NIST CYBERSECURITY PRACTICE GUIDE HEALTH IT

SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES

How-To Guides

For Security Engineers

Gavin O'Brien

Brett Pleasant

Colin Bowers

Sue Wang

Kangmin Zheng

Kyle Kamke

Nate Lesser

Leah Kauffman, Editor-in-Chief

NIST SPECIAL PUBLICATION 1800-1c

DRAFT

NIST Special Publication 1800-1c

SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES

Health IT Sector

DRAFT

Gavin O'Brien
Nate Lesser
National Cybersecurity Center of Excellence
Information Technology Laboratory

Brett Pleasant
Sue Wang
Kangmin Zheng
The MITRE Corporation
McLean, VA

Colin Bowers
Kyle Kamke
Ramparts, LLC
Clarksville, MD

Leah Kauffman, Editor-in-Chief
National Cybersecurity Center of Excellence
Information Technology Laboratory

July 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-1c
Natl. Inst. Stand. Technol. Spec. Publ. 1800-1c, 82 pages (July 2015)
CODEN: NSPUE2

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov.

Comments on this publication may be submitted to: HIT_NCCoE@nist.gov

Public comment period: July 22, 2015 through September 25, 2015

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
9600 Gudelsky Drive (Mail Stop 2002) Rockville, MD 20850
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable. The center's work results in publicly available NIST Cybersecurity Practice Guides, Special Publication Series 1800, that provide users with the materials lists, configuration files, and other information they need to adopt a similar approach.

To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them more easily align with relevant standards and best practices.

The documents in this series describe example implementations of cybersecurity practices that may be voluntarily adopted by businesses and other organizations. The documents in this series do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

Health care providers increasingly use mobile devices to receive, store, process, and transmit patient clinical information. According to our own risk analysis, discussed here, and in the experience of many health care providers, mobile devices can present vulnerabilities in a health care organization's networks. At the 2012 Health and Human Services Mobile Devices Roundtable, participants stressed that mobile devices are being used by many providers for health care delivery before they have implemented safeguards for privacy and security.[*]

This NIST Cybersecurity Practice Guide provides a modular, open, end-to-end reference design that can be tailored and implemented by health care organizations of varying sizes and information technology sophistication. Specifically, the guide shows how health care providers, using open source and commercially available tools and technologies that are consistent with cybersecurity standards, can more securely share patient information among caregivers using

[*] Mobile Devices Roundtable: Safeguarding Health Information Real World Usages and Safeguarding Health Information Real World Usages and Real World Privacy & Security Practices, March 16, 2012, U.S. Department of Health & Human Services

mobile devices. The scenario considered is that of a hypothetical primary care physician using her mobile device to perform reoccurring activities such as sending a referral (e.g., clinical information) to another physician, or sending an electronic prescription to a pharmacy. While the design was demonstrated with a certain suite of products, the guide does not endorse these products in particular. Instead, it presents the characteristics and capabilities that an organization's security experts can use to identify similar standards-based products that can be integrated quickly and cost-effectively with a health care provider's existing tools and infrastructure.

KEYWORDS

implement standards-based cybersecurity technologies; mobile device security standards; HIPAA; electronic health record system; risk management; electronic health record security; breaches of patient health information; stolen medical information; stolen health records

ACKNOWLEDGEMENTS

We gratefully acknowledge the contributions of the following individuals and organizations for their generous contributions of expertise, time, and products.

Name	Organization
Curt Barker	NIST
Doug Bogia	Intel
Robert Bruce	Medtech Enginuity
Lisa Carnahan	NIST
Verbus Counts	Medtech Enginuity
Sallie Edwards	MITRE
David Low	RSA
Adam Madlin	Symantec
Mita Majethia	RSA
Peter Romness	Cisco
Steve Schmalz	RSA
Ben Smith	RSA
Matthew Taylor	Intel
Steve Taylor	Intel
Jeff Ward	IBM (Fiberlink)
Vicki Zagaria	Intel

Table of Contents

Disclaimer ii
National Cybersecurity Center of Excellence iii
NIST Cybersecurity Practice Guides iii
Abstract iii
Keywords iv
Acknowledgements v
List of Figures vii
List of Tables vii
1 Practice Guide Structure 1
2 Introduction 1
3 Basic Network Infrastructure Services 2
3.1 Hostnames 2
3.2 Bind DNS and DNSE Installation and Hardening 4
3.3 Access Point: Cisco RV220W 10
3.4 Firewalls: IPTables 13
4 Backup 15
4.1 URBackup 15
5 Configuration Management 20
5.1 Puppet Setup 21
5.2 Puppet Enterprise Configuration 22
5.3 Production Web Server 27
6 Intrusion Detection System (IDS) 28
6.1 Security Onion 28
7 Certificate Authority 29
7.1 Fedora PKI 29
7.2 Post-Installation 29
8 Hosts and Mobile Device Security 30
8.1 Mobile Devices 30
8.2 MaaS360 44
8.3 Host Based Security 48
9 Identity and Access Control 48
9.1 Cisco Identity Services Engine 49

9.2 Cisco ISE Post-Installation Tasks 50
9.3 Configure CISCO ISE to Support EAP-TLS Authentication 50
10 Governance, Risk, and Compliance (GRC) 57
10.1 RSA Archer GRC 57
11 Operating Systems 79
11.1 Windows Installation and Hardening 79
11.2 Linux Installation and Hardening 81

List of Figures

Figure 1: Web Server (IIS) Components Selection Screenshot 60
Figure 2: .NET Framework 4.5 Features Selection Screenshot 61

List of Tables

Table 1: Content Sources for GRC Tool 66
Table 2: High Level Process Steps 68

1 Practice Guide Structure

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate this approach to securing electronic health records transferred among mobile devices. The reference design is modular and can be deployed in whole or in parts.

This practice guide is made up of five volumes:

- NIST SP 1800-1a: Executive Summary
- NIST SP 1800-1b: Approach, Architecture, and Security Characteristics – what we built and why
- **NIST SP 1800-1c: How To Guides – instructions to build the reference design** ⬅ **YOU ARE HERE**
- NIST SP 1800-1d: Standards and Controls Mapping – listing of standards, best practices, and technologies used in the creation of this practice guide
- NIST SP 1800-1e: Risk Assessment and Outcomes – risk assessment methodology, results, test, and evaluation

2 Introduction

The following guides show IT professionals and security engineers how we implemented this example solution for securing the transfer of electronic health records on mobile devices. We cover all the products employed in this reference design. We do not recreate the product manufacturer's documentation, which is presumed to be widely available. Rather, these guides show how we incorporated the products together in our environment.

These guides assume that you have experience implementing security products in a health care organization. While we have used the commercially available products described here, we assume that you have the knowledge and expertise to choose other products that might better fit your IT systems and business processes.[1] If you use substitute products, we hope you'll seek products that are congruent with standards and best practices in health IT, as we have. Refer to NIST SP 1800-1d: Standards and Controls Mapping, Section 5, Table 2, for a list of the products that we used mapped to the cybersecurity controls provided by this reference design, to understand the characteristics you should seek in alternate products. NIST SP 1800-1d, Section 4, Security Characteristics and Controls, Table 2 describes how we arrived at this list of controls.

This NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a draft version. We are seeking feedback on its contents and welcome your

[1] Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

input. Comments and suggestions will improve subsequent versions of this guide. Please contribute your thoughts to hit_nccoe@nist.gov, and join the discussion at http://nccoe.nist.gov/forums/health-it.

The National Cybersecurity Center of Excellence (NCCoE) response to the problem of securing electronic health care information on mobile devices has been to take the following actions:

- The NCCoE developed an example solution to this problem using commercially available products that conform to Federal standards and best practices.
- This example solution is packaged as a “How To” guide. In addition to helping organizations comply with Health Insurance Portability and Accountability Act (HIPAA), the guide demonstrates how to implement standards-based cybersecurity technologies in the real world, based on risk analysis.

Conventions

Filenames, pathnames, partitions, URLs, and program names are in italic text:

filename.conf

…/folder/filename.conf

http://nccoe.nist.gov

Commands and status codes are in `Courier`:

```
mkdir
```

Code that a user inputs is in **Courier bold**:

```
service sshd start
```

This guidance is applicable to the build that the NCCoE completed. These are not comprehensive tutorials. There are many possible service and security configurations for these products that are out of scope for this reference design.

3 Basic Network Infrastructure Services

Basic network infrastructure services exist throughout the architecture and consists of all switching and routing protocols related to layer 2 and layer 3 of the Open Systems Interconnection (OSI) model. Additional fully qualified domain name (FQDN) resolution, and wireless access services are in this section of the network. These components facilitate network traffic throughout the enterprise and interconnect systems.

3.1 Hostnames

This section references all fully qualified domain names and IP addresses used in this build. The information here can be used to build an exact duplicate of the architecture used in this build.

You do not have to use this host-naming convention or IP structure to successfully deploy this example solution. If, however, you change any of the hostnames while setting up other products mentioned in this guide, you should make the appropriate hostname changes to the configuration files for those products.

Capability Name	Hostname/FQDN	IP
OpenEMR	openemr1.healthisp.com	192.168.200.80
Fedora PKI Manager	healthitca.healthisp.com	192.168.200.73
Bind DNS and DNSE	healthitdns.healthisp.com	192.168.200.86
	healthitdnse.healthisp.com	192.168.200.85
Puppet Enterprise	puppet.healthisp.com	192.168.200.88
Security Onion IDS	healthitids.healthisp.com	192.168.200.98
Cisco ISE 1 and 2	healthitise1.healthorg1.org	10.10.101.101
	healthitise2.healthorg2.org	192.168.100.87
Symantec Endpoint Protection	healthithostprotect.healthisp.com	192.168.200.93
Vulnerability Scanner	healthitscancon.healthisp.com	192.168.100.95
RSA Archer	healthitriskman.healthisp.com	192.168.200.200
VPN Server	healthitvpn.healthisp.com	192.168.200.250
Health ISP External Firewall	healthitfirewall.healthisp.com	192.168.200.254
		192.168.100.87
Cisco AP 1	healthitorg1fw.healthitorg1.org	192.168.100.101
		10.10.101.1
Cisco AP 2	healthitorg1fw.healthitorg1.org	192.168.100.102
		10.10.102.1
URBackup Server	healthitbackup.healthisp.com	192.168.200.99
HealthIT Organization #1 Mobile Devices		10.10.101.0/24
HealthIT Organization #2 Mobile Devices		10.10.102.0/24

3.2 Bind DNS and DNSE Installation and Hardening

The Bind DNS application is based on a distributed hierarchical naming system for computers, services, or any IP based system resource connected to a public or a private network. This build utilized both an internal and external DNS server. Each was named DNS for internal and DNSE for external host resolution. This implementation forms what is known as split-DNS or spilt-brained DNS. Use of this implementation approach provides security separation of name to IP resolution. Used effectively it will essentially protect a private (RFC-1918) network from being enumerated by unauthorized external users via DNS lookups. Additionally, if an external unauthorized user attacks the external DNS the internal DNS will continue to function.

This section will show you how to install and configure both DNS servers then integrate them with the internal firewall, puppet and all other hosts on this build that need FQDN resolution.

System requirements

Processor	Minimum 1.4 GHz 64-bit processor
RAM	Minimum 8G
Disk space	Minimum 150 GB

You will also need the following parts of this guide:

- Section 11.2, Linux Installation and Hardening
- Section 3.1, Hostnames
- Section 5.2, Puppet Enterprise Configuration

3.2.1 Bind DNS Setup

> You can install Bind in several ways, such as with Linux installers like *apt-get*, *yum* and *rpm*. We used *yum*. If you install Bind using *yum,* you must either have admin/root privilege or use `sudo` to run the following commands. We recommend that you run all commands with `sudo`, rather than at the root terminal.

To install Windows Dynamic updates to Bind, see *https://support.microsoft.com/en-us/kb/275866*

Install Bind DNS by entering the following:

```
> yum install bind bind-utils
```

Configure Bind by entering:

```
> cd /var/named
```

Create DNS zone files by entering:

```
> touch dynamic/healthisp.com, healthitorg1.org, healthitorg2.org
```

Edit the zone file for the Health ISP by entering:

```
> vi dynamic/healthisp.com
```

Paste the following into *dynamic/healthisp.com:*

```
            $TTL 1D
            @ IN SOA dns.healthisp.com. admin.healthisp.com. (
                                        2 ; serial
1D ; refresh
1H ; retry
1W ; expire
3H ) ; minimum
                        NS dns.healthisp.com.
                        A 192.168.100.87
        www             A 192.168.200.80
        healthitvpn             A 192.168.200.250
        healthitriskman                 A 192.168.200.200
        healthitca              A 192.168.200.73
        openemr1                A 192.168.200.80
        healthitdns             A 192.168.200.86
        healthitdnse            A 192.168.200.85
        dns             A 192.168.200.86
        healthitconfman                 A 192.168.200.88
        puppet                  A 192.168.200.88
        healthitbackup                  A 192.168.200.99
```

Create the zone file for Health IT Organization #1 by entering the following:

```
> vi healthitorg1.org
```

Paste the following into *healthitorg1.org:*

```
            $TTL 1D
            @ IN SOA @ rname.localhost. (
0 ; serial
1D ; refresh
1H ; retry
1W ; expire
3H ) ; minimum
        NS @
                                                A 192.168.100.87
                                      www               A 192.168.100.87
                healthitise1    A 10.10.101.101
```

Create the zone file for Health IT Organization #2 by entering the following:

```
> vi healthitorg2.org
```

Paste the following into *healthitorg2.org:*

```
        $TTL 1D
        @ IN SOA @ rname.localhost. (
             0 ; serial
1D ; refresh
1H ; retry
1W ; expire
3H ) ; minimum
     NS @
                                        A 192.168.100.87
                               www      A 192.168.100.87
                               healthitise2      A 192.168.100.87
```

Open the *named.conf* configuration file for DNS by entering the following:

```
> vi/etc/named.conf
```

Paste the following into the *named.conf* file, or edit the file to look like this:

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
 listen-on port 53 { 127.0.0.1; 192.168.200.86; };
 listen-on-v6 port 53 { ::1; };
 directory "/var/named";
 dump-file "/var/named/data/cache_dump.db";
 statistics-file "/var/named/data/named_stats.txt";
 memstatistics-file "/var/named/data/named_mem_stats.txt";
 allow-query { any;};

 /*
 - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
 - If you are building a RECURSIVE (caching) DNS server, you need to enable
 recursion.
 - If your recursive DNS server has a public IP address, you MUST enable access
 control to limit queries to your legitimate users. Failing to do so will
 cause your server to become part of large scale DNS amplification
 attacks. Implementing BCP38 within your network would greatly
 reduce such attack surface
 */
 recursion yes;

 dnssec-enable yes;
 dnssec-validation yes;
 dnssec-lookaside auto;

 /* Path to ISC DLV key */
 bindkeys-file "/etc/named.iscdlv.key";

 managed-keys-directory "/var/named/dynamic";

 pid-file "/run/named/named.pid";
 session-keyfile "/run/named/session.key";
};

logging {
 channel default_debug {
 file "data/named.run";
 severity debug;
 };
};

zone "." IN {
 type hint;
 file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

Open the named*.rfc1912.zones* configuration file by entering the following:

```
> vi/etc/named.rfc1912.zones
```

Paste the following into the *named.rfc1912.zones* file, or edit the file to look like this:

```
// named.rfc1912.zones:
//
// Provided by Red Hat caching-nameserver package
//
// ISC BIND named zone configuration for zones recommended by
// RFC 1912 section 4.1 : localhost TLDs and address zones
// and http://www.ietf.org/internet-drafts/draft-ietf-dnsop-default-local-zones-02.txt
// (c)2007 R W Franks
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

zone "localhost.localdomain" IN {
 type master;
 file "named.localhost";
 allow-update { none; };
};

zone "localhost" IN {
 type master;
 file "named.localhost";
 allow-update { none; };
};

zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
 type master;
 file "named.loopback";
 allow-update { none; };
};

zone "1.0.0.127.in-addr.arpa" IN {
 type master;
 file "named.loopback";
 allow-update { none; };
};

zone "0.in-addr.arpa" IN {
 type master;
 file "named.empty";
 allow-update { none; };
};

// START CUSTOM DOMAINS FOR LAB


zone "healthitorg1.org" IN {
 type master;
 file "healthitorg1.org";
 allow-update { none; };
};

zone "healthitorg2.org" IN {
 type master;
 file "healthitorg2.org";
 allow-update { none; };
};

zone "healthisp.com" IN {
 type master;
 file "dynamic/healthisp.com";
 allow-update { 192.168.200.70; 192.168.200.71; 192.168.200.83; 192.168.200.93; 192.168.200.72; };
};

zone "_msdcs.healthisp.com" IN {
 type master;
 file "dynamic/_msdcs.healthisp.com";
 allow-update { 192.168.200.70; 192.168.200.71; 192.168.200.83; 192.168.200.93; 192.168.200.72;};
```

};

3.3 Access Point: Cisco RV220W

This build uses the Cisco business class wireless access points (AP). These business class APs have additional functions beyond normal home use APs. As an example, the APs allow enterprise connection security to enable certificated based authentication to the AP. The APs assist in facilitating mobile device connectivity to each of the remote health organization networks. Each connected mobile device can then securely connect to the EHR server using the AP connection.

This section will describe how to configure the APs with IPs, MAC address filtering and certificate based access control.

System requirements

- Two Cisco RV220W APs
- At least version 1.0.6.6 and up firmware
- A PC to connect to and configure the Web-based interface

You will also need the following parts of this guide:

- Section 3.1, Hostnames
- Section 8.2.1, MDM Setup
- Section 9.1, Cisco Identity Services Engine

3.3.1 Cisco RV220 AP Setup

We assume that you have a functional Internet connection via Ethernet.

1. Connect the Ethernet cable from the Internet to the WAN port of the RV220W.
2. Connect one end of a different Ethernet cable to one of the LAN (Ethernet) ports on the back of the unit.
3. Connect the other end to an Ethernet port on the PC that will be used to run the Web-based device manager.
4. Connect the power line and turn on the power switch.

More detailed procedures for installing the Cisco® RV220W Network Security Firewall is available from the Cisco installation guide at *http://www.cisco.com/c/dam/en/us/td/docs/routers/csbr/rv220w/administration/guide/rv220w_ag_78-19743.pdf.*

3.3.2 Post-Setup Tasks

1. Use a PC to connect to a LAN port of the Cisco RV220W. If DHCP is enabled, the PC should receive an IP address and the PC becomes a DHCP client of the RV220W. Otherwise, you may need to configure the PC to obtain an IP address from a DHCP server.
2. From the PC, use a compatible browser (e.g. Firefox) to connect to the Cisco® RV220W administration portal using the default address (192.168.1.1) and the default credentials (username “cisco” and password “cisco”).

3. After logging in to the configuration utility, click Run Setup Wizard in the navigation tree to detect and configure the Internet setting automatically. In addition to setting up the Internet connection, the setup wizard will also request that the user change the default password.

4. Verify that the IPv4 WAN setting is correctly set, which should include the IP address of the device in the WAN with proper subnet mask, default gateway, and primary DNS server IP address. If the IPv4 WAN is not configured automatically, check with the Internet service provider to obtain these required parameters and configure the Internet connection under: *Networking > WAN (Internet) > IPv4WAN (Internet)*. Be sure to specify the correct Internet Connection Type: Static IP, DHCP or other types.

5. Verify the Cisco RV 220W has the latest firmware installed:

   - Navigate to the path: *Status > System Summary* to check the software version. The current version is 1.0.6.6. If your AP firmware version is lower than the current one, update the firmware by following these steps:

     - Download the firmware from https://software.cisco.com/download/release.html?mdfid=283118607&softwareid=282487380&release=1.0.2.4&rellifecycle, and save it to a file.

     - From the Cisco RV220W configuration utility, navigate to *Administration > Firmware Upgrade.*

     - Browse to the saved download file.

     - Press the Start Firmware Upgrade button and following the instruction from the installer.

3.3.3 Cisco RV220 AP Setup for EAP-TLS Authentication

3.3.3.1 To configure LAN for IPv4

1. Use 10.10.101.0 Org1 and 10.10.102.0 Org2

2. Navigate to the path from the Configuration Utility Portal: *Network > LAN (Local Network) > IPv4 LAN (Local Network)* to setup the IPv4 LAN.

3. Change the default setting to meet your specific requirements to include:

   - IP address for this device in the LAN (e.g. 10.10.101.1)
   - subnet mask (e.g. 255.255.255.0)
   - DHCP mode for assigning IP addresses to the client connect to this LAN (e.g. DHCP server)
   - domain name (e.g. HealthITOrg1)
   - starting IP address (e.g. 10.10.101.2)
   - ending IP address (e.g. 10.10.101.25)
   - primary DNS server (e.g. 192.168.100.87)

If you want to configure a static IP address and MAC address for a known computer:

1. Use the path: *Network > LAN (Local Network) > Static DHCP***.** This will reserve the IP addresses for a list of known computer devices linked to the LAN.

2. Click Add to add an IP address and the MAC address for each computer you wish to include.

3.3.3.2 Cisco RV220 AP Wireless Setup for IPv4 LAN

1. Navigate to the path from the Configuration Utility Portal by following the path *Wireless > Basic Setting.*
2. Enable one of the four default preset SSIDs in the wireless Basic Setting table setting:
