: A system 0 Image: A system Image: A system Image: A system 0 Image: A system Image: A system Image: A system 0 Image: A system Image: A system Image: A system 0 Image: A system Image: A system Image: A system 0 Image: A system Image: A system Image: A system 0 Image: A system Image: A system Image: A system 0 Image: A system Image: A system Image: A system 0 Image: A system Image: A system Image: A system 0 Image: A system Image	Fault Summary		dubb
is 9 4 EadJoint Server: LAN: Stall. MM Admin Filter: Admin Stall: Imabled I diabled Imabe: Imable: Imable: Imable: Imable: Imable: Imable: Imable: Imable: Imable: Imable: Imable: Imable: Imable: Imable: Imable: <		🗄 🌍 🛄 New 📲 🛃 Options 🛛 😗 🕕 🔟 Exit	cisco
System System Filter Advin M System System System System <t< td=""><td>• ·</td><td>>> 🛱 All > 🗸 Faults, Events and Audit Log > 🗸 Syslog</td><td>🗸 Syslog</td></t<>	• ·	>> 🛱 All > 🗸 Faults, Events and Audit Log > 🗸 Syslog	🗸 Syslog
Educement Lifewider Lifewi	0 15 9 4		TT Class
Image: Transfer A Image: Transfer A <td>Equipment Servers LAN SAN VM Admin</td> <td>Syslog</td> <td></td>	Equipment Servers LAN SAN VM Admin	Syslog	
Image: Server 1 Image: Server 2 Image		Local Destinations	Remote Destinations
dom State: enabled dom State: <t< td=""><td>Filter: All</td><td>Course la</td><td>6</td></t<>	Filter: All	Course la	6
Autoritude Construction Autoritude Construction Autoritude Admin State: Orabled deabled d	± =	Console	Server 1
Autoritude Construction Autoritude Construction Autoritude Admin State: Orabled deabled d		Admin State: enabled e disabled	Admin State: @ enabled () disabled
Concerting Concerting <td></td> <td></td> <td></td>			
Control of the set of the se			Level: information
Faults Strings Deer Management Admin State: IDAP Admin State: IDAP Admin State: IDAP IDAP IDAP <td></td> <td>Monitor</td> <td>Hostname (or IP Address): 192.168.42.124</td>		Monitor	Hostname (or IP Address): 192.168.42.124
Bettage Bettagetage Bettage Bettage Bettage Bettage Bettage		Admin State: (a) enabled (c) disabled	Fadility: local7
Usere Interface Usere Interface Interface I			
Uer Management Authorization Loa? RADUS RACKS+ Loades Loades Loades Remotely Authenticated Users Remotely Authentited Re		Level: information	Server 2
File Admin State: PADBUS PADBUS TACACS+ Locals Locals Locals Locals Size (G): 194304 Particle Padbus Control Name: messages Size (G): Padbus Communication Naragement Padbus Padbus Padbus Padbus Size (G): Padbus Size (G): Padbus Padbus Padbus Padbus Size (G): Padbus Padbus Padbus Padbus Size (G): Padbus <			
Admin State: Ad	Authorization	File	Admin State: O enabled O disabled
Adduss Level: Ider Services Locales Size (v3): Hydroids Remotely Authenticated Users Remotely Authenticated Users Remotely Authenticated Users Size (v3): Hydroids Communication Services Communication Poly adapter State Management State Management State Management So Collection Poly dapter So Collection Poly dapter So Collection Poly states Collection Poly states Collection Poly states State Management Collection Poly states Collection Poly states <		A duris Shatay (0, anablad (0, disablad	
Ider Services Isolals		Aumin State: Cenapled O disabled	
Name: messages Size (K6): 4194304 Admin State: enabled Management KeyKing default Comunication Management For Comunication Services DVS Management Proof (ext mgnt) Management 1P Pool (ext mgnt) <		Level: information	Common 2
Reverse in the second services State Management Key Management Key Management Key Management Communication Management Management IP Pol (ext-mgmt) Management IP fol (ext-mgmt) Management IP fol (ext-mgmt) Management State Management State Management Solution Policy adapter Solution Policy sever Solution Policy sever Solution Policy sever Solution Policy sever Solution Policy default Abd-Organizations Timezone Management Solution Policy adapter Solution Policy adapter Solution Policy adapter Solution Policy sever Solution Policy adapter	Services	Name: messages	Server J
Render Authenticated Users Roles Roles Ker Management Ker Management Ker Management Ker Management Communication Nanagement Rome Stats Management Stats Management Stats Management Stats Management Stats Management Solicition Policy adapter Solicition Policy adapter Solicition Policy server Solicition Policy default Aid-Organizations Soli	Locally Authenticated Users	Size (/P): 4104204	Admin State: o enabled o disabled
Key Kanagement Key King default Communication Management Colal Home Management Pool (ext-mgmt) Management Interfaces Stats Monagement Monagement <td>Remotely Authenticated Users</td> <td>3/2E (ND). 1191301</td> <td></td>	Remotely Authenticated Users	3/2E (ND). 1191301	
Ceylang default Call Home Communication Management Coll Home Communication Services Coll Komagement Management IP Pool (ext mgmt) Management IP Fool (ext mgmt) Management IP Fool (ext mgmt) Stats Management Stats Poloes Stats Poloes So Collection Policy dapter So Collection Policy host So Collection Policy So Collection			
Communication Management Communication Services Communication Services DNS Management Prool (ext-mgmt) Management Interfaces Stats Polices Stats Polices Stats Policy datast Stats Policy datast Stats Policy host State Didexton Policy host State Collection Policy port State Collection Policy assis State Collection Policy host State Collection Policy port State Collection Policy and the Collection Policy host State Collection Policy host			
Comunication Services DNS Management IP Pool (extremut) Management IP Frod (extremut) Stats Management Stats Management Stats Nanagement Stats Polices Solection Policy adapter Solection Policy hassis Solection Policy hassis Solection Policy hassis Solection Policy hassis Solection Policy hassis Solection Policy for the Solection Policy default Autor Thermone Management Consistence Adapters Adapters Colestion Services Management I Produce International I			
Comunication Services Communication Services Communications Communica			
Monagement IP Pool (ext-mgmt) Management IP for (ext-mgmt) Management IN fraces Stats Management Stats Policies Solicition Policy adapter Solicition Policy hassis Solicition Policy hassis Solicition Policy port Solicition Policy server fabric fabri			
Amagement Interfaces Stats Management Stats Policies Stats Policies <td< td=""><td></td><td></td><td></td></td<>			
Stats Management Stats Policies Stats Policies Solection Policy adapter Solection Policy host Solection Policy port Solection Policy port Solection Policy server Solection Policy server Solection Policy cont Solection Policy adapter	Management IP Pool (ext-mgmt)		
Collection Policy adapter Collection Policy adapter Collection Policy adapter Collection Policy port Collection Policy port Collection Policy port Collection Policy adapter Collection Policy adapter Col			
S Collection Policy adapter S Collection Policy hassis Collection Policy hassis Collection Policy port Collection Policy server Thermal LAN Collection Policy server Thermal LAN Collection Policy adapter S Collection Policy adapter Collection Policy adapter S Collection Policy port S Collection Policy po			
S Calection Policy chasss S Calection Policy host Collection Policy port Collection Policy server Thermal LAN Collection Policy server Thermal LAN Collection Policy server Thermal LAN Collection Policy server Thermal LAN Collection Policy fault Collection Policy and the server Collection Policy and			
S Calection Policy host S Calection Policy server Calection Policy host Calection Policy host			
Solection Policy pert Solection Policy server Internal LAN Collection Policy server Internal LAN Collection Policy server Internal LAN Solection Solection Solection Policy server Internal LAN Solection Policy server Solection Policy s			
Internal AN Internal AN DAN Cloud SAN Cloud Solv-Organizations Timezone Management Coubling Content of the conte			
Consistence Consistence Construction			
Copyling Catalog A chosis			
A root Sub-Organizations A Sub-Organizations Capability Catalog A Adopters CPUs A Adopters CPUs A Chasis			
Sub-Organizations Sub-Organizations Capability Catalog Adapters Adapters Adapters Achassis			
A sub-Organizations Graditly Catalog Adopters Adopte			
Immit Timezone Management Immit Construction Immit Construction Immit Construction Immit Construction			
Capability Catalog Adapters Adapters Adapters Capability Catalog Capabi			
- X Adotes - X CPUs - X Chasis			
-X CPUs ····································			
-X Chassis			
		· · · · · · · · · · · · · · · · · · ·	Þ
			Save Changes Reset Values
		L	Sure Granges Acset values
A Logged in as bmcgloth@ucsmanager.disco+m	A Logged in as bmcgloth@ucsmanager.cisco-irn		System Time: 2011-06-03T15:53

As a best practice, NTP is used to synchronize clocks among network devices (see Figure 5-47). 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.



Figure 5-47 NTP Screen

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Cisco UCS Express on Services Ready Engine

......

The Cisco Unified Computing System (UCS) Express and Services Ready Engine (SRE) is designed to allow 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 clinic 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 clinic 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.

lable 5-10	PHI HIPAA Assessment Summary—Cisco UCS Express	

Models Assess	ed				
Cisco UCS Exp	press version 1.1 on SRE900				
HIPAA Safegua	rds Addressed				
Administrative	Standards/Implementation Specifications				
164.308	(a)(1)(i) Security Management Process				
	(a)(3)(ii)(A) Authorization/Supervision				
	(a)(4)(ii)(A) Isolating Clearing House Functions				
	(a)(4)(i) Access Authorization				
	(a)(5)(i) Log-in Monitoring				
	(a)(6)(i) Security Incident Procedures				
	(a)(6)(ii) Response and Reporting				
Technical	Standards/Implementation Specifications				
164.312	(a)(i) Access Control				
	(b) Audit Controls				
	(c)(1) Data Integrity				
HIPAA Standard	ls Failed				
No HIPAA stan	dards were failed.				
HIPAA Impleme	ntation Specifications Failed				
No HIPAA imp	lementation specifications were failed.				

Primary PHI Function

The primary 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. 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 sensitive ePHI (in-scope) from other non-sensitive data (out-of-scope).

Design Considerations

The major consideration when using Cisco UCS Express with sensitive applications is the security of the hypervisor. Verizon considers all hypervisors to be insecure because of vulnerabilities that may exist resulting in data leakage between VMs. Therefore, use separate Cisco UCS Express implementations when scoping. Although it is acceptable to mix non-sensitive applications onto a Cisco UCS Express deployment with sensitive applications, doing so brings those applications into scope and audit. (See Figure 5-48.)



Figure 5-48 Using UCS Express with Cisco SRE



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 clinic, this may require the use of bridged virtual interfaces.
- Cisco UCS Express is based on VMware's ESXi and uses vSphere client for management.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the UCS Express shown below were used to meet the following list of satisfied controls:

• Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards

<u>Note</u>

- §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
- §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
- §164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a healthcare clearinghouse
 is part of a larger organization, the clearinghouse must implement policies and procedures that
 protect the electronic protected health information of the clearinghouse from unauthorized
 access by the larger organization. Requirements addressed include: Access Control, Integrity,
 Incident Response and Auditing.
- §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
- §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4). Requirements addressed include: Access Control and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical Safeguards.
 - \$164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.
 - \$164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
 - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4). Requirements addressed include: Access Control and Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - \$164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - \$164.308(a)(6)(i) Response and Reporting. Implement policies and procedures to address security incidents. Requirements addressed include: Incident Response and Auditing.

- §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.

Sample Configuration

Cisco UCS servers are able to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership. Cisco UCS Express includes extensive controls for defining user privileges and by default denies access to all individuals without a system user ID. On the UCS server configuration of the ESX hypervisor is part of the vSphere and vCenter infrastructure.

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 established policies for passwords.

To secure authentication information and management of the UCS server, addressing Safeguard 164.308(a)(1)(i) Security Management, the UCS management console supports only HTTPS and SSH access.

Cisco UCS Express is designed to track and monitor all administrative user access, events such as profile creation, interface up/down, and device authentications. All of these events are sent to the vSphere and vCenter infrastructure.

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
lime Configuration	
General	
Date & Time	21:28 6/23/2011
NTP Client	Running
NTP Servers	192.168.62.161, 192.168.62.162

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications 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

Table 5-11 PHI HIPAA Assessment Summary—Cisco ACS

Models Assessed		
Cisco Secure Access Control Server	Release 4.2(1) Build 15 Patch 3	
HIPAA Safeguards Addressed		

Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(ii)(A) Authorization/Supervision
	(a)(3)(ii)(C) Termination Procedures
	(a)(4)(ii)(B) Access Authorization
	(a)(4)(ii)(C) Access Establishment and Modification
	(a)(5)(ii)(C) Log-in Monitoring
	(a)(6)(ii) Response and Reporting
Technical	Standards/Implementation Specifications
164.312	(a)(2)(i) Unique User Identification
	(a)(2)(ii) Emergency Access Procedures
	(a)(2)(ii) Automatic Logoff
	(b) Audit Controls
	(d) Person or Entity Authentication
HIPAA Standards	Failed
No HIPAA stand	ards were failed.
HIPAA Implemen	tation Specifications Failed
No HIPAA imple	ementation specifications were failed.

Table 5-11	PHI HIPAA .	Assessment	Summary	v—Cisco	ACS
------------	-------------	------------	---------	---------	-----

Primary PHI Function

The primary function of Cisco Secure ACS is to securely authenticate users to the systems within the ePHI environment. The ACS allows for management of user access (authorization) to systems containing ePHI. Additionally, the ACS can prevent unauthorized devices from accessing systems containing ePHI and protect access from unauthorized locations. Users can be assigned to groups and, based on privilege levels, have access to only the information they require for their job function.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

HIPAA safeguards are spread across multiple categories. ACS allows healthcare-covered entities and business associates to meet access control safeguards in the Administrative and Technical categories. The access control can be applied to both internal and external users that access ePHI data.

All of the sample configurations of the ACS shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - \$164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations it might be accessed. Requirements addressed include: Access Control and Auditing.

- §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
- §164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Requirements addressed include: Access Control, Incident Response, and Auditing.
- \$164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- §164.312(a)(2)(ii) Automatic logoff. Implement electronic procedures that terminate an
 electronic session after a predetermined time of inactivity. Requirements addressed include:
 Access Control.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
 - §164.312(a)(2)(i) Unique User Identification. Assign a unique name and/or number for identifying and tracking user identity. Requirements addressed include: Access Control and Auditing.
 - §164.312(a)(2)(ii) Emergency Access Procedures. Establish (and implement as necessary) procedures for obtaining necessary ePHI during an emergency. Requirements addressed include: Access Control.
 - §164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical Safeguards.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.

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 HIPAA 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.

L

User authentication services for Cisco Secure ACS are linked to a centralized Active Directory user database. When personnel are added or removed from Active Directory, their access to infrastructure is similarly affected addressing Safeguard 164.308(a)(3)(ii)(C) Termination Procedures.

Sample Configuration

Cisco ACS is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through Cisco ACS and ISE via LDAP, RADIUS, and TACACS+ services enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

Cisco Secure ACS supports the creation of local administrative users. Each user must be assigned a unique ID. Cisco Secure ACS password policy enables setting of an inactivity option where an administrator is locked out after a specified period of inactivity determined by company policies. Local administrator user accounts in Cisco Secure ACS require the setting of a password according to the password requirements, as shown in Figure 5-50. By default, Cisco Secure ACS requires another administrator to re-enable locked out accounts.



Figure 5-50 Administrator Password Requirements

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco Secure ACS supports session policies under the Administration Control/Session tab. The default session timeout is 60 minutes. It is a best practice to change the session timeout to 15 minutes, as shown in Figure 5-51.



Figure 5-51 Session Timeout

To address the Incident Response and Auditing HIPAA Safeguards identified above, Cisco Secure ACS can be configured to send its log data to the RSA enVision log management platform. 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 5-52 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.

Γ

irefox 🔻		
CiscoSecure ACS	+	
-)-> 👩 cisco-irn	.com https://tacacs.cisco-irn.com:2005/index2.htm	🚖 + C Scogle 🔎 🏫 Feedback •
Most Visited 🐝 Ciso	o UCS Manager 📄 UIM 📄 NCM 📄 WCS 👩 TACACS 🧭 RSA enVision 📄 HyTrust 🚟 CM-2 📄	RSA-AM 👑 VSOM 🚾 RSA-KMA 🚾 RSA Access Manager: 💽 Bookmark
	Administration Control	X
cisco		
User Setup Group Setup	Administrator Password Policy Setup	Dassword Validation Options Dassword Unit Unitime Options Password Inactivity Options Incorrect Password Attempt Options
Shared Profile Components	Password Validation Options	Use this page to configure the Administrator password policy.
-I Network	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.
System Configuration	Minimum length 7 characters	 Minimum Length - Enter a value between 4 and 20 for the password length. The default length is 4. Password must contain: - Use these options to determine the password complexity
Configuration		constraints.
Administration	Password must contain:	 Uppercase alphabetic characters - If enabled, the password must contain uppercase alphabetic characters.
	Iower case alphabetic characters	 Lowercase alphabetic characters - If enabled, the password must contain lowercase alphabetic characters.
External User 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
) 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 th last time the password was changed.
	Password Lifetime Options	 The password will require change after (x) days - Following a change of password, if enabled, x specifies the number of days before ACS requires a
		change of password due to password age (default = 30). The range is 1 to 365.
	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 ?	Password inactivity updons Following last account activity - Use these options to place restrictions on the use of
		inactive administrator accounts. The value in represents the number of days that passed since the activity (administrator login).
	Following last account activity:	
	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.
		 The Administrator will be locked out after (X) days - Following a change of password, if enabled, x specifies the number of days before ACS locks out
	Incorrect Password Attempt Options	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
		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	[Back to Top]

Figure 5-52 Syslog for Passed Authentications

To secure authentication information and management of the ACS server, addressing Safeguard 164.308(a)(1)(i) Security Management, the ACS 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 5-53). Cisco Secure ACS employs port hopping to a random high port for secured communication transport.

Figure 5-53 HTTP Configuration

HTTP Configuration ?	
HTTP Port Allocation	
\circ Allow any TCP ports to be used for Administration HTTP $_{\rm Access}$	
 Restrict Administration Sessions to the following port range From Port 2002 to Port 2009 	
Secure Socket Layer Setup	la
☑ Use HTTPS Transport for Administration Access	ŭ 8

As a best practice, 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. 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 implementation of Cisco ACS was Windows-based.

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications 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). As the management component, RSA Authentication Manager is used to verify authentication requests and centrally administer authentication policies for enterprise networks.

Table 5-12	PHI HIPAA Assessment Summary—Cisco RSA Authentication Manager
------------	---

Models Assessed	
RSA Authenticat	ion Manager 7.1 Service Pack 2
HIPAA Safeguard	s Addressed
Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
	(a)(6)(ii) Response and Reporting
Technical	Standards/Implementation Specifications
164.312	(a)(i) Access Control
	(b) Audit Controls
	(c)(1) Data Integrity
HIPAA Standards	Failed
No HIPAA standa	ards were failed.
HIPAA Implement	ation Specifications Failed
No HIPAA imple	mentation specifications were failed.

Primary PHI Function

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

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/).

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the RSA Authentication Manager shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
 - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(6)(i) Security Incident Procedures. Implement policies and procedures to address security incidents.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.

- §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.

Sample Configuration

RSA Authentication Manager has powerful access control capabilities to limit, track, and monitor all user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. RSA Authentication Manager protects epHI data based on user role or group membership. Users and groups are created under the Identity tab of the Security console, as shown in Figure 5-54.

Figure 5-54 Users and Groups

dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u>							
🔹 🕥 👻 😰 🏠 🔎 Sear							
https://rsa-am.cisco-irn.com:70	04/cons	ole-ims/ListUser.do					🗾 🔁 Go 🛛 Li
A Security Cons	ole			Logged o	n as: bmcglo	oth <u>My Permissions</u> <u>N</u> Realm: SystemE	<u>1y Preferences</u> Log Ol Domain <u>Configuratio</u>
Identity - Authentication -	Acce	ss 🔻 Reporting 👻 RADIUS 👻 Ad	Iministration 🔻 Setup 💌	Help 🔻			
Users V							elp on this page *
User Groups	2						eip on this page
A Identity Attribute Definitions	stem w	th a unique account within this realm.					
	4 fo	und. Showing 1-4.					
Search	0 se	lected: Add to User Groups	Go ≥			:	5how 250 💌 per page
Security Domain: SystemDomain +		User ID	Last, First Name	Disabled	Locked	Security Domain	Identity Source
Identity Source:		🍙 bart 🗸	mcglothin, bart			ং≣্ত SystemDomain	Internal Database
Internal Database 💌		🔐 bmcgloth 👻	McGlothin, Bart			°ল্⊒ SystemDomain	Internal Database
For:		🔐 chjanoff 👻	janoff, Christian			ैर्ह्न SystemDomain	Internal Database
Where:		SelfServiceAdmin_zw44oqry 🗸	Administrator, Self-Service	~		°ল্≓ SystemDomain	Internal Database
User ID		User ID	Last, First Name	Disabled	Locked	Security Domain	Identity Source
starts with	0 sel	ected: Add to User Groups	Go D		1		5how 250 💌 per page
More criteria	4 fo	und. Showing 1-4.					
Search		-					
Advanced Search							
Advanced Search							
		Copyright ©2007 - 200	8 RSA Security Inc. All rights r	eserved.			

Local individual user accounts are configured in the event that the centralized authentication server cannot be reached, and support advanced policies regarding password rotation and expiration as can be configured as necessary. 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:7004 🛐	/console-ims/AddUser.do?action=r	vPreAdd&ptoken=UVS7O2ZDZKECDDO6
	Last Name:	K	
	User ID:	k	
	Email:		
	i Certificate DN:		
	Notes:		A ¥
	Password		
	i Password:	•	What's a valid password?
	Confirm Password:	•	Your password must contain:
	i Force Password Change:	Require user to change pas	characters
	Account Information		 At least 1 numeric characters At least 1 special characters Not allowed: @~
	i Account Starts:	June 🔹 17 💌 2011	You may not re-use one of your last 5
	1 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.
	i Locked Status:	☐ Account is locked by lockout ☐ Account is locked out of eme	

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.

🔹 🕤 👻 📓 🐔 🔑 Search 👷 Favo		-												6	
https://rsa-am.cisco-irn.com:7004/console-ar	/ListAssign	edToken.do?pageaction=nv	/PreSearchAl	BitokenCatego	ry=assignedi	Bptoken=EKK	J6OA4E835CIBC)							Go L
Security Console										Lo	gged in as: I	omcgloth <u>My Pe</u> Rea		<u>My Preferences</u> nDomain <u>Co</u>	
e Identity • Authentication • Access •	Reportin	g 🔻 🛛 RADIUS 👻 🛛 Admir	nistration 🔻	Setup 🔻	Help 🔻										
SecurID Tokens Import	ecurID T	okens ව	_										i	Help on this page	e *
Assigned Unassigned															
Hardware or software-based security tokens the	t have bee	n assigned to users manage	d in this reali	n.											
Security Domain:	2 fo	und. Showing 1-2.													
SystemDomain -	0 s	elected: Unassign			• Go	Σ								Show 250 -	ner nane
For:		Serial Number	Token	Algorithm			Enabled For	Requires	Pending	Will	CT-KIP	Last Used To	Expires	Security	Notes
All Assigned Tokens	• •	<u>Performaniaer</u>	Type	<u>Angoricum</u>	To	UISUULU	Emergency	Passcode	Replacement By Token	Replace Token	Capable	Authenticate	On	Domain	tiotes
Where:							Access		by token	TOKEN					
Serial Number starts with		000115335607 👻	Standard Card	AES-TIME	bricgloth			~				3/9/11 1:18:58 PM PST	12/31/11 12:00:00	SystemDomain	
Istarts with			Card									record.	AM PST		
More criteria		000115400388 🗸	Software	AES-TIME	bart			~			~		12/31/11 12:00:00	SystemDomain	
Search													AM PST		
Search Z		Serial Number	<u>Token</u> Type	<u>Algorithm</u>	<u>Assigned</u> <u>To</u>	Disabled	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> <u>Capable</u>	<u>Last Used To</u> Authenticate	<u>Expires</u> On	<u>Security</u> Domain	Notes
	0 se	ected: Unassign	-		• Go	2					1		1	Show 250 -	Der Dage
	26	und. Showing 1-2.													
	2.15	and showing r Er					Inc. All rights res								

Figure 5-56 Assigned Tokens

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. 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 5-57.

Figure 5-57	Session Lifetime for Console
-------------	------------------------------

RSA Security Console: - Edit Session	n Lifetime - Microsoft Internet Explorer	
e Edit View Favorites Iools E	Help	
i Back 🝷 🕘 👻 👔 🐔 🔎 Sea	arch 📩 Favorites 🙆 🚽 😓 🗔	
dress 🙆 https://rsa-am.cisco-irn.com:71	004/console-ims/AddSessionManagement.do?action=nvPreEdit&guid=ims.000000000000000000000000000000000000	inks »
RSA Security Con	Logged on as: bmcgloth My Permissions My Preferences Log Ol SOIE Realm: SystemDomain Configuration	
Home Identity Authentication	Access ▼ Reporting ▼ RADIUS ▼ Administration ▼ Setup ▼ Help ▼	
Session Lifetime: C	Console/Command API Session Li 🔻 🚺 Help on this page *	
Edit		
Session lifetimes define session du Cancel 🔀 Reset	urations. They are assigned to resources to limit sessions times for users who access those resources.	
	* Required field	
Session Lifetime Basics		
i Session Lifetime Name:	* Console/Command API Session Lifetime	
1 Time-out:	✓ Time out idle sessions Close idle sessions after 15 minutes ▼ of inactivity	
Maximum Lifetime:	Imit session lifetime Close sessions after 8 hours ▼	
i System Default:	□ Set as the default session lifetime for all resources	
Notes:	The authenticated session lifetime.	
Cancel 🗙 Reset		
	Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.	
		1
one	📄 📄 🖉 Trusted sites	

To secure authentication information and management of the server, addressing Safeguard 164.308(a)(1)(i) Security Management, the management console supports only HTTPS access by default.

To address the Incident Response and Auditing HIPAA Safeguards identified above, RSA Authentication Manager can be configured to send its log data to the RSA enVision log management. 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 5-58.





As a best practice, 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. 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 implementation was Windows-based.

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Cisco Identity Services Engine

The Cisco Identity Services Engine (ISE) allows for management of user access (authorization) to systems containing PHI. Additionally, the Access Control Server is designed to prevent unauthorized devices from accessing systems containing PHI and protect access from unauthorized locations. ISE is a security component that 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 allow you to see 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 5-59 shows an example of a Cisco ISE-based LAN deployment.

L

Device 560000

Figure 5-59 Cisco ISE-Based LAN Deployment

Table 5-13 PHI HIPAA Assessment Summary—Cisco ISE

Models Assessed	
Cisco Identity Ser	vice Engine version 1.0.3.377
HIPAA Safeguards	Addressed
Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(ii)(A) Authorization/Supervision
	(a)(4)(ii)(A) Isolating Clearing House Functions
	(a)(4)(ii)(B) Access Authorization
	(a)(4)(ii)(C) Access Est./Modification
	(a)(5)(ii)(C) Log-in Monitoring
	(a)(5)(ii)(D) Password Management
	(a)(6)(i) Security Incident Procedures
	(a)(6)(ii) Response and Reporting
Technical	Standards/Implementation Specifications
164.312	(a)(i) Access Control
	(b) Audit Controls
	(a)(2)(ii) Emergency Access Procedures
	(a)(d) Personal Entity Authentication
HIPAA Standards F	ailed
No HIPAA standa	rds were failed.
HIPAA Implementa	tion Specifications Failed

No HIPAA implementation specifications were failed.

Primary PHI Function

Cisco ISE identity features are designed to detect and prevent rogue wireless devices from connecting to in-scope PHI networks; in addition, Cisco ISE locks down publicly accessible network ports to only authorized devices and users.

The Identity Services Engine allows for management of user access (authorization) to systems containing PHI. Additionally, the Access Control Server can prevent unauthorized devices from accessing systems containing PHI and protect access from unauthorized locations.

Identity Services Engine logs can be used to identify unauthorized attempts to connect to systems containing PHI to help meet the supervision requirements.

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 HIPAA 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 HIPAA 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 HIPAA segmentation of a network. For example, members of the HIPAA active directory group are automatically moved to the HIPAA 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 PHI data environment.
- 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 HIPAA.

HIPAA Assessment Detail—HIPAA Safeguards Passed

All of the sample configurations of the Cisco ISE shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.

- §164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a healthcare clearinghouse
 is part of a larger organization, the clearinghouse must implement policies and procedures that
 protect the electronic protected health information of the clearinghouse from unauthorized
 access by the larger organization. Requirements addressed include: Access Control, Integrity,
 Incident Response, and Auditing.
- §164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Requirements addressed include: Access Control, Incident Response, and Auditing.
- §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- §164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.
- §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
 - §164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.

Sample Configuration

Cisco ISE is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via

LDAP and RADIUS services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

Figure 5-60 shows admin authentication configured to use Active Directory.

Figure 5-60 Admin Access Using Active Directory for Authentication

N	Maintenance Backup & Restore Admin Access	Settings	
	Authentication Method Password Policy		
Aut	thentication Type		
۲	Password Based	* Identity Source AD:AD1 *	
0	Client Certificate Based		293332

Cisco ISE entrols access so that only privileged users can access the ePHI environment. 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 for proper configuration.

Figure 5-61 shows the Authorization Profiles screen.

Dictionaries Conditions Results		
Results	Authorization Profiles > PCI_in_S	Scope
(م •	* Name PCI_in_Scope	e
¢- ≡ ≡ ⊗-	Description For Hosts Tha	at Need Access To PCI CDE
🛪 🚞 Authentication		
Allowed Protocols	* Access Type ACCESS_AC	CEPT
Default Network Access		
🛪 🚞 Authorization		
Authorization Profiles	▼ Common Tasks	
Cisco_IP_Phones	Common Tasks	
OenyAccess	DACL Name	PERMIT ALL TRAFFIC
PCI_in_Scope	E DAOL Name	
PermitAccess	E VLAN	1:POS
Downloadable ACLs	Voice Domain Permission	
Inline Posture Node Profiles	Voice Domain Permission	
Profiling	Posture Discovery	
Posture	Controlized Mah Authentiest	Non
Client Provisioning	Centralized Web Authenticat	
Security Group Access	Auto Smart Port	dot1x

Figure 5-61 Authorization Profiles

If Cisco ISE does not explicitly match an authorization policy as shown in Figure 5-62, network access is denied.

Authentication	Authorization	Refiling	Posture	Client Provisioning	Security Group	Access	Policy Eler	nents
efine the Authoriza	tion Policy by configu	iring rules based of	on identity gro	oups and/or other condition	S			
First Matched Rule	Annlies							
Exceptions Standard								
Exceptions Standard	Name	Identit	y Groups	Other Conditions		Pe	rmissions	
Exceptions Standard Status Rule				Other Conditions and Condition(s)			rmissions Cisco_IP_Pho	4
Exceptions Standard Status Rule	Name		o-IP ⇔			then (\$ \$

Figure 5-62 Authorization Policy

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 established policies for passwords. The passwords used for these accounts can be tailored by editing of the Password Policy to match corporate requirements as shown in Figure 5-63.

Figure 5-63 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
Vumeric characters
✓ Non-alphanumeric characters
Password History
Password must be different from the previous 5 versions [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) ^ Disable account
Email remediation message ^
This account has been locked. For this account to become unlocked, please contact your IT helpdesk.
Save Reset

293334

203335

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco ISE supports session idle timeout under the Administration Access/Session tab. It is a best practice to change the session timeout to 15 minutes, as shown in Figure 5-64, which will re-authenticate both admin users and RADIUS users.

Feed Service 🔆 System 💯 Identity Management Network Resources 🛃 Web Portal Management Deployment Licensing Certificates Logging Maintenance Backup & Restore Admin Access Settings sion Timeout Session Info Admin Access Q * Session Idle Timeout 10 minutes (Valid Range 6 to 100) 103-. E Authentication Authorization Administrators Settings

Figure 5-64 Admin Access

E Access

E Session

To secure authentication information and management of the ISE server, addressing Safeguard 164.308(a)(1)(i) Security Management, the ISE management console supports only HTTPS access.

Additionally, Cisco ISE NAC capabilities can be configured on the clinic and hospital 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, adding 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 switch port that could potentially let a host find its way to the ePHI 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
1
   ---Configurations to add for NAC ----
1
!
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
Т
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
```

L

```
radius-server host 192.168.42.111 auth-port 1812 acct-port 1813 key 7 <removed>
radius-server vsa send accounting
radius-server vsa send authentication
authentication mac-move permit
1
1
ip device tracking
ip admission name ise proxy http inactivity-time 60
cts sxp enable
cts sxp default source-ip 10.10.111.13 {use Switch Management IP}
dot1x system-auth-control
fallback profile ise
ip access-group ACL-DEFAULT in
ip admission ise
! ----Auto Smart Ports Macro method for port configurations-----
Т
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 device to connect to the wired network. Cisco ISE was configured to alert and mitigate this threat.

Cisco ISE was configured to profile all devices connected to the network. Any devices 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.

To address the Incident Response and Auditing HIPAA Safeguards identified above, Cisco ISE can be configured to send its log data to the RSA enVision log management platform. Figure 5-65 shows the configuration of logging servers.

🔆 System 🛛 🖉 Identity Management	Network Resources 🛛 🛃 Web Porta	I Management	Feed Service		
Deployment Licensing Certificates Log	ging Maintenance Backup & Resto	Admin Access	Settings		
Logging	Remote Logging Targets				
Local Log Settings					
Remote Logging Targets	/ Edit + Add Duplicate	XDelete			
			1222 C	Description .	
Logging Categories	Name	 IP Address 	Туре	Description	Status
Logging Categories	Name O LogCollector	 IP Address 10.1.103.4 	UDP SysLog	Syslog Target for Log Collector	Status Enable
Message Catalog					
	O LogCollector	10.1.103.4	UDP SysLog	Syslog Target for Log Collector	Enable

Figure 5-65 Remote Logging Targets

As a best practice, 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

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications 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 complying with corporate and regulatory requirements.

Models Assessed			
Cisco Prime Man	agement Solution		
HIPAA Safeguard	s Addressed		
Administrative	Standards/Implementation Specifications		
164.308	(a)(1)(i) Security Management Process		
	(a)(3)(i) Authorization/Supervision		
	(a)(4)(i) Access Authorization		
	(a)(5)(i) Log-in Monitoring		
	(a)(6)(i) Response and Reporting		
Technical	Standards/Implementation Specifications		
164.312	(a)(i) Access Control		
	(b) Audit Controls		
HIPAA Standards	Failed		
No HIPAA stands	ards were failed.		
HIPAA Implement	ation Specifications Failed		
No HIPAA imple	mentation specifications were failed.		

Table 5-14 PHI HIPAA Assessment Summary—Cisco LMS

Primary PHI 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 compliance dashboard to simplify the ongoing management for administrators.

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.
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.

HIPAA Assessment Detail—HIPAA Safeguards Passed

All of the sample configurations of the LMS shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - \$164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - \$164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
 - \$164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in \$164.308(a)(4).
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.

Γ

- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.

Sample Configuration

A centralized user database (Active Directory) 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 all of the safeguards listed under Access Control above.

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 5-66).

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 Ma	anagement Setup		
Navigator	Role Management Setup		
Local User Policy Setup			Showing 6 records
Local User Setup	Roles	Description	Default Roles
Notify Users Role Management Setup	1. Approver	Approver Role	
	2. Help Desk	Help Desk Role	V
	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 Ex	port Import I Set as default Clear	default

Figure 5-66 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. (See Figure 5-67.)

	bmcgloth	1			
ssword:	•••••		/erify Pas	sword:	
nail:	bmcgloth@	cisco-irn.com			
uthorization Type					
	Authorization 🔍 E	nable Task Autho	rization	Enable Device Authorization	
Roles		Device lev	el Auth		
🗷 Help Desk		Not Appli	cable		
Network Operator					
Approver					
Network Administr	ator				
🗵 System Administra	tor				
🗵 Super Admin					
etwork Level Login Cre	dentials				
		n credentials for l	.MS to co	mmunicate with the network	
ername: bmcgle	- 44-				
Diricgi					
ssword: ••••	••••	Verify Pass		•••••	
able Password:		Verify Pass			

Figure 5-67 LMS Local User Profile and Roles

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 5-68). As of version 4, LMS no longer supports external authorization.

Figure 5-68 Authentication Mode Setup

Cisco Prime Cisco LAN Management Solu	Ny Menu 🔻	Monitor 🔻	Inventory 🔻	Configuration	▼ R
Admin > System > Authentication Mod	e Setup				
uthentication Mode Set	ир				
Authentication Mode Setup					
Current Login Mode: TACACS+					
Available Login Modules					
1 C Local Authentication					
20 Local UNIX System					
30 MS Active Directory					
4C RADIUS					
5 C TACACS+					
L					
				Change	

In the TACACS server configuration, either all accounts or only specified accounts can be allowed for authentication in the event that the ACS server cannot be reached. (See Figure 5-69.)

Figure 5-69 Login Module Options

<i>e</i> Ims - ChangeLoginSe	ettings - Windows Internet Explorer 🗁 🗖 🗖 💌 🗙
Login Module Options	
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
	$\ensuremath{\bigcirc}$ 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

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.

293317

To address the Incident Response and Auditing HIPAA Safeguards identified above, 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 5-70). Select "Console logs from Tomcat" in the component dropdown. Click the **Enable** radio button and then click **Apply**.

cisco LAN Managemen	🔍 My Mi	enu 🔻 Mor	nitor 🔻	Inventory	 Cor 	nfiguration 🔻	Reports 🖪
Admin > System > Debug Setting:	s > Common Services Log Config	gurations					
Navigator	Common Servic	es Log C	onfig	uration	5		
Discovery Logging Configuration	Common Services Lo	og Configurati	ons				
Layer2 Configuration and	Component:	Console logs	s from Ta	Imcat	-		
Reports	Log File(s) Location:	C:/PROGRA~2	/CSCOpx/	'MDC/tomcat/l	ogs/stdou	t.log	
Common Services Log Configurations	Description:	Enables/Disabl tomcat	es debug f	or direct cons	ole logs fr	om web applical	tions in
comgurations	Debug Mode:	⊙ _{Enable} O	Disable				
Data Collection							
Dynamic User Tracking						Reset All	Apply
Dynamic User Tracking							

Figure 5-70 Common Services Log Configurations

<u>Note</u>

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. Information 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 5-71.)

Figure 5-71 Adding Logs to the Rotation

54. C C:\PROGRA~2\CSCOpx\MDC\tomcat\logs\stdout.log 55. C C:\PROGRA~2\CSCOpx\log\syslog.log 56. C C:\PROGRA~2\CSCOpx\log\CMFOGSClient.log	102400 1048576 307200	gz gz gz	99 3 5
57. O C:\PROGRA~2\CSCOpx\log\CMFOGSServer.log	307200	gz	5
58. C C:\PROGRA~2\CSCOpx\log\Campus.log	600	gz	2
59. C C:\PROGRA~2\C5COpx\log\Cmapps.log	600	gz	2
Rows per page: 100 💌	l. I	<< Go to page:	1 of 1 pages Go >>
Select an item then take an action>			Edit Delete I Add

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 5-72.)

Figure 5-72 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
Vo	te: * - Required Field	

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 0-8.)

233223

Figure 5-73 Server Side File Selector

Server Side I	File Selector	
File:	C:/PROGRA~2/CSCOpx/MDC/tomcat/logs/	
	stderr.log-OLD-3	
Directory Cont	stdout.log ent: stdout.log-OLD-1 stdout.log-OLD-2 stdout.log-OLD-3	
Drive:		
	OK Cancel	20,332.4

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

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. 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 (Linux, Solaris, Windows) based on the deployment OS. Logs stored locally are buffered and require operator level privileges on the system to be viewed.

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.

To secure authentication information and management of the LMS server and the devices that it manages, addressing Safeguard 164.308(a)(1)(i) Security Management, the LMS system was configured to support only encrypted protocols, as shown in Figure 5-74. Device management preferences are configured in Admin > Collection Settings > Config Transport Settings. Add secure protocols to the list in order of preference and remove insecure protocols for each Application Named function.

	ettings			
onfig Transpo	t Settings			
pplication Name:	Archive Mgmt 💌			
	Available Protocols		Selected Protocol O	rder
	SSH		HTTPS SSH	
	SCP	Add >>	SCP	Up
Config Fetch :	TELNET	< Remove		Down
				Lowin
	Available Protocols		Selected Protocol O	rder
	HTTPS		HTTPS	
	SSH SCP		SSH SCP	
Config Deploy :	TFTP	Add >>		Up
2	RCP	< Remove		Down

Figure 5-74 Device Management Transport Settings

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 5-75. These configuration steps can also be found in the LMS 4.2 Administration Guide, page 53.

LAN Management Solution		bmcgloth	
CISCO LAN Management Solution	My Menu 🔻 Monitor 🔻 Inventory 🔻 Configuration 🔻 Reports 🔻	Admin	•
Admin > Trust Management > Local Server > Bro	wser-Server Security Mode Setup		
Navigator	Browser-Server Security Mode Setup		
Current Settings			
Browser-Server Security	Browser-Server Security Mode Setup		
Mode Setup	Current Setting: Enabled		
Certificate Setup	Change Setting To: O Enable O Disable		
Single-Server Management			

Figure 5-75 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 (such 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.properties
```

Soft appliance:

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

b. Update the field IS_DEFAULT_PAGE as "false".

c. Clear the browser cache and login-in (Daemon restart not required).

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco LMS supports session policies under the Admin > System > System Preferences tab. It is a best practice to change the session time-out to 15 minutes, as shown in Figure 5-76.

Figure 5-76 LMS System Preferences for Idle Timeout

w / Edit System Preferences E mail Settings	
5MTP Server:	msexchange.cisco-irn.co
5MTP Server TimeOut:	6000 in Milliseconds
Administrator E-mail ID:	administrators@cisco-irn
Enable E-mail Attachment:	
Maximum Attachment Size:	2 MB 💌
Other Settings	
CP User:	cwuser
iCP User:	cwuser
iCP Password:	•••••
iCP Verify Password:	•••••
Disable Idle Timeout Settings:	
dle Timeout:	15 🗾 in Minutes

As a best practice, 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

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications 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.

Models Assess	ed
Cisco Security	Manager version 4.0.1
HIPAA Safegua	rds Addressed
Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(ii)(A) Authorization/Supervision
	(a)(4)(ii)(B) Access Authorization
	(a)(4)(ii)(C) Access Establishment and Modification
	(a)(5)(ii)(C) Log-in Monitoring
	(a)(6)(i) Response and Reporting
Technical	Standards/Implementation Specifications
164.312	(a)((2)(i) Unique User Identification
	(b) Audit Controls
	(d) Person or entity authentication
HIPAA Standard	ls Failed
No HIPAA star	dards were failed.
HIPAA Impleme	ntation Specifications Failed
No HIPAA imp	lementation specifications were failed.

Table 5-15 PHI HIPAA Assessment Summary—Cisco Security Manager

Primary PHI 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 ePHI data. The Cisco Security Manager allows for the secure configuration of network devices to enforce user access (authorization) to systems containing PHI. Additionally the Cisco Security Manager can run reports on access attempts and can help troubleshoot security events across the infrastructure allowing the organization to monitor access to systems and devices that contain ePHI.

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.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

HIPAA safeguards are spread across multiple categories. The CSM allows healthcare-covered entities and business associates to meet access control safeguards in the Administrative and Technical categories. The access control can be applied to both internal and external users that access ePHI data.

All of the sample configurations of the CSM shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations it might be accessed. Requirements addressed include: Access Control and Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
 - §164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Requirements addressed include: Access Control, Incident Response, and Auditing.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
 - §164.312(a)(2)(i) Unique User Identification. Assign a unique name and/or number for identifying and tracking user identity. Requirements addressed include: Access Control and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.
 - §164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.

Sample Configuration

Cisco CSM is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

To secure authentication information and management of the CSM server, addressing Safeguard 164.308(a)(1)(i) Security Management, the CSM management console was configured to support HTTPS access only. Figure 5-77 shows that Cisco Security Manager is configured in Common Services so that only encrypted communications for administration are used, and AAA role setup type was implemented as Cisco Secure ACS and identified the appropriate Cisco Secure ACS servers.

	lost Wated disco UCS Manager UIM NCM WCS TACACS Image: Second S	
Common Servir Control Servir Software Center Device and Credentials Groups Cecurity Ceports Val Mode Page Admin Terrer Software Center Device and Credentials Groups Cecurity Ceports Val Mode Page Admin Terrer Software Center Device and Credentials Groups Add Mode Setup Coal User Party Software Center Device and Credentials Groups Cerrer Login Module: TACACS+ Security P Address/Hostname Acts TaCACS+Port [4] Secondary P Address/Hostname Acts TaCACS+Port [4] Cogin Acts Admin Name [sm-acs-admin Acts TaCACS+Port [4] Common Setup Acts Shared Secret Key. Cerrent ACS Admin Name [sm-acs-admin Acts TaCACS+Port [4] Cerrent Acts Administrative Access Protocol HTTP Marty P Mitter	CiscoWorks P CISCO Home Server Software Center Device and Credentials Groups	Bookm Help Al
Common Services Image: Service Services Security Common Service Security Security Common Service Security Securi	Common Services CISCO Home Server Software Center Device and Gredentials Groups	Help I At
CISCO Tome Server Server Device and Credentials Groups Image: Server Security Admin Home Page Admin Image: Server Security Admin Home Page Admin Image: Server Security Admin Home Page Admin Image: Server Security Admode Setup Security New Security Admode Setup Admode Setup Admode Setup Security Mode Setup Social User Setup Coal User Setup Current Login Module: TACACS+ Image: Security Add Mode Setup Security Address:Hostname 192:168:42:131 ACS TACACS+ Port: 49 Image: Security Address:Hostname	CISCO Home Server Software Center Device and Credentials Groups	
Nome Server Software Center Device and Credentials Groups • Security • Reports • Admin • Home Page Admin	Home Server Software Center Device and Credentials Groups	
Security Reports Admin Home Page Admin Refere + Server X-Security + AAA Mode Setup AAA Mode Setup AAA Mode Setup Codi Server Setup Codi User Poly Setup Codi User Account Setup Seter a Type: AAA Mode Setup Seter a Type: ACS Admin Name Server-Certificate Setup Setup ACS Admin Name Server-Setup ACS Admin Name Server-Setup ACS Admin Name Server-Setup ACS Admin Name Server-Setup ACS Admin Name Meragement ACS Admin Name Server-Setup ACS Admin Name Meragement ACS Admin Name Server-Setup ACS Admin Name Meragement ACS Admin Name Meragem		
reflect + Server > Security > AAAMode Setup TOC Single-Server Management = Brows-Server Security Mode Setup - Coell User Solery Setup - Coell User Solery Setup - Coell User Solery Account Setup = Pers Server Account setup = Server Account setup = Server Modement - Second Commetion Management - Second Commetion - Second C		
AAA Mode Setup Security Mode Setup Local User Setup Current Login Module: TACACS+ Current ACS Adminin Reserve: Setup Current Login Module: TACACS+ Current A	- United Company Company Address Address Contract	
100 Single-Server Management • Brower-Server • Coal User Policy Setup • Local User Setup • Coal User Setup • Setsets • Server Account • Setup		
	TOC	
Security Mode Setup Local Liser Yorky Setup Local Liser Yorky Setup Certificate Setup Current Login Module: TACACS+ Current Login Module: TACACS+ Current Login Module: TACACS+ Server Certificate Setup Secure Certificate Setup Secure Setup Connection Setup Connection Setup Connection Setup Connection Setup Connection Setup Connection Register al Installed applications with ACS Current ACS Admin Istrative Access Protocol Current ACS Administrative Acces		
- Local User Policy Setup - Local User Policy Setup - Local User Policy Setup - Local User Policy - Contributed Setup Multi-Server Account Setup - Peer Server Account Setup - System Identity Setup - Proxy Server Certificate Setup - Proxy Server Setup - Proxy S		
Aul-Server Trust Kragement - Peer Server Account Stup - System Identity Setup - Peer Server Certificate Setup - Sign-On Setup AAM Node Setup - Soco com User Account Setup - Osco com User Account Setup - Proxy Server Setup - Register al installed applications with ACS - Register al installed applications with ACS	Local User Setup	
Server Dotalis Primary P Account Setup System Identity Setup Per Server Contilis Per Server Contribute Secondary P Address/Hostname Per Server Contribute Stup ACS Admin Name: Corracts-admin ACS Admin Name: Stup ACS Admin Name: Corracts-admin ACS Started Sector Verify ACS Schrini Name: Verify ACS Schrini Name: Verify ACS Schrini Name: Verify ACS Schrini Name: Verify <td></td> <td></td>		
Setup Secondary IP Address/tostname: ACS TACACS+ Port. 49 - System Identify Setup Tertiary IP Address/tostname: ACS TACACS+ Port. 49 - Single Sign-On Setup ACS TacACS+ Port. 49 - Caco conf Connection ACS TACACS+ Port. 49 - Caco conf User Account ACS Admin Name: Csmacs-admin - Caco conf User Account ACS Admin Password:	Anagement Server Details	
- System Koretty Setup - Peer Server Certificate Secondary IP Address/Hostname: ACS TACACS+ Port. [49 Tertiary IP Address/Hostname: ACS TACACS+ Port. [49 Contain Name: Contain Connection ACS Admin Name: Contain Co		
Peer Server Certificate Setup Stopde Sign-On Setup IAA Mode Setup Second Setup Account Setup ACS Admin Name: Cisco: con User Account Setup Proxy Server Setup Acs Shared Secret Key: Proxy Server Setup Register all instaled applications with ACS Current ACS Administrative Access Protocol Current ACS Administrative Access Protocol Child The Point Hittps:		
Setup Login LAR Mode Setup ACS Admin Name: csm-acs-admin Jaco com Connection ACS Admin Name: csm-acs-admin ACS Admin Password: ••••••••• • Osco con User Account Setup • Proxy Server Setup Venify: •••••••• Proxy Server Setup Venify: ••••••• Proxy Server Setup Register all installed applications with ACS Current ACS Administrative Access Protocol ••••••• ••••••• •••••••••		
WA Mode Setup ACS Admin Name: csm-acs-admin Jaco com User Account ACS Admin Name: csm-acs-admin - Osco com User Account ACS Admin Name: csm-acs-admin ACS Admin Password Ventfy: oscooso Proxy Server Setup ACS Shared Secret Key: oscooso Proxy Server Setup Registration Register all installed applications with ACS Current ACS Administrative Access Protocol HTTP © HTTPS	Setup	
ACS Admin Name: Csm-acs-admin ACS Admin Name: Csm-acs-admin ACS Admin Name: Csm-acs-admin ACS Admin Name: Csm-acs-admin ACS Admin Name: Csm-acs-admin Verify:		
- Clobic com User Account ACS Autilini Password, ACS Shared Secret Key:		
ACS Shared Secret Key. ••••••• Verify: ••••••••		
Procy Server Setup Application Registration Register all installed applications with ACS Current ACS Administrative Access Protocol C HTTP C HTTPS	- Usco.com User Account	
Current ACS Administrative Access Protocol C HTTP C HTTPS	Hos onlined occitency.	
Current ACS Administrative Access Protocol	Application Registration	
С нтр С нтрз	Register all installed applications with ACS	
С нтр С нтрз	Current ACS Administrative Access Protocol	
Apply		
Apply		
	Annly	

Figure 5-77 CSM Secure Administration and AAA Policy

Sample Configuration

Cisco Security Manager is designed to track and monitor all administrative user access and events. To address the Incident Response and Auditing HIPAA safeguards identified above, Cisco Secure CSM can be configured to send its log data to the RSA enVision log management platform.

Figure 5-78, Figure 5-79, and Figure 5-80 show the Logs, Audit Report, and View Settings screens.

i iguit 570 Eog3	Figure	5-78	Logs
------------------	--------	------	------

Logs			
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

291468

	Message Level	Date	Source	Action	Object	User Name	Activity
Search by action:	Success	07-Jun-2011 14:08:48	Devices	Add	1811	admin	None
⊡ □ 🕌 All 🔶	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	PolicyManager	Assign	None	admin	admin_31.May.2011_1
Devices Devices Devices	Success	07-Jun-2011 10:53:12	PolicyManager	Create	None	admin	admin_31.May.2011_1
🕀 🔲 🎴 License	Success	07-Jun-2011 10:53:12	PolicyManager	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	LDAPserver1	admin	admin_31.May.2011_1
From: Jun 06 2011	Success	07-Jun-2011 02:00:00	Deployment	Purge	None	System	None
	Success	07-Jun-2011 02:00:00	Deployment	Purge	None	System	None
To: Jun 07 2011	Success	07-Jun-2011 02:00:00	Deployment	Purge	None	System	None
	Success	06-Jun-2011 02:00:00	Deployment	Purge	None	System	None
earch for activity by state: Filter: No Activity	Success	06-Jun-2011 02:00:00	Deployment	Purge	None	System	None
Filter: No Activity	Success	06-Jun-2011 02:00:00	Deployment	Purge	None	System	None
iearch by message warning level:							
Information A Warning							
Warning Success	Showing page 1 of 1	# of rows per page:	50 💌				
Search Reset							< >

Figure 5-79 Audit Report



ews	Event Monito	oring													
New 📝 Edit 📋 Delete	🛃 All De	vice Events	Firewall Tr	affic Events 🚿	🔹 🤙 Firewa	I Denied Events	📅 AAA Eve	nts 🛛 🛺 IPSee	: VPN Events					4 0	De
Predefined Views	View Set	ttings													×
All Device Events	Search within	results: Q Ty	be here to sear	ch	रुँ। last 1	0 min 👻 All Ever	nts (Default) 👻	Save •	Start S	top 1 Clear				12	2.86
Firewall Denied Events	Peceive Time	Severity -	¥ Ev ▼	Event Name	Device -		Sourc +		Destin	Direction -	1	Action 👻	Conne 🗸	Policy	m
AAA Events		A Informa	302013	Built TCP	💭 ny-asa		tcp/14633	208.72		autbound		✓ built	63555433	roncy	
NAT Events		A Informa	302013	Teardown TCP			tcp/5636		tcp/20998	C- Outbound	ter ter	➡ ^c teardown			-
IPSec VPN Events		A Informa			ny-asa		tcp/16825	208.72		and outbound		w built	63555431		
SSL VPN Events	6/7/11 2:27			Teardown TCP		66,98,1			tcp/11650	C- outboaria	TOP top	➡ ⁴ teardown			
		A Informa			ny-asa		tcp/17284	66.98.1		A outbound		✓ built	63555430		
- All IPS Events		A Informa	302014	Teardown TCP		216.188			tcp/16019		top	➡ ^c teardown			
- TPS Priority Alerts		A Informa		Teardown TCP		75, 125,			tcp/23005		TOP top	■ teardown			
IPS Alert Events	6/7/11 2:27		302021	Teardown I	-0.	4.69.15		172.16			Kill icmp	n ^d teardown			
IPS Status Events	6/7/11 2:27		302020	Built ICMP	S ny-asa	4.69.15		172.16		inbound	Kitte icmp	✓ built			
My Views		A Informa	302013		S ny-asa		tcp/30537	216.188		and outbound		✓ built	63555428		
All Device Events -Admin		A Informa	302013		ny-asa		tcp/34457	75.125		and outbound		🖌 built	63555427		
Firewall Traffic Events last		A Informa	302014	Teardown TCP		208.72			tcp/17225	*	REP top	□ ^c teardown	63555017		
	6/7/11 2:27		302013		ny-asa		tcp/27866	208.72		autbound		🖌 built	63555426		
		A Informa		Teardown TCP		208.72			tcp/26412	*	top	n [∉] teardown	63555015		
	6/7/11 2:27		302013		ny-asa		tcp/10323	208.72	tcp/5636	al outbound		🖌 built	63555424		
	6/7/11 2:27	A Informa	302014	Teardown TCP		216.188	tcp/443	10.10.1	tcp/29199		top	n [€] teardown	63555014		
	6/7/11 2:27	A Informa	302014	Teardown TCP		75.125	tcp/22	10.10.1	tcp/31612		top	n [€] teardown			
	6/7/11 2:27	A Informa	302013	A Built TCP	🔗 ny-asa	172.16	tcp/30704	216.188	tcp/443	all outbound	tcp	🖌 built	63555423		
	6/7/11 2:27	A Informa	302013	Built TCP	🔗 ny-asa	172.16	tcp/33061	75.125	tcp/22	al outbound	top top	🖌 built	63555422		
	6/7/11 2:27	A Informa	302021	Teardown I	🔗 ny-asa	38.104	0	172.16	24790		Km icmp	☐ ⁴ teardown			
	6/7/11 2:27	A Informa	302020	Built ICMP	🔗 ny-asa	38.104	0	172.16	24790	🐴 inbound	Km icmp	🖌 built			
	6/7/11 2:27	A Informa	302014	Teardown TCP	🔗 ny-asa	208.72	tcp/5636	192.168	tcp/13551		top top	☐ ⁴ teardown	63555011		
	6/7/11 2:27	A Informa	302013	Built TCP	🔗 ny-asa	172.16	tcp/24790	208.72	tcp/5636	autbound 🥵	tcp	🖌 built	63555419		
	6/7/11 7.77	• •	202014	Taardaum TCD	Ø	200 72	ton /6676	100 100	ton/16000				69666010		
	•													70	-
	50														
	0	2:18 PM	2:19 PM	2:20 8	PM	2:21 PM	2:22 PM	2:23 PI	A 2:2	4 PM	2:25 PM	2:26 PM	2:27	PM 🏓	F

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of Automatic logoff options. Cisco CSM supports session idle timeout under the Administration Custom Desktop Settings tab. It is a best practice to change the session timeout to 15 minutes, as shown in Figure 5-81.

AutoLink	Cus	itomize Desktop		
Configuration Archive Configuration Archive Configuration Archive Debug Options Debug Options Debug Options Device Communication Device Option Device Optio		Reset "Do Not Adi' on Warnings	Sove Reset	Restore Defaults

Figure 5-81 Customize Desktop

As a best practice, 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. 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 implementation of Cisco CSM was Windows-based.

91467

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Encryption

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 HIPAA requirements for protecting stored ePHI 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 properly secure information and enables its accessibility when needed at any point in its lifecycle through a powerful management console and built-in high availability features. RSA Data Protection Manager provides a comprehensive platform for enforcing and managing the security of sensitive data.

Table 5-16 PHI HIPAA Assessment Summary—Cisco RSA Data Protection Manager

Models Assessed

RSA Data Protection Manager	version KM-3.1 / AM-6.1.SP3	

HIPAA Safeguards Addressed

Γ

Administrative	Standards/Implementation Specifications				
164.308	(a)(1)(i) Security Management Process				
	(a)(3)(i) Authorization/Supervision				
	(a)(4)(i) Access Authorization				
	(a)(5)(i) Log-in Monitoring				
	(a)(6)(i) Security Incident Procedures				
Technical	Standards/Implementation Specifications				
164.312	(a)(i) Access Control				
	(b) Audit Controls				
	(c)(1) Data Integrity				
HIPAA Standards F	ailed				
No HIPAA standar	rds were failed.				
HIPAA Implementa	tion Specifications Failed				

Table 5-16 PHI HIPAA Assessment Summary – Cisco RSA Data Protection Manager

No HIPAA implementation specifications were failed.

Primary PHI Function

The primary function of RSA Data Protection Manager is to securely manage the keys that protect ePHI data.

This safeguard was met using the RSA Data Protection Manager to encrypt data in the database, file server, and storage. All ePHI data is encrypted to prevent unauthorized access or modification to the data. Unauthorized access attempts are logged and automatic notification can be sent to authorized personnel. With automated event notification, the RSA Data Protection Manager's detection capabilities can help an organization quickly identify and contain security violations.

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 PHI 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 ePHI data or not.

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 5-82.)



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.

Because of vulnerabilities with RSA signatures with a small public exponent, especially 3, RSA recommends that an exponent of F4 (216+1) be used.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of RSA Data Protection Manager shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.

L

- §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical Safeguards.
 - §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.

Sample Configuration

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 and is designed to meet all of the Access Control safeguards above. The included RSA Access Manager Internal Database is used. Within RSA Data Protection Manager (and the included Access Manager), individual user IDs are assigned. Roles are defined and based on group membership.

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 5-83 shows an appropriate password policy for compliance.

Figure 5-83 Pa	assword Policy Settings	
RSA Access Manager: Edit I	Password Policy +	
(Carteria Contraction (Carteria Contraction)	https://rsa-kma.cisco-irn.com/admingui/ListPolicies.jsp?id=1&edit= 🏫 🛪 🕑 🚷 🛪 Google	P 🔒 Feedback
Most Visited	S Manager 📄 UIM 📄 NCM 📄 WCS 👩 TACACS 🎯 RSA enVision 📄 HyTrust 🕮 CM-2 📄 RS	iA-AM 🛛 🛛 🔀 Bookma
RSA Access M	He	
Home Define Re Delegate Adr	sources Authorize Access Manage Users Delegate Administration ministration > Password Policies	
🔍 <mark>></mark> Edit Pa	ssword Policy	How To Hide
	ets of requirements for user passwords, such as minimum and maximum password length. Password policies oups and govern password requirements for all users within that administrative group.	Understand Password Policies
* is a required field		Add Password Policies
Password Policy Basics		
i Policy Name *		
Description	Default Password Policy 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 *	7	
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	C Users can enter an unlimited number of incorrect passwords without being locked out. C Lock out a user after 6 incorrect password entries in 1 Days 💽	
i Unlock	 Require an administrator to unlock users who have been locked out. Automatically unlock users after 30 Minutes 	
i Notification E-mail	.::	
Update > Cancel X	3	

RSA Data Protection Manager is designed to track and monitor all administrative user access and events. RSA Data Protection Manager can be configured to send its log data to the RSA enVision log management platform to address the Incident Response and Auditing HIPAA Safeguards identified above. 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/). 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

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications 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 Assesse	d
EMC CLARiiO	N CX-240
EMC Unified In	frastructure Manager version 2.0.1.1.160
HIPAA Safeguar	ds Addressed
Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(ii)(A) Authorization/Supervision
	(a)(4)(ii)(B) Access Authorization
	(a)(5)(ii)(C) Log-in Monitoring
	(a)(6)(ii) Response and Reporting
Technical	Standards/Implementation Specifications
164.312	(a)(i) Unique User Identification
	(b) Audit Controls
	(c)(1) Data Integrity
HIPAA Standard	s Failed
No HIPAA stand	dards were failed.
HIPAA Implemen	ntation Specifications Failed
No HIPAA impl	ementation specifications were failed.

Table 5-17 PHI HIPAA Assessment Summary—EMC SAN Disk Array

Primary PHI Function

The primary function of the EMC SAN disk array is to store ePHI data. There is no direct PHI requirement for this storage function. This control was met using the EMC SAN Disk Array granular access control to minimize the access to the ePHI data in storage. Additionally the EMC SAN Disk Array can work with application security controls to minimize access privileges to ePHI data. This helps meet the requirement for minimal use by allowing the individual to only access what is needed to perform the job function. Users can be assigned to groups and, based on privilege levels, have access to only the information they require for their job function.

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.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

HIPAA safeguards are spread across multiple categories. The EMC SAN allows healthcare covered entities and business associates to meet access control safeguards in the Administrative and Technical categories. The access control can be applied to both internal and external users that access ePHI data.

All of the sample configurations of the EMC SAN Disk Array shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations it might be accessed. Requirements addressed include: Access Control and Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
 - §164.312(a)(2)(i) Unique User Identification. Assign a unique name and/or number for identifying and tracking user identity. Requirements addressed include: Access Control and Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
 - §164.312(c)(1) Data Integrity. Implement policies and procedures to protect ePHI from improper alteration or destruction. Requirements addressed include: Encryption, Integrity, and Auditing.

Sample Configuration

EMC SAN Disk Array is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. A centralized user database (Active Directory) is accessed by the EMC SAN Disk Array using LDAP services. Individual user IDs are assigned. Roles are defined and based on group membership

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.

- **Step 1** To configure LDAP authentication, go to the Domains tab, then select **Configure LDAP for CLARiiON Systems** from the Users menu on the left.
- **Step 2** Add a new LDAP service by clicking **Add** and then **OK**, as shown in Figure 5-84.

ze

Figure 5-84 Adding LDAP Service

Step 3 Configure the LDAP server for Active Directory, as shown in Figure 5-85.

Figure 5-85 Configuring the LDAP Server for Active Directory

IP Address	192	168	. 42	. 130		Port Number	636
Server Type	Active Di	rector	r		*	Protocol	LDAPS V
BindDN	CN=Bart Mo	:Glothin	.CN=Use	ers.DC=c	isco-ir	n.DC=com	
(Example: cr						=bigcorp,dc=co	om)
Bind Passwor		****	*****				
	-						
Confirm Bind	Password	****	*****				
User Search I	Path						
CN=Users,DC=	isco-irn,DC=	-com					
(Example: o	u=Users,do	c=bigc	orp,dc=	=corn)			
Group Search	Path (Opt	ional)					
CN=Users,DC=0	isco-irn,DC=	-com					
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 5-86.

Gro 🖌 <i< th=""><th>nsert Name> Monitor</th><th>Add</th></i<>	nsert Name> Monitor	Add
Туре	Name	Role
Group Group Group	Storage-Admin Storage-Security Storage-Monitor	Administrator Security Administrator Monitor
	Remove	

Figure 5-86 Role Mapping

- **Step 5** The Advanced features were left at their default settings, as shown in Figure 5-87.
 - Figure 5-87 Advanced Settings

User ID Attribute	sAMAccountName	
User Name Attribute	m	
Group Name Attribute	m	
Group Member Attribute	member	
User Object Class (optional)		
Group Object Class	group	
Additional Functions Duplicate the current service	settings	Duplicate

Step 6 You can then log out, and log back in, selecting the **Use LDAP** option for centralized authentication, as shown in Figure 5-88.

V1.0.50 V1.0.50 System 192.168.42.51 Name pmcgloth Password protection Use LDAP Scope Global @ Use LDAP Scope Global @ Use LDAP

Figure 5-88 Selecting Use LDAP Function

Step 7 For further installation information, see the *FLARE 30 Security Configuration Guide* on EMC Powerlink for configuring LDAP/Active Directory authentication.

EMC CLARiiON is designed to track and monitor all administrative user access and events.

To address the Incident Response and Auditing HIPAA safeguards identified above, SP event logs on CLARiiON storage systems can store only a fixed number of events, and wrap if that limit is exceeded. This may take days, weeks, months, or years depending on the logging activity. To keep 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 5-89.)

Γ



Figure 5-89 Using Log to System Log Option

To secure authentication and management of the EMC Array, addressing Safeguard 164.308(a)(1)(i) Security Management, when you connect to Unisphere through http://<clariton_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.

As a best practice, 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. EMC CLARiiON uses Network Time Protocol (NTP) to update and synchronize local clock facilities.

CLARiion uses the NTP configuration statements shown in Figure 5-90.

Figure 5-90 NTP Configuration for Domain: Local

EMC Unisphere

< > 🔒 All Systems	-	Dashboard	Syste	em List	🔯 Domains	🛕 Alerts	0
All Systems > Domains							
Multi-Domain Manage Multi-Domain Configuration	<u> </u>	NTP Configu	ration for Do	main: Loca	1 Hour 💌	Time Sync Inte	- 🗆 🗙
Local Domain	*	NTP Servers					
<u>Select Domain Master</u> <u>Configure NTP</u> <u>Add/Remove Systems</u> <u>Scan for CLARiiON Systems</u>			Server 168 . 62 168 . 62	. 161 . 162	Key ID	Key Value	
Users <u>Manage Global Users</u> <u>Configure LDAP for CLARiiON Systems</u>	*			•			~
				<u>o</u> i	< <u>A</u> pply	Cancel	<u>H</u> elp

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Monitoring

RSA enVision

RSA enVision is a security information and event management (SIEM) platform that addresses HIPAA safeguards to track and monitor all access to systems and network resources containing ePHI 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 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.

Γ

Models Assessed				
RSA enVision ve	rsion 4.0, Revision 5			
HIPAA Safeguard	s Addressed			
Administrative	Standards/Implementation Specifications			
164.308	(a)(1)(i) Security Management Process			
	(a)(1)(ii)(D) Information System Activity Review			
	(a)(3)(i) Authorization/Supervision			
	(a)(5)(i) Log-in Monitoring			
	(a)(6)(i) Security Incident Procedures			
	(a)(6)(ii) Response and Reporting			
Technical	Standards/Implementation Specifications			
164.312	(b) Audit Controls			
HIPAA Standards	Failed			
No HIPAA standa	ards were failed.			
HIPAA Implement	ation Specifications Failed			
No HIPAA imple	mentation specifications were failed.			

Table 5-18 PHI HIPAA Assessment Summary—RSA enVision

Primary PHI Function

The primary function of RSA enVision is to securely store and correlate the system logs that is receives.

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.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the RSA enVision shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - \$164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - \$164.308(a)(1)(ii)(D)Information System Activity Review. Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking.
 - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.

Sample Configuration

The RSA enVision Internal Database is used (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.

RSA enVision management interfaces implement role-based access control that can be used to restrict access to privileged user IDs, as shown in Figure 5-91.

L

System Configuration - RSA enVision	on - Microsoft Internet Explorer	_ 🗆 >
Overview Alerts Analysis Reports		
Dashboard System Performance	Use this window to add or modify a user. RSA en	Vision
Best Practices	Manage Users - Add/Modify User	
System Configuration	User information	۲
Devices Manage Monitored Devices Manage Device Group Filters	User ID: bmcgloth Enabled: First name: bat Last name: mcglothin	
Manage Device Attribute Definition Import/Export Device Attributes Manage Device Types Messages Messages	Password: Confirm password: Co	
Directories 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 Permissi	Report folder permissions	۲
Manage Event Explorer Permission Set Up Access Denied Display License Information	Device access permissions	۲
Services	Site login permissions	۲
Manage Collector Service Set Up DNS Resolver Service	Alert view permissions	۲
- Set Up DHCP Polling Service	Dashboard permissions	۲
∢► Vulnerabilities	Event Explorer permissions	۲
Assets Task Viewer	Apply Cancel Delete	
Jser: bart moglothin (bmogloth) Log Out		
Done	📄 📄 🔂 Local intrane	t

Figure 5-91	RSA enVision	User H	Profile
i iguit o o o i		03011	101110

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 5-92.

System Configuration - RSA enVisio		plorer		
Overview Alerts Analysis Reports	<u>+</u> 4 0			
Dashboard	Lice this window	v to display the Authentication Serve	rconfiguratione	RSA enVision
System Performance		vio uispiay tre Autrentication Serve	r comigurations.	INSA EINISION
Best Practices	Manage Authentication	Servers		
	Delete	Fully Qualified Hostname	IP Address	
System Configuration		RSAenVision-ES.RSAenVision.nic	127.0.0.1	
Devices Manage Monitored Devices Manage Device Group Filters Manage Device Attribute Definition ImportExport Device Attributes Manage Device Types Messages Directories		activedirectory.cisco-im.com	192.168.42.130	
Users Anage Users Anage User Sessions Manage Authentication Servers Manage Groups Manage Site Log In Permissions Manage Device Access Filters		Log in attribute:	activedirectory, cisco-irn, com User logon name CDAP protocol over TLS/SSL on port 636 CDAP on port 389	
Manage Module and Tool Permiss Manage Event Explorer Permissio Set Up Access Denied Display License Information Services Manage Services Manage Collector Service Set Up DNS Resolver Service		Apply	Cancel Help	
Set Up DHCP Poling Service		Dele	te Add	
Jser: bart mcglothin (bmcgloth) Log Out	Connected to:NIC / RSAenV	ision / RSAenVision-ES Logged in	since: Mon Jun 20 12:57:57 PDT 2011 Server Tin	ne: Mon Jun 20 13:23:50 PDT 2011
Done				🔒 🍕 Local intranet

Figure 5-92 RSA enVision Authentication Servers

RSA enVision is designed to track and monitor all administrative user access and events. To address the Incident Response and Auditing HIPAA safeguards identified above, it performs the role of a central logging repository. RSA enVision 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.

To secure authentication information and management of the RSA enVision server, addressing Safeguard 164.308(a)(1)(i) Security Management, the management console is accessible only via HTTPS.

As a best practice, NTP is used to synchronize clocks among network devices. 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.

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications 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 PHI 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

Virtualized technologies create additional security requirements to ensure that the virtualized environment security controls are appropriate for the data sensitivity. 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 Assessed					
HyTrust versior	n 2.2.1.14064				
HIPAA Safeguar	rds Addressed				
Administrative	Standards/Implementation Specifications				
164.308	(a)(1)(i) Security Management Process				
	(a)(3)(ii)(A) Authorization/Supervision				
	(a)(4)(ii)(B) Access Authorization				
	(a)(5)(ii)(C) Log-in Monitoring				
	(a)(6)(ii) Response and Reporting				
Technical	Standards/Implementation Specifications				
164.312	(a)(1) Access Control				
	(b) Audit Controls				
HIPAA Standard	ls Failed				
No HIPAA stan	dards were failed.				

 Table 5-19
 PHI HIPAA Assessment Summary – HyTrust Appliance

Table 5-19 PHI HIPAA Assessment Summary—HyTrust Appliance

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Primary PHI Function

The primary function of HyTrust Appliance is to provide an automated control and audit facility for the virtual infrastructure and cloud stack.

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.

HIPAA Assessment Detail—HIPAA Safeguards Passed

The HyTrust Appliance allows for management of user access (authorization) to systems containing ePHI. Additionally, the HyTrust Appliance can prevent unauthorized devices from accessing systems containing ePHI and protect access from unauthorized locations.

The HyTrust Appliance logs can be used to identify unauthorized attempts to connect to systems containing PHI to help meet the supervision requirements.

All of the sample configurations of the HyTrust Appliance shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
 - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.

- §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.

Sample Configuration

The Hytrust Appliance is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. By integrating HyTrust Appliance authentication with Microsoft Active Directory, user accounts and passwords are not managed on the HyTrust Appliance; instead, when authentication is requested by the user, the HyTrust Appliance performs the actual authentication request against Active Directory. Complex AD environments with multiple domains are supported for authentication. Individual user IDs and roles are based on group membership.

The 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 virtual systems to operating only on the PHI portion of the infrastructure and enforced separation of duties between the network administrators and application owners. (See Figure 5-93.)

🚺 Edi	t Rule			
			PCINetworkAdminOnly support	_
		Role		
		Propagate	A	
		Description		
		Assign to Policy Resource	Assign	
🗆 Sek	ect Al 🗆 View.	AI		
Add	Delete			
Showin	g 1 to 2 of 2			<<<1>>>>
	Edit	Constraint Type	Description	
	Edit	Client IP Match	172.16.2.10	
	Edit	Client Protocol	vSphere (SOAP)	
				Ok Cancel

Figure 5-93 Edit Rule Screen

Policy and privilege definition was performed by a separate group of authorized users, typically security professionals.

The 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.

RSA two-factor authentication is supported, where the user enters the AD password (something they know) in conjunction with an RSA physical token (something they have).

The HyTrust Appliance enables RSA two-factor authentication to work with any methods of access to VMware vSphere or Cisco Nexus 1000V Vblock infrastructure.

The 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 5-94). 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.

Figure 5-94 Using Root Passwords



To secure authentication information and management of the HyTrust and VMware vSphere hosts, addressing Safeguard 164.308(a)(1)(i) Security Management, the HyTrust Appliance configures the virtualization platform (VMware ESX server) to disable unsecure protocols. In addition, the 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 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
```

As a best practice, 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 by specifying the NTP server in the IP settings. (See Figure 5-95.)



Firefox 🔨			
HyTrust - Network Configuration +			~
(+) III 192.168.42.135 https://192.168.42.135:8443/hytrust/network-config	🟫 - 🧭 🚼 - Google	•	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^{\circ}$ Network Configuration		<i>b</i>	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	255.255.255.0		
Connection 2: IP Address	192.168.41.1		
Connection 2: Mask	255.255.255.0		
	192.168.42.1		
*List of DNS Server IP Addresses			
	192.100.42.130		
			==
▼ NTP Servers			
Enable NTP Servers	V		
*NTP Servers	192.168.62.161,192.168.62.162		
			Apply
Copyright © 2009-2011 HyTrus	t Inc. All rights reserved.		

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.
Infrastructure

Routing

L

Router—Clinic

The primary HIPAA function of the Cisco Integrated Services Router (ISR) is the segmentation of ePHI scope and enforcement of that new scope boundary. The ISR is the component that is used as the main routing and security platform of the clinic. 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 clinics 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 5-20	PHI HIPAA Assessment Summary—Cisco ISR
------------	--

Models Assessed	i
CISCO891W ver	rsion c890-universalk9-mz.151-3.T.bin
CISCO1941W-A	/K9 version c1900-universalk9-mz.SPA.151-3.T.bin
CISCO2921/K9	version c2900-universalk9-mz.SPA.151-3.T.bin
CISCO2951/K9	version c2951-universalk9-mz.SPA.151-3.T.bin
CISCO3945-SPE	E150/K9 version c3900-universalk9-mz.SPA.151-3.T.bin
HIPAA Safeguard	ls Addressed
Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Response and Reporting
Technical	Standards/Implementation Specifications
164.312	(a)(1) Access Control
	(b) Audit Controls
	(e)(2)(ii) Encryption
HIPAA Standards	Failed
No HIPAA stand	ards were failed.
HIPAA Implemen	tation Specifications Failed
No HIPAA imple	ementation specifications were failed.

Cisco Compliance Solution for HIPAA Security Rule

Primary PHI Function

The primary function of the Cisco ISR is the segmentation of HIPAA scope and enforcement of that new scope boundary.

It has five primary functions/capabilities in relation to HIPAA.

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 ePHI data environment. Depending on risk vectors within the clinic, 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 ePHI 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 clinic, (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 clinic connects to untrusted networks directly, items 3 and 4 below become relevant. (See Figure 5-96.)





3. As a stateful firewall, restricting traffic between the ePHI data environment and other areas of the network

As soon as any untrusted network is introduced at the clinic level, stateful firewalling needs to be implemented. The following are examples of untrusted networks:

- The Internet
- Wireless
- Satellite
- 3G/4G cellular backup

Step 8 As an intrusion prevention system, inspecting all traffic going to and from the ePHI data environment.

HIPAA Safeguard 164.308(a)(1)(i) requires policies and procedures to detect security violations. IDS is used to address wherever ePHI is present in the organization to detect for anomalous behavior of the sensitive area. (See Figure 5-97.)



Figure 5-97 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 clinic 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.

4. As a VPN system, encrypting all traffic going to and from the clinic across open and public networks.

The Cisco ISR can be used to address the need to encrypt the transmission of ePHI data across open, public networks such as 3G/4G/Wi-fi, and satellite technologies using SSL and IPSec technologies.

Design Considerations

- The security features of the Cisco ISR routers in the clinic 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 clinic designs 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 ePHI data environment (for example, hospitals) networks.
- Enable inspection rules and/or zones 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 clinic router from the WAN needs to be protected by a clinic-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 Solution lab, a private MPLS WAN is simulated, and filtering of the clinic 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 coordinate all logging.
- Disable un-necessary services (for example, Bootp, Pad, ipv6).
- Shutdown unused interfaces.

Each of the clinic 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
- Cisco Enterprise Branch Security Design Guide http://www.cisco.com/en/US/docs/solutions/Enterprise/clinic/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

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the ISR shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - \$164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
 - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
 - §164.312(e)(2)(ii) Encryption. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.
- Incident response—Implement security incident response as required by HIPAA Administrative Safeguards.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.

Sample Configuration

Cisco ISR routers are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership. The following configurations enable central Authentication, Accounting and Authorization:

```
aaa new-model
aaa authentication login CiscoACS 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
```

```
action-type start-stop
group tacacs+
1
aaa accounting commands 15 default
action-type start-stop
group tacacs+
1
aaa accounting system default
action-type start-stop
group tacacs+
aaa session-id common
ip tacacs source-interface Loopback0
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.

```
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 \ensuremath{\mathsf{CiscoACS}}
```

line con 0
login authentication CiscoACS
line vty 0 4
login authentication CiscoACS
line vty 5 15
login authentication CiscoACS

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco ISR routers support session timeout. It is a best practice to set the session timeout to 15 minutes, as shown below.

```
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.

To secure authentication information and management of the ISR router, addressing Safeguard 164.308(a)(1)(i) Security Management, the ISR management interfaces were configured to support HTTPS access, and SSH. 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 1024

Configure the SSH server to use the more secure protocol version SSHv2:

ip ssh version 2

Configure the HTTP server to use HTTPS, and only more secure ciphers:

```
no ip http server
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
```

Cisco ISR routers use firewalling and intrusion detection capabilities to address Safeguard 164.308(a)(1)(i) Security Management by segmenting ePHI networks from other networks and monitoring activity across these networks.

To segment ePHI information, 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
```

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
```

In the clinic, 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
```

Cisco routers are capable of performing intrusion detection. Each of the reference designs includes networks where 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 CISCO-IPS
1
ip ips signature-category
category all
 retired true
category ios_ips default
 retired false
interface GigabitEthernet0/0
description WAN
ip ips CISCO-IPS in
ip ips Store-IPS out
interface GigabitEthernet0/1.11
description POS
ip ips CISCO-IPS in
ip ips CISCO-IPS out
interface GigabitEthernet0/1.15
description WIRELESS-POS
ip ips CISCO-IPS in
ip ips CISCO-IPS out
```

To address the Incident Response and Auditing HIPAA safeguards identified above, Cisco ISR routers can be configured to send log data to the RSA enVision log management platform. 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
```

And SNMP:

```
snmp-server user remoteuser remote 192.168.42.124 v3 access 88
snmp-server user remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps flash insertion removal
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
```

```
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server host 192.168.42.124 remoteuser
```

Public WAN link connections include technologies such as DSL, cable, satellite, Wi-Fi, and 3G/4G networks. These are public networks and Safeguard §164.312(e)(2)(ii) Encryption specifies that electronic protected health information is to be encrypted. A VPN is required to securely tunnel traffic between the clinic and the enterprise network across these mediums.

Cisco Virtual Office provides reference designs for building a VPN solution to connect clinics 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_pape r0900aecd8051bf3b_ns855_Networking_Solutions_White_Paper.html.

The following example describes equipment located at the clinic and the data center headend router. The clinic router is referred to as the spoke router, and the data center router as the hub. Figure 5-98 shows a simplified Cisco VPN topology.



Cisco VPN technology connects the clinics to the data center over the Internet. As a result, a secure, encrypted tunnel is used to secure sensitive information such as ePHI data. Cisco VPN technologies offer a choice to protect the data in transit and provide a secure access to the clinics' 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 clinic 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, clinic 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 Clinic 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

match ip address split_in

```
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
                                                                              11
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
```

As a best practice, 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
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Routers—Data Center

The primary function of data center routers from a HIPAA perspective is routing between ePHI networks and out-of scope networks and enforcing that boundary with firewall services. 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 clinic, security functions are typically separated physically into distinct appliances. The Cisco ASR routers were used for the Internet edge and clinic WAN edge portions of the network within the solution testing.

Models Assesse		
ASR-1002 (RP)	1) version asr1000rp1-adventerprisek9.03.02.01.S.151-1.S1.bin	
HIPAA Safeguar	rds Addressed	
Administrative	Standards/Implementation Specifications	
164.308	(a)(1)(i) Security Management Process	
	(a)(3)(i) Authorization/Supervision	
	(a)(4)(i) Access Authorization	
	(a)(5)(i) Log-in Monitoring	
	(a)(6)(i) Response and Reporting	
Technical	Standards/Implementation Specifications	
164.312	(a)(i) Access Control	
	(b) Audit Controls	

 Table 5-21
 PHI HIPAA Assessment Summary – Cisco ASR

Table 5-21 PHI HIPAA Assessment Summary—Cisco ASR (continued)

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Primary ePHI Function

The primary function of the data center routers is the segmentation of ePHI scope and enforcement of that new scope boundary. The data center router has four primary functions/capabilities in relation to HIPAA:

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 HIPAA ePHI 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 ePHI networks 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 ePHI networks from other internal networks, an organization may use router access lists to protect its scope. As soon as this segment connects to untrusted networks directly, item number 3 becomes relevant.

3. As a stateful firewall, restricting traffic between the ePHI environment and other untrusted areas.

As soon as any untrusted network is introduced to the connections of the data center router, firewalling 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 ePHI environment. HIPAA Safeguard 164.308(a)(1)(i) requires policies and procedures to detect security violations. IDS is used to address wherever ePHI is present in the organization to detect for anomalous behavior of the sensitive area.

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).
- 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.

```
1
ip access-list extended COARSE-FILTER-INTERNET-IN
remark -----
remark ---Block Private Networks---
      ip 10.0.0.0 0.255.255.255 any log
denv
denv
      ip 172.16.0.0 0.15.255.255 any log
      ip 192.168.0.0 0.0.255.255 any log
denv
remark -
remark ---Block Autoconfiguration Networks---
      ip 169.254.0.0 0.0.255.255 any log
deny
remark -
remark ---Block Loopback Networks---
      ip 127.0.0.0 0.0.255.255 any log
deny
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
!
```

<u>Note</u>

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.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the Cisco ASR shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing
 - \$164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
 - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.

Sample Configuration

Cisco ASR routers are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership. The following configurations enable central Authentication, Accounting and Authorization:

```
aaa new-model
aaa authentication login CiscoACS 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.

```
username bart privilege 15 secret 5 <removed>
username bmcgloth privilege 15 secret 4 <removed>
username csmadmin privilege 15 secret 4 <removed>
```

These AAA authentication groups are assigned to the administrative interfaces where users connect:

```
ip http authentication aaa login-authentication \ensuremath{\mathsf{CiscoACS}}
```

```
line con 0
login authentication CiscoACS
line vty 0 4
login authentication CiscoACS
line vty 5 15
login authentication CiscoACS
```

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco ASR Routers support session timeout. It is a best practice to set the session timeout to 15 minutes, as shown below.

```
ip http timeout-policy idle 60 life 86400 requests 10000
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
```

<u>Note</u>

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.

To secure authentication information and management of the ASR router, addressing Safeguard 164.308(a)(1)(i) Security Management, the ASR management interfaces were configured to support HTTPS access, and SSH. 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 1024

Configure the SSH server to use the more secure protocol version SSHv2.

ip ssh version 2

Configure the HTTP server to use HTTPS, and only more secure ciphers:

```
no ip http server
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
```

Configure the use of Secure Copy in place of TFTP:

ip scp server enable

To address the Incident Response and Auditing HIPAA safeguards identified above, Cisco ASR Routers can be configured to send log data to the RSA enVision log management platform. 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
```

And SNMP:

```
snmp-server engineID remote 192.168.42.124 000000000
snmp-server user remoteuser remoteuser remote 192.168.42.124 v3 access 88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0snmp-server enable traps snmp authentication linkdown
linkup coldstart warmstart
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps flash insertion removal
snmp-server enable traps energywise
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server host 192.168.42.124 remoteuser
```

As a best practice, 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 PSTDST recurring
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Switching

Switches—Clinic

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 ePHI applications and devices onto their own network and segregate them from devices that are on non-sensitive networks.

- Cisco branch switches are stackable, expandable switches that can be used for wired device port density in 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 healthcare organization. Modular functionality provides the ability to insert security technology as the needs of the business expand into new areas.

Table 5-22 PHI HIPAA Assessment Summary – Cisco Clinic Switches

Models Assessed

WS-C3560E-PS-24 c3560e-universalk9-mz.122-35.SE5.bin WS-C2960PD-8TT-L c2960-lanbasek9-mz.122-55.SE1.bin WS-C2960G-8TC-L c2960-lanbasek9-mz.122-50.SE4.bin WS-C2960S-48FPS-L c2960s-universalk9-mz.122-53.SE1.bin WS-C2960S-48FPS-L c2960s-universalk9-mz.122-53.SE2.bin WS-C2960CPD-8PT-L c2960c405-universalk9-mz.122-55.0.43.SK.bin WS-4507+R SUP-7 cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin WS-C3560X-48PF-S c3560e-universalk9-mz.122-53.SE2.bin WS-C3560X-48PF-S c3560e-universalk9-mz.122-53.SE2.bin

HIPAA Safeguards Addressed

Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
	(a)(6)(ii) Response and Reporting
Technical	Standards/Implementation Specifications
164.312	(a)(1) Access Control
	(b) Audit Controls
	(c)(1) Data Integrity
	(e)(i) Transmission Security
	(e)(2)(i) Integrity Controls.
	(e)(2)(ii) Encryption
HIPAA Standard	ls Failed
No HIPAA stan	dards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Primary PHI Function

The primary HIPAA compliance feature of clinic switches is to provide secure wired port access.

Clinic switches also provide compliance via segmentation of sensitive networks from out-of-scope networks. Switches extend that Layer 3 boundary to Layer 2. Using VLANs, Cisco clinic switches allow organizations to put their networks into separate VLANs (scopes) from other non-sensitive data (out-of-scope).

Figure 5-99 shows an example of 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 devices from the clinic floor.

Design Considerations

- The configurations of the Cisco Catalyst switches in the clinic 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.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the Cisco clinic switches shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - \$164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
 - §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.
 - §164.312(e)(1) Transmission Security. Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Requirements addressed include: Encryption and Integrity.
 - §164.312(e)(2)(i) Integrity Controls. Implement security measures to ensure that ePHI is not improperly modified without detection until disposed of. Requirements addressed include: Integrity.
 - §164.312(e)(2)(ii) Encryption. Implement a mechanism to encrypt ePHI whenever deemed appropriate. Requirements addressed include: Encryption.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(6)(i) Security Incident Procedures. Implement policies and procedures to address security incidents.
 - \$164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.

Sample Configuration

Cisco switches are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

```
aaa new-model
aaa authentication login CiscoACS 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.

```
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 CiscoACS
```

```
line con 0
login authentication CiscoACS
line vty 0 4
login authentication CiscoACS
line vty 5 15
login authentication CiscoACS
```

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco Clinic switches supports session timeout. It is a best practice to set the session timeout to 15 minutes, as shown below.

```
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
```

To secure authentication information and management of the clinic switch, addressing Safeguard 164.308(a)(1)(i) Security Management, the clinic switch management interfaces were configured to support HTTPS access, and SSH. Before crypto keys can be generated hostname and domain name must be entered:

```
hostname S-A2-MED-1/2
ip domain name cisco-irn.com
```

Generate keys with 1024 or larger bit key generation, not the default 512.

```
Crypto key generate rsa 1024
```

Configure the SSH server to use the more secure protocol version SSHv2:

```
ip ssh version 2
```

Configure the HTTP server to use HTTPS, and only more secure ciphers:

```
no ip http server
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
```

Configure the use of Secure Copy in place of TFTP:

```
ip scp server enable
```

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. See Cisco ISE for more information regarding port authentication.

To address the Incident Response and Auditing HIPAA safeguards identified above, Cisco Switches can be configured to send log data to the RSA enVision log management platform. Cisco switches 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
```

And SNMP:

hidekevs

```
snmp-server user remoteuser remote 192.168.42.124 v3 access 88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan
no-guest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps power-ethernet group 1-4
snmp-server enable traps power-ethernet police
snmp-server enable traps cpu threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
```

snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server host 192.168.42.124 remoteuser

As a best practice, 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 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 PSTDST recurring
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Cisco Catalyst Switches—Data Center

The Cisco Catalyst family of data center switches are designed to securely switch 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 ePHI 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 5-23 PHI HIPAA Assessment Summary – Cisco Data Center Switches

Models Assessed

Cisco Catalyst6509-Sup720-3BXL version s72033-adventerprisek9_wan-mz.122-33.SXJ.bin WS-C3750-48P version c3750-ipbasek9-mz.122-55.SE1.bin

HIPAA Safeguards Addressed	
Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
	(a)(6)(ii) Response and Reporting
Technical	Standards/Implementation Specifications
164.312	(a)(1) Access Control
	(b) Audit Controls
	(c)(1) Data Integrity
	(e)(i) Transmission Security
	(e)(2)(i) Integrity Controls.
	(e)(2)(ii) Encryption
HIPAA Standard	ls Failed
No HIPAA stan	dards were failed.
HIPAA Impleme	ntation Specifications Failed
No HIPAA imp	lementation specifications were failed.

Table 5-23 PHI HIPAA Assessment Summary—Cisco Data Center Switches

Primary PHI Function

Securing the infrastructure is a key PHI compliance feature of Cisco Catalyst data center switches. Cisco Catalyst switches have firewall/IDS modules for perimeter security. (See Figure 5-100.)

Figure 5-100 Cisco Catalyst Data Center Switches



Catalyst Switches with Services Modules VLAN Routing

Firewall Segmentation

Load Balancing

Content Inspection and Filtering

Intrusion Detection and Prevention

Wireless Services Control 290977

The primary function of the Cisco Catalyst data center switches is segmentation of scope and enforcement of that new scope boundary. These switches have five primary functions/capabilities in relation to HIPAA:

- Using VLANs, Cisco Catalyst switches allow an organization to put its ePHI 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 ePHI 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 ePHI 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 ePHI data environment and other areas of the network. As soon as any untrusted network is introduced, firewalling must be deployed.
- The Layer 3 Cisco Catalyst switch with an intrusion prevention module inspects all traffic going to and from the ePHI data environment. HIPAA Safeguard 164.308(a)(1)(i) requires policies and procedures to detect security violations. IDS is used to address wherever ePHI is present in the organization to detect for anomalous behavior of the sensitive area.

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.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the Cisco Catalyst data center switches shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - \$164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.
 - \$164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
 - §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.
 - §164.312(e)(1) Transmission Security. Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Requirements addressed include: Encryption and Integrity.
 - §164.312(e)(2)(i) Integrity Controls. Implement security measures to ensure that ePHI is not improperly modified without detection until disposed of. Requirements addressed include: Integrity.
 - §164.312(e)(2)(ii) Encryption. Implement a mechanism to encrypt ePHI whenever deemed appropriate. Requirements addressed include: Encryption.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(6)(i) Security Incident Procedures. Implement policies and procedures to address security incidents.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.

Sample Configuration

Cisco switches are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

```
aaa new-model
aaa authentication login CiscoACS 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.

```
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 {\tt CiscoACS}
```

```
line con 0
login authentication CiscoACS
line vty 0 4
login authentication CiscoACS
line vty 5 15
login authentication CiscoACS
```

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco data center switches support session timeout. It is a best practice to set the session timeout to 15 minutes, as shown below.

```
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
```

To secure authentication information and management of the Cisco data center switches, addressing Safeguard 164.308(a)(1)(i) Security Management, the Cisco data center switches management interfaces were configured to support HTTPS access, and SSH. Before crypto keys can be generated hostname and domain name must be entered:

hostname S-A2-MED-1/2 ip domain name cisco-irn.com

Generate keys with 1024 or larger bit key generation, not the default 512.

```
Crypto key generate rsa 1024
```

Configure the SSH server to use the more secure protocol version SSHv2:

```
ip ssh version 2
Configure the HTTP server to use HTTPS, and only more secure ciphers:
no ip http server
ip http secure-server
ip http secure-ciphersuite 3des-ede-cbc-sha
```

Configure the use of Secure Copy in place of TFTP

```
ip scp server enable
```

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. See Cisco ISE for more information regarding port authentication.

To address the Incident Response and Auditing HIPAA safeguards identified above, Cisco Switches can be configured to send log data to the RSA enVision log management platform. Cisco switches 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
```

And SNMP:

```
snmp-server user remoteuser remote 192.168.42.124 v3 access 88
snmp-server user remoteuser remoteuser v3
snmp-server group remoteuser v3 noauth
snmp-server trap-source Loopback0
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan
no-quest-vlan
snmp-server enable traps energywise
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps power-ethernet group 1-4
snmp-server enable traps power-ethernet police
snmp-server enable traps cpu threshold
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps errdisable
```

snmp-server enable traps mac-notification change move threshold snmp-server enable traps vlan-membership snmp-server host 192.168.42.124 remoteuser

As a best practice, 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 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 PSTDST recurring
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications 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 PHI applications and devices onto their own network and segregate them from devices that are on non-sensitive networks.

The Cisco Nexus 1000V Series Switch provides advanced networking functions and a common network management model in a virtualized server environment. The Cisco Nexus 1000V Series Switch replaces the virtual switching functionality of the VMware vCenter data center container of servers. Each server in the data center container is represented as a line card in the Cisco Nexus 1000V Series Virtual Supervisor Module (VSM) and is managed as if it were a line card in a physical Cisco switch.

Key benefits of the Nexus 1000V include the following:

- Policy-based virtual machine (VM) connectivity
- Mobile VM security and network policy
- Non-disruptive operational model for your server virtualization, and networking teams

Table 5-24 PHI HIPAA Assessment Summary—Cisco Nexus 1000V Switch

Models Assessed

Cisco Nexus 1000V version 4.2(1)SV1(4)

Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(ii)(A) Isolating Healthcare Clearinghouse Functions
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
Technical	Standards/Implementation Specifications
164.312	(a)(i) Access Control
	(b) Audit Controls
HIPAA Standards	Failed
No HIPAA stand	lards were failed.

Table 5-24 PHI HIPAA Assessment Summary—Cisco Nexus 1000V Switch

No HIPAA implementation specifications were failed.

Primary PHI Function

The primary HIPAA compliance feature of Cisco Nexus switches is secure aggregation and access layer connectivity.

- Using VLANs, Cisco Nexus switches allow an organization to put its ePHI 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 ePHI 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 ePHI 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.

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 primary 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.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the Cisco Nexus 1000V Series Switch shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
- §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
- §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
- §164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
 - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical Safeguards.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.

Sample Configuration

Cisco Nexus 1000V is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

To enable central authentication, you first 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
aaa authentication login console group CiscoACS
```

Number 7 in the key command specifies an encrypted string (key) to follow.

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 established policies for passwords. Configure the local user with encrypted passwords for fallback authentication:

username janoff password 5 <removed> role network-admin username bart 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.

To address the Incident Response and Auditing HIPAA safeguards identified above, Cisco Nexus 1000V can be configured to send its log data to the RSA enVision log management platform. 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
```

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco Nexus 1000V supports session timeout, it is a best practice to set session timeout to 15 minutes, as shown below.

```
line vty
exec-timeout 15
line console
exec-timeout 15
```

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.

```
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
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Cisco Nexus Switches—Data Center

The Cisco Nexus family of data center switches is designed to securely switch data from healthcare 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 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 5-25 PHI HIPAA Assessment Summary—Cisco Nexus Data Center Switches

Models Assessed

Cisco Nexus5020 Chassis ("40x10GE/Supervisor") version n5000-uk9.5.0.3.N1.1b.bin Cisco 7010 Chassis ("Supervisor module-1X") version n7000-s1-dk9.5.1.2.bin

HIPAA Safeguards Addressed	
Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(ii)(A) Isolating Healthcare Clearinghouse Functions
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
Technical	Standards/Implementation Specifications

164.312	(a)(i) Access Control
	(b) Audit Controls
HIPAA Standa	ards Failed
No HIPAA st	andards were failed.
HIPAA Impler	nentation Specifications Failed
No HIPAA ir	nplementation specifications were failed.

Table 5-25 PHI HIPAA Assessment Summary—Cisco Nexus Data Center Switches

Primary PHI Function

The primary HIPAA 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 ePHI 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 ePHI 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 ePHI 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.

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.

HIPAA Assessment Detail—HIPAA Safeguards Addressed.

All of the sample configurations of the Cisco Nexus data center switches shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
 - §164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
 - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.

Sample Configuration

Cisco Nexus switches are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.
To enable central authentication, you first 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 "<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
```

Number 7 in the key command specifies an encrypted string (key) to follow.

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 established policies for passwords. Configure the local user with encrypted passwords for fallback authentication:

username janoff password 5 <removed> role network-admin username bart 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.

To address the Incident Response and Auditing HIPAA Safeguards identified above, Cisco Nexus 1000v can be configured to send its log data to the RSA enVision log management platform. 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
!
! --- for implementations using VRF's ----
!
logging server 192.168.42.124 6 use-vrf servers1
aaa accounting default group CiscoACS
```

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco Nexus 1000V supports session timeout, it is a best practice to set session time-out to 15 minutes, as shown below.

```
line vty
exec-timeout 15
line console
exec-timeout 15
```

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 !
```

L

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

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Wireless

Cisco Wireless technologies provide connectivity for mobile clients within the clinic. They are designed to securely connect traditional business functions such as guest access, without increasing risk. In addition to expanding business functionality, Cisco wireless technology seamlessly provides the capability to detect rogues.

Cisco Aironet access points are designed to provide industry-leading performance to enable 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 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 5-26 PHI HIPAA Assessment Summary—Cisco Wireless Products

Models Assessed

AIR-CT5508-12-K9 version 7.0.114.112 MSE3550 version 7.0.200.125 Cisco WCS Manager version 7.0.171.107 AIR-CAP1042N AIR-CAP3502i AIR-CAP3502E AIR-LAP1262N

HIPAA Safeguar	HIPAA Safeguards Addressed				
Administrative Standards/Implementation Specifications					
164.308	(a)(1)(i) Security Management Process				
	(a)(3)(i) Authorization/Supervision				

	(a)(4)(i) Access Authorization				
	(a)(5)(i) Log-in Monitoring				
	(a)(6)(i) Security Incident Procedures				
	(a)(6)(i) Response and Reporting				
Technical	Standards/Implementation Specifications				
164.312	(a)(i) Access Control				
	(a)(2)(i) Unique User Identification				
	(a)(2)(ii) Emergency Access procedures				
	(a)(2)(ii) Automatic Logoff				
	(a)(ii)(iv) Encryption and Decryption				
	(b) Audit Controls				
	(c)(1) Data Integrity(d) Person or Entity Authentication				
	(e)(i) Transmission Security				
	(e)(2)(i) Integrity Controls				
	(e)(2)(ii) Encryption lards Failed				
HIPAA Stand					
No HIPAA s	tandards were failed.				
HIPAA Imple	mentation Specifications Failed				
No HIPAA ii	mplementation specifications were failed.				

Table 5-26 PHI HIPAA Assessment Summary—Cisco Wireless Products (continued)

Primary PHI Function

The primary ePHI function of Cisco Unified Wireless is secure connectivity and authentication of wireless clients as well as rogue device detection.

Design Considerations

Wireless technology in the PHI environment is a growing concern for organizations in the healthcare field. Implementing wireless requires that appropriate security controls are in place to prevent, detect and respond to security violations. A hacker might infiltrate a PHI environment 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 PHI environment (from the parking lot, for example) that is hard to detect. There are several methods for detecting rogue devices. Cisco Unified Wireless offers the benefit of continuous rogue detection while simultaneously passing normal wireless traffic.

Wireless technology is an untrusted network connection. Appropriate security must be is in place for wireless technology in the ePHI environment. Organizations must ensure that controls are in place to prevent unauthorized access. Appropriate controls include a firewall to segment and protect the PHI data environment and intrusion detection services to identify potential intrusion attempts to the secured network. 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 should be denied.

When implementing wireless in an ePHI environment, encryption must be configured to adequately protect ePHI transmitted over the wireless medium. Today the minimum level of encryption deemed acceptable by auditors is WPA2.

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

HIPAA Assessment Detail—HIPAA Safeguards Addressed

All of the sample configurations of the Cisco Wireless technologies shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a healthcare clearinghouse
 is part of a larger organization, the clearinghouse must implement policies and procedures that
 protect the electronic protected health information of the clearinghouse from unauthorized
 access by the larger organization. Requirements addressed include: Access Control, Integrity,
 Incident Response, and Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
 - §164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and
 procedures that, based upon the covered entity's or the business associate's access authorization
 policies, establish, document, review, and modify a user's right of access to a workstation,
 transaction, program, or process. Requirements addressed include: Access Control, Incident
 Response, and Auditing.
 - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
 - §164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.
 - §164.308(a)(5)(ii)(D) Password Management. Procedures for creating, changing, and safeguarding passwords. Requirements addressed include: Access Control and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.

- §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.
- \$164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Requirements addressed include: Access Control, Incident Response, and Auditing.
- §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- §164.312(a)(2)(ii) Emergency Access Procedure. Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
- §164.312(e)(1) Transmission Security. Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Requirements addressed include: Encryption and Integrity.
- §164.308(e)(2)(i) Integrity Controls. Implement security measures to ensure that ePHI is not improperly modified without detection until disposed of. Requirements addressed include: Integrity.
- §164.308(e)(2)(ii) Encryption. Implement a mechanism to encrypt ePHI whenever deemed appropriate. Requirements addressed include: Encryption.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
 - §164.312(a)(2)(i) Unique User Identification. Assign a unique name and/or number for identifying and tracking user identity. Requirements addressed include: Access Control and Auditing.
 - \$164.312(a)(2)(ii) Automatic logoff. Implement electronic procedures that terminate an
 electronic session after a predetermined time of inactivity. Requirements addressed include:
 Access Control and Auditing.
- Encryption—Implement mechanisms to encrypt and decrypt ePHI.
 - §164.312(a)(ii)(iv) Encryption and Decryption. Implement a mechanism to encrypt and decrypt electronic protected health information. Requirements addressed include: Encryption and Integrity.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
 - §164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.

L

Sample Configuration

Cisco WCS is designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

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.

For network security, the Cisco solution uses profiles for appropriate access where a user is assigned to the profile, and user access can be restricted as shown in Figure 5-101 and Figure 5-102.

Figure 5-101 Local Management Users Screen

ာါကျက cisco	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	Local Ma User Nam Password Confirm F User Acce	Password	nt Users > Nev	Only V Only		
Logs Mgmt Via Wireless						

Figure 5-102 Management Via Wireless Screen

.ılı.ılı. cısco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT
Management	Managem	nent Via	Wireless			
Summary SNMP HTTP-HTTPS Telnet-SSH Serial Port Local Management Users User Sessions	Enable Co	ontroller Ma	anagement to be a	ccessible from	Wireless Clier	nts
Logs Mgmt Via Wireless						

Cisco WCS is configured to use TACACS+ for authentication of administrators, as shown in Figure 5-103.

290932

200031



Figure 5-103 WCS Manager AAA Authentication Mode

The authentication servers for TACACS+ in WCS Manager are configured as shown in Figure 5-104.

	192.168.43.135/webacs/tACACS5erverGeneralAction.do?command=detail8subl 🏫 👻 😋 😫	
Most Visited Cisco UCS Manager	UIM NCM WCS TACACS R5A enVision HyTrust CM-2 R5A-4	<ip. mac="" name,="" ssid,=""> Search Advanced Search Saved Search User: <u>bmcqloth</u> @ Virtual Domain: root ▼</ip.>
 Monitor ▼ <u>Reports</u> ▼ <u>Con</u> Change Password Local Password Policy 	igure ▼ Services ▼ Administration ▼ Tools ▼ Help ▼ TACACS+ Server Detail : 192.168.42.131 Administration > AAA > TACACS> > TACACS+ Server Detail	🅜 tੇ 🖺 Logout
AAA Mode Users Groups	Port 49	
Active Sessions TACACS+	Shared Secret Format ASCII 💌 Shared Secret	
RADIUS	Retransmit Timeout 5 (secs) Retries 1 Authentication Type PAP x Locel Interface IP 192.168.43.135 x	
	Submit Cancel	

Figure 5-104 WCS Manager TACACS+ Server Configuration

The citations in this section were addressed with the sample configuration at the end of this section.

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 established policies for passwords. Local user accounts on Cisco WCS Manager and controllers require a password.

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of Automatic logoff options. Cisco WCS supports session policies under the management tab. It is a best practice to change the session timeout to 15 minutes, as shown in Figure 5-105.

- 🗆 × Cisco WCS - Configure Controllers - 192.168... + 🗲) P **Feedback** Cisco UCS Manager UIM NCM WCS TACACS RSA enVision HyTrust CM-2 RSA-AM 👑 V50M 🔝 Bookm Wireless Control Syster Search սիսիս 73 -Alarm 🔺 40 8 CISCO User: bmcgloth @ Virtual Domain: root 🕜 관 📇 Logout 🚡 Monitor Telnet SSH : Properties € Controllers > 192.168.43.21 > Management Telpet SSH System ۲ WLANs € **Telnet SSH Configuration** H-REAP ۲ Template Applied (None) Security ۲ Session Timeout 15 Access Points • Б Maximum Sessions 1 802.11 ۲ Allow New Telnet Sessions No 🔽 Allow New SSH Sessions Yes -802.11a/r • 802.11b/g/ Save Audit ۲ Mesh Ð Footnotes Setting 0 value for "Maximum Sessions' parameter will cause the CLI session to terminate immediately if logging in using SSH. Ports Management • Trap Receiver: Trap Control Telnet SSH Multiple Syslog 📄 Web Admin Local Management User Authentication Priority

Figure 5-105 Controller Secure Management for SSH

The Cisco WLAN performs 24-hour scanning to immediately detect and contain unauthorized and rogue wireless devices addressing safeguard 164.308(a)(1)(i) Security Management. Threats to network security can occur in between regularly scheduled 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 wireless 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 5-106 and Figure 5-107.)

291607

،، ،،، ،، cısco	<u>M</u> onitor <u>w</u> l	ANs <u>C</u> ON	TROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	Sa <u>v</u> e Conf C <u>O</u> MMANDS
Security AAA General Authentication Accounting Fallback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients	AP Policies Policy Configu Accept Self Sig Accept Manufa Accept Local S Authorize MIC	gned Certifica ctured Instal ignificant Ce APs against	led Certific rtificate (LS auth-list or	C)			
User Login Policies AP Policies Password Policies Local EAP	Authorize LSC		auth-list			Entr	ies 0 - 0 of 0
 Priority Order Certificate Access Control Lists Wireless Protection Policies 	Search by MAC	Certificat Type		Search	1		
 Web Auth Advanced 							

Figure 5-106 Security—AP Policies Screen

Figure 5-107 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	

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 5-108.)

290946

	tification 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	

Figure 5-108 Notification Receiver Screen

Cisco offers Control and Provisioning of Wireless Access Points (CAPWAP)-compliant DTLS encryption to provide full-line-rate encryption between access points and controllers across remote WAN/LAN links (see Figure 5-109). 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 5-109 CAPWAP with DTLS

(WiSM-slot3-1) >show sysinfo	
Product Version Indicates CAPWAP . Bootloader Version with DTLS .	Cisco Controller 7.0.116.0 1.0.7 1.0.0 FPGA 1.6, Env 0.0, USB console
Build Type	DATA + WPS

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 5-110.)

Figure 5-110 WLAN Information

						ntries 1 - 4 of 4
WLAN ID	Profile_Name	SSID	WLAN/Guest/Remote LAN	Security Policies	<u>Status</u>	Task List
<u>3</u>	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 4

The citations in this section were addressed with the sample configuration at the end of this section.

To address the Incident Response and Auditing HIPAA Safeguards identified above, the Cisco Unified Wireless system is designed to track and monitor all administrative user access and events. Cisco Unified Wireless tracks individual administrator actions through several mechanisms including AAA, logging, and system events.

Figure 5-111 shows the configuration of local logging settings, and Figure 5-112 shows the syslog server configuration used to send logs to RSA enVision.

Figure 5-111 Local Logging Configuration



Firefox 🔻	
Cisco WCS - Syslog Configuration -	
() 192.168.43.135 http	ps://192.168.43.135/webacs/Logging5yslogAction.do?command=init&subMenuBitMa 👚 - C 🔣 - Google 🔊 🍙 Feedback -
Most Visited Cisco UCS Manag	
Alarm Summary	Advanced Search Saved Search
	User: <u>bmcqloth</u> @ Virtual Domain: root 🗡 Configure • Services • Administration • Tools • Help •
	Configure ▼ Services ▼ Administration ▼ Tools ▼ Help ▼
General Logging 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
	Jave
	<u> </u>

Figure 5-112 WCS Manager Syslog Configuration

As a best practice, 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.

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 5-113.

192.168.43.135 http	s://192.168.43	3.135/webacs/ntpServerGeneralAction.do?comma	nd=list&controllerIc 🚖 🛛 C) 🚼 - Google	P 🟫 Feedback
Most Visited 📄 Cisco UCS Manage	er 🗋 UIM 🗌	NCM 📄 WCS 📄 TACACS 📄 RSA enVisi	on 📄 HyTrust 📄 CM-2 📄 R5A-AM 🚟 VSOM	🔝 Bookmar
Alarm Summary 🔍	4	0 73 08 7	Wireless Control System	<ip,name,ssid,mac> Search</ip,name,ssid,mac>
ISCO				dvanced Search Saved Search
	~			oth @ Virtual Domain: root 🔻
		Services • Administration • Tools •	Help ▼	😢 🤂 📇 Logout
Properties		etwork Time Protocol nfigure > Controllers > 192.168.43.21 > Syster	n > Network Time Protocol	Select a command 💌 🗔
System	•	<u></u>		
📄 General				Entries 1 - 2 of 2
Commands				
Interfaces		Server Index	Server Address	
Interface Groups			192.168.62.161	
Network Route			192.168.62.162	
Mobility Groups			192.100.02.102	Entries 1 - 2 of 2
Network Time Protocol				
QoS Profiles				
DHCP Scopes				
User Roles				
AP Username Password				
Global CDP Configuration				
AP 802.1X Supplicant Cr				
DHCP				
Multicast				
AP Timers	۲			
H-REAP	۲			
Security	۲			
Access Points	Ð			

Figure 5-113 NTP Servers Screen for Controllers

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications 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 Assessed

	apervisor/Fabric-2") version m9500-sf2ek9-mzg.5.0.1a.bin.S4 apervisor/Fabric-2") version m9500-sf2ek9-mz.5.0.4.bin
HIPAA Safeguards Addressed	
Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(4)(i) Access Authorization
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
Technical	Standards/Implementation Specifications
164.312	(a)(i) Access Control
	(a)(2)(iv) Encryption and Decryption
	(b) Audit Controls
	(c)(1) Data Integrity
HIPAA Standard	ls Failed
No HIPAA stan	dards were failed.
HIPAA Implementation Specifications Failed	
No HIPAA implementation specifications were failed.	

Table 5-27 PHI HIPAA Assessment Summary – Cisco MDS Storage Switches

Primary PHI Function

The primary function of Cisco MDS storage switches is to securely encrypt ePHI data at rest as it passes from server to storage. This safeguard was met using the MDS configuration to implement encryption for ePHI data in storage to prevent unauthorized access and prevent unauthorized modification to the ePHI data. Logs can be used to monitor access attempts to ePHI data in storage.

Design Considerations

Cisco MDS 9000 Family security features such as VSANs, advanced zoning, fabric binding, port security, Fiber 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 MDS 9500s were configured for zoning and LUN masking to secure the logical partitioning of disk used for storing ePHI 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

HIPAA Assessment Detail—HIPAA Safeguards Passed

All of the sample configurations of the Cisco MDS storage switches shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
 - §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
 - §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.

Sample Configuration

Cisco MDS storage switches are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

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
```

L

```
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*.

Assignment of privileges to individuals based on job classification and function is accomplished with the following configuration:

```
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)
```

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 established policies for passwords.

username bmcgloth password 5 <removed> role network-admin username bart password 5 <removed> role network-admin

HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options. Cisco MDS supports session timeout configuration in the CLI. It is a best practice to set the session timeout to 15 minutes, as shown below.

line vty exec-timeout 15 line console exec-timeout 15

To secure authentication information and management of the Cisco MDS Switch, addressing Safeguard 164.308(a)(1)(i) Security Management, the management intercedes are configured to support only encrypted access using the following configurations:

```
Configure terminal
feature ssh
ssh key dsa or ssh key rsa <768-2048>
no feature telnet
no feature http-server
```

And access to the management interface is restricted with an access list.

Secure access to the management port as follows:

```
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 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
```

To address the Incident Response and Auditing HIPAA safeguards identified above, 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 and SNMP traps offers detailed entries and can be redirected to the RSA enVision log server to consolidate IT infrastructure monitoring information. Note that the log never contains application data. Cisco MDS is designed to track and monitor all administrative user access and events.

Logs stored locally are buffered and require operator level privileges to be viewed. External logging and SNMP traps are enabled by implementing the following configuration statements:

```
logging server 192.168.42.124 6
snmp-server host 192.168.41.101 traps version 2c public udp-port 2162
snmp-server host 192.168.42.121 traps version 3 auth public
```

A central logging repository, RSA enVision, collects syslog and SNMP information from all devices to ensure the integrity and correlation of events.

As a best practice, 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
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.

Security

Cisco ASA Firewalls

The Cisco Adaptive Security Appliance (ASA) is designed to provide secure segmentation within a network. The stateful firewall and modular intrusion detection modules enable the healthcare entity to securely connect public networks to the PHI environment. The ASA also enables secure connectivity from remote locations via encrypted tunnels using its VPN technology.

The Cisco ASA 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 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 investment protection provided by the Cisco ASA 5500 Series and allowing businesses to adapt their network defenses to new threats as they arise.

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.

All Cisco ASA 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 provides highly customizable, granular network access tailored to meet the requirements of diverse deployment environments, while providing advanced endpoint and network-level security.

Models Assess	sed
Cisco ASA551	5-X w/vIPS Module version asa900-129-smp-k8.bin and IDS version 7.1(6)
Cisco ASA555	5-X w/vIPS module version asa900-129-smp-k8.bin and IPS version 7.1(6)E4
Cisco ASA558	35-S60-2A-K9 asa901-smp-k8.bin
Cisco ASA Se	rvice Module WS-SVC-ASA-SM1 version asa851-smp-k8.bin
HIPAA Safegua	ards Addressed
Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(1)(ii)(D) Information System Activity Review
	(a)(3)(ii)(A) Authorization/Supervision
	(a)(4)(ii)(A) Isolating Healthcare Clearinghouse Function
	(a)(4)(ii)(B) Access Authorization
	(a)(4)(ii)(C) Access Est./Modification
	(a)(5)(ii)(C) Log-in Monitoring
	(a)(6)(ii) Response and Reporting
Technical	Standards/Implementation Specifications
164.312	(a)(1) Access Control
	(a)(2)(i) Unique User Identification
	(a)(2)(ii) Emergency Access procedures
	(a)(2)(ii) Automatic Logoff
	(a)(ii)(iv) Encryption and Decryption
	(b) Audit Controls
	(c)(1) Data Integrity
	(d) Person or Entity Authentication
	(e)(1) Transmission Security
	(e)(2)(i) Integrity Controls
	(e)(2)(ii) Encryption
HIPAA Standar	ds Failed
No HIPAA sta	ndards were failed.
HIPAA Implem	entation Specifications Failed
No HIPAA imp	plementation specifications were failed.

Table 5-28 PHI HIPAA Assessment Summary—Cisco ASA

Primary PHI Function

The primary function of the Cisco ASA firewall in a healthcare network environment is to securely segment PHI data environments to prevent unauthorized access from public and business associate networks at clinics, hospitals, clearinghouses and to provide intrusion detection capabilities. Additionally, the firewall can provide the isolation necessary for organizations with clearing house functions to protect against unauthorized access to the clearing house from the larger organization.

Design Considerations

- Select the appropriate Cisco ASA model/SSM module for the traffic needs in the healthcare entity.
- Configure security policies, objects, and rules centrally with Cisco Security Manager to support segmentation of the LAN from Internet exposure, implement restrictions based on identity and authorization to access ePHI, and set up logging and monitoring alerts for central capture and auditing.
- 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.
- Allow only SSHv2 (and not Telnet or SSHv1) connection from network management station to Cisco ASA.
- Configure appropriate banner messages on login, incoming, and exec modes of the Cisco ASA. The login banner warning should not reveal the identity of the company that owns or manages the Cisco ASA. 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 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 connectivity or Cisco Secure ACS failure.
- Change default passwords and community strings to appropriate complexity.
- 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 ASA.
- For Internet edge, disable **icmp permit** on the outside interface of Cisco ASA. 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.

HIPAA Assessment Detail—HIPAA Safeguards Addressed

HIPAA safeguards are spread across multiple categories. The ASA firewall helps healthcare-covered entities and business associates meet access control safeguards in the Administrative and Technical categories. The access control can be applied to both internal and external users that access ePHI data. Additionally, controls to protect the administrator accounts on the firewall have been implemented to protect the firewall from unauthorized modification if the authentication server fails. These local accounts represent only a subset of select individuals that would need access in the event central authentications services are unavailable.

All of the sample configurations of the ASA shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - 164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - 164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a health care clearinghouse
 is part of a larger organization, the clearinghouse must implement policies and procedures that
 protect the electronic protected health information of the clearinghouse from unauthorized
 access by the larger organization. Requirements addressed include: Access Control, Integrity,
 Incident Response, and Auditing.

- 164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
- 164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Requirements addressed include: Access Control, Incident Response, and Auditing.
- 164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4).
- 164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.
- 164.308(a)(5)(ii)(D) Password Management. Procedures for creating, changing, and safeguarding passwords. Requirements addressed include: Access Control and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
 - 164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.
 - 164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Requirements addressed include: Access Control, Incident Response, and Auditing.
 - 164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
 - 164.312(a)(2)(ii) Emergency Access Procedure. Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
 - 164.312(e)(1) Transmission Security. Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Requirements addressed include: Encryption and Integrity.
 - 164.308(e)(2)(i) Integrity Controls. Implement security measures to ensure that ePHI is not improperly modified without detection until disposed of. Requirements addressed include: Integrity.
 - 164.308(e)(2)(ii) Encryption. Implement a mechanism to encrypt ePHI whenever deemed appropriate. Requirements addressed include: Encryption.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - 164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
 - 164.312(a)(2)(i) Unique User Identification. Assign a unique name and/or number for identifying and tracking user identity. Requirements addressed include: Access Control and Auditing.

L

- 164.312(a)(2)(ii) Automatic logoff. Implement electronic procedures that terminate an
 electronic session after a predetermined time of inactivity. Requirements addressed include:
 Access Control and Auditing.
- Encryption—Implement mechanisms to encrypt and decrypt ePHI.
 - 164.312(a)(ii)(iv) Encryption and Decryption. Implement a mechanism to encrypt and decrypt electronic protected health information. Requirements addressed include: Encryption and Integrity.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - 164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.
 - 164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
 - 164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.

Sample Configuration

Cisco ASA firewalls are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

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 *Oncology*, 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 CiscoACS protocol tacacs+
aaa-server CiscoACS (inside) host 192.168.42.131
key *****
user-identity default-domain LOCAL
aaa accounting ssh console CiscoACS
aaa accounting enable console CiscoACS
aaa accounting command privilege 15 CiscoACS
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 established policies for passwords.

```
username csmadmin password <removed> encrypted privilege 15
username janoff password <removed> encrypted privilege 15
username bart password <removed> encrypted privilege 15
```

It is a best practice that these local accounts represent only a subset of key network or security device administrators that would need administrative access in the event central authentications services are unavailable. This should not be the complete list of users that require access to ePHI.

These AAA authentication groups are assigned to the administrative interfaces where users connect.

```
aaa authentication ssh console CiscoACS LOCAL
aaa authentication enable console CiscoACS LOCAL
aaa authentication http console CiscoACS LOCAL
```

Cisco ASA firewalls are configurable to restrict traffic through the use of object and service-based access lists, thereby addressing Safeguard 164.308(a)(4)(ii)(A), which requires isolating healthcare information. By default, the firewall does not forward any traffic unless explicitly permitted.

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 outside
nameif north
bridge-group 1
security-level 0
1
interface inside
nameif south
bridge-group 1
security-level 100
! ----Defining Objects and Object Groups----
Т
object-group network EMC-NCM
description EMC Network Configuration Manager
network-object 192.168.42.122 255.255.255.255
object-group network CSManager
description Cisco Security Manager
network-object 192.168.42.133 255.255.255.255
object-group network RSA-enVision
description RSA EnVision Syslog collector and SIM
network-object 192.168.42.124 255.255.255.255
object-group network AdminStation3
network-object 192.168.42.138 255.255.255.255
object-group network Admin-Systems
group-object EMC-NCM
group-object AdminStation
group-object AdminStation2
group-object CSManager
group-object RSA-enVision
group-object AdminStation3
group-object AdminStation4-bart
object-group service CSM_INLINE_svc_rule_77309411635
description Generated by CS-Manager from service of FirewallRule# 3
(ASA-DC-1-vdc1_v1/mandatory)
service-object tcp destination eq ssh
service-object tcp destination eq https
group-object HTTPS-8443
I
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
!
```

L

```
! ----One line of the larger access-list permitting traffic----
!
access-list CSM_FW_ACL_south extended permit object-group
CSM_INLINE_svc_rule_77309411635 object-group Admin-Systems object-group
CSM_INLINE_dst_rule_77309411635
!
! ----Applying the access-list to an interface----
!
access-group CSM_FW_ACL_south in interface south
```

Administration access to the firewall is further restricted through the use of network permit statements applied to the web and terminal interfaces. Isolating administrative access to this device enforces the perimeter of the ePHI scope of the infrastructure.

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
```

It is a recommended practice to enable only management interface protocols that use strong encryption, to best protect the ePHI information and the identities and passwords of those who must have 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>

VPNs enable secure communication between locations by encrypting and decrypting traffic addressing Safeguard 164.312(a)(ii)(iv).

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 HEALTH-HIPAA internal
group-policy HEALTH-HIPAA 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 ComplianceLab type remote-access
tunnel-group ComplianceLab general-attributes
authentication-server-group partnerauth LOCAL
default-group-policy HEALTH-HIPAA
```

Cisco ASA firewalls track individual administrator actions, which address all of the HIPAA Auditing safeguards summarized above, 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

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
```

In addition to being able to set timeout limits for remote access VPNs, Safeguard 164.312(a)(2)(ii) Automatic Logoff, requires that the administrative sessions to the Cisco ASA firewalls be limited with the following configurations:

```
http server idle-timeout 15
ssh timeout 15
console timeout 15
```

As a best practice, 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. Cisco ASA firewalls use NTP 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
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002 and NIST Security Publications.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications 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 ePHI 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 enabling administrative segregation to meet regulatory and audit requirements and reduce administrative errors.

Table 5-29 PHI HIPAA Assessment Summary – Cisco Virtual Security Gateway

Models Assessed	
Nexus VSG versi	on 4.2(1)VSG1(1)
HIPAA Safeguards	Addressed
Administrative	Standards/Implementation Specifications

164.308	(a)(1)(i) Security Management Process
	(a)(1)(ii)(D) Information System Activity Review
	(a)(3)(i) Authorization/Supervision
	(a)(4)(ii)(A) Isolating health care clearinghouse function
	(a)(4)(i) Access Authorization
	(a)(4)(ii)(C) Access Est./Modification
	(a)(5)(i) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
	(a)(6)(i) Response and Reporting
Technical	Standards/Implementation Specifications
164.312	(a)(i) Access Control
	(a)(2)(i) Unique User Identification
	(a)(2)(ii) Emergency Access procedures
	(a)(2)(ii) Automatic Logoff
	(a)(ii)(iv) Encryption and Decryption
	(b) Audit Controls
	(c)(1) Data Integrity
	(d) Person or Entity Authentication
	(e)(i) Transmission Security
	(e)(2)(i) Integrity Controls
	(e)(2)(ii) Encryption
HIPAA Standar	ds Failed
No HIPAA star	ndards were failed.
HIPAA Impleme	entation Specifications Failed
No HIPAA imp	elementation specifications were failed.

Table 5-29 PHI HIPAA Assessment Summary—Cisco Virtual Security Gateway (continued)

Primary PHI Function

The primary function of the Cisco VSG is segmentation of PHI 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.

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. (See Figure 5-114.)



Figure 5-114 Cisco Nexus VSG System Architecture

HIPAA Assessment Detail—HIPAA Safeguards Addressed

HIPAA safeguards are spread across multiple categories. The VSG firewall helps healthcare covered entities and business associates meet access control safeguards in the Administrative and Technical categories. The access control can be applied to both internal and external users that access ePHI data. Additionally, controls to protect the administrator accounts on the firewall have been implemented to protect the firewall from unauthorized modification if the authentication server fails. These local accounts represent only a subset of select individuals that would need access in the event central authentications services are unavailable.

All of the sample configurations of the VSG shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(4)(ii)(A) Isolating healthcare clearinghouse function. If a healthcare clearinghouse
 is part of a larger organization, the clearinghouse must implement policies and procedures that
 protect the electronic protected health information of the clearinghouse from unauthorized
 access by the larger organization. Requirements addressed include: Access Control, Integrity,
 Incident Response, and Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.

- §164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Requirements addressed include: Access Control, Incident Response and Auditing.
- §164.312(a)(1) Access Control. Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).
- §164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.
- §164.308(a)(5)(ii)(D) Password Management. Procedures for creating, changing, and safeguarding passwords. Requirements addressed include: Access Control and Auditing.
- Integrity—Protect electronic protected health information from improper alteration or destruction as required by HIPAA Technical safeguards.
 - §164.312(c)(1) Data Integrity. Implement policies and procedures to protect health information from improper alteration or destruction.
 - §164.308(a)(4)(ii)(C) Access Establishment and Modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Requirements addressed include: Access Control, Incident Response, and Auditing.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
 - \$164.312(a)(2)(ii) Emergency Access Procedure. Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
 - §164.312(e)(1) Transmission Security. Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Requirements addressed include: Encryption and Integrity.
 - \$164.308(e)(2)(i) Integrity Controls. Implement security measures to ensure that ePHI is not improperly modified without detection until disposed of. Requirements addressed include: Integrity.
 - §164.308(e)(2)(ii) Encryption. Implement a mechanism to encrypt ePHI whenever deemed appropriate. Requirements addressed include: Encryption.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
 - §164.312(a)(2)(i) Unique User Identification. Assign a unique name and/or number for identifying and tracking user identity. Requirements addressed include: Access Control and Auditing.
 - §164.312(a)(2)(ii) Automatic logoff. Implement electronic procedures that terminate an
 electronic session after a predetermined time of inactivity. Requirements addressed include:
 Access Control and Auditing.

L

- Encryption—Implement mechanisms to encrypt and decrypt ePHI.
 - §164.312(a)(ii)(iv) Encryption and Decryption. Implement a mechanism to encrypt and decrypt electronic protected health information. Requirements addressed include: Encryption and Integrity.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
 - §164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Requirements addressed include: Access Control and Auditing.

Sample Configuration

Cisco VSG firewalls are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

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.

 In the Navigation pane, select the Roles node. In the Work pane, click Create Roles (see Figure 5-115.)



Figure 5-115 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 5-116.)





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
HIPAA Safeguard 164.312(a)(2)(ii) requires the enabling of automatic logoff options.
Cisco VSG supports session timeout. It is a best practice to set session time-out to
15 minutes,
line vty
exec-timeout 15
```

exec-timeout 15 line console exec-timeout 15

It is a recommended practice to only enable management interface protocols which use strong encryption in order to best protect the ePHI information and the identities and passwords of those who must have access. Cisco VSG firewalls support strong encryption for SSH and HTTPS. 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.

Cisco ASA firewalls track individual administrator actions, which address all of the HIPAA Auditing Safeguards summarized above, through several mechanisms including AAA, logging, and system events by implementing the following syslog server configurations 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 5-117.

Figure 5-117 Configuring Syslog

Tenant Management Resource Manager	ment Policy Management Administration
Security Policies Device Policies Capat	bilities Diagnostics
Device Configuration Solution	🥗 root 🕨 🙏 Niners 🕨 🎜 Policies 🕨
S Policies	Syslog Policies
Cisco	General Faults
w M Niners ↓ S Policies	Add Syslog
Fault	Name Win7_Syslog
⊨ S Log File	
Syslog Policies	
Win7_Syslog	
A. Raiders	8

2. The severity of the logging should be at level 6 to capture the firewall policy hit in the VSG. (See Figure 5-118).

Figure 5-118 Configuring Logging Severity

Add Syslog S	erver	0
Server Type: Hostname / IP Address: Severity: Forwarding Facility: Admin State:	primary 10.29.172.53 information (6) Iocal0 enabled	
	OK Cance	Т торе

3. The syslog policy is attached to the Device Profile to enable the settings in the VSG. CLI configuration of logging services is as follows:

```
logging logfile messages 2
logging server 192.168.42.124 6 facility local0
logging monitor 2
```

As a best practice, 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 5-119.

Figure 5-119 Configuring NTP

DNS Servers		NTP Servers	
Add DNS Server	🏫 Up 🔸 Down	Add NTP Server	n Up 🔸 Dowr

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications 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 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 ability 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 ability to detect and stop the broadest range of malicious traffic before it affects business continuity.

Models Assesse	ed
WS-SVC-IDSM	1-2 version 7.0(4)
HIPAA Safeguar	rds Addressed
Administrative	Standards/Implementation Specifications
164.308	(a)(1)(i) Security Management Process
	(a)(3)(i) Authorization/Supervision
	(a)(4)(i) Access Authorization
	(a)(5)(ii)(B) Protection from Malicious Software
	(a)(5)(ii)(C) Log-in Monitoring
	(a)(6)(i) Security Incident Procedures
	(a)(6)(i) Response and Reporting
Technical	Standards/Implementation Specifications
164.312	(a)(i) Access Control
	(b) Audit Controls
HIPAA Standard	ls Failed
No HIPAA stan	dards were failed.
HIPAA Impleme	ntation Specifications Failed
No HIPAA imp	lementation specifications were failed.

Table 5-30 PHI HIPAA Assessment Summary – Cisco IDSM2

Primary PHI Function

The primary function of the Cisco IDSM2 is to monitor all traffic at the perimeter of the ePHI data environment as well as at critical points inside of the ePHI data environment, and alert personnel to suspected compromises.

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 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

HIPAA Assessment Detail—HIPAA Safeguards Passed

All of the sample configurations of the IDSM shown below were used to meet the following list of satisfied controls:

- Access Control—Restrict access to ePHI data as required by HIPAA Administrative and Technical safeguards
 - §164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements addressed include: Access Control, Integrity, Incident Response, and Auditing.
 - §164.308(a)(3)(ii)(A) Authorization/Supervision. Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed. Requirements addressed include: Auditing.
 - §164.308(a)(4)(ii)(B) Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Requirements addressed include: Access Control and Auditing.
 - \$164.308(a)(5)(ii)(B) Protection from malicious software. Procedures for guarding against, detecting, and reporting malicious software. Requirements addressed include: Incident Response and Auditing.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.
- Incident response—Implement security incident response as required by HIPAA Administrative safeguards.
 - §164.308(a)(6)(i) Security Incident Procedures. Implement policies and procedures to address security incidents. Requirements addressed include: Incident Response and Auditing.

- §164.308(a)(6)(ii) Response and Reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. Requirements addressed include: Incident Response and Auditing.
- Auditing—Implement mechanisms to record and examine activity in systems that contain or use ePHI as required by HIPAA Technical safeguards.
 - §164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that
 record and examine activity in information systems that contain or use electronic protected
 health information. Requirements addressed include: Auditing.
 - §164.308(a)(5)(ii)(C) Log-in Monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Requirements addressed include: Access Control and Auditing.

Sample Configuration

Cisco IDSM modules are designed to track and monitor all administrative user access and events, thereby addressing all of the safeguards listed under Access Control above. User access throughout the solution uses a centralized user database in the Active Directory, which is linked through authentication servers via LDAP, RADIUS, and TACACS+ services, enabling verification of users and administrators of devices and endpoints. These services are located in the data center. Individual user IDs are assigned, and roles are based on group membership.

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 and 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
! ------
```

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.

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 established policies for passwords.

Cisco IDSM2 modules support the ability to specify a minimum password length for local accounts.

```
! ------
service authentication
password-strength
size 7-64
! -----
```

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
! -----
```

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
! ------
```

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
! -----
```

Cisco IDSM2 modules support the ability to lockout local accounts after the specified number of failed attempts, requiring an administrator to re-enable them. Locked accounts are indicated by parentheses when using the show users command:

```
sensor# show users all
CLI ID User Privilege
* 1349 bart administrator
5824 (pauljones) viewer
9802 christian operator
```

Cisco IDSM2 modules are capable of performing intrusion detection and prevention through the use of VLAN interfaces from the host Cisco Catalyst service chassis addressing safeguard 164.308(a)(1)(i) Security Management. 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:

Т

To address the Incident Response and Auditing HIPAA Safeguards identified above, Cisco IDSM can be configured to send its log data to the RSA enVision log management platform. RSA enVision collects information from all devices to ensure the integrity and correlation of events.

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
' -----
```

As a best practice, 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
```

Clock synchronization is a requirement for common industry security frameworks such as the HiTrust Common Security Framework (CSF), ISO 27002, and NIST Security Publications, as well as other industry-based standards.

HIPAA Standards Failed

No HIPAA standards were failed.

HIPAA Implementation Specifications Failed

No HIPAA implementation specifications were failed.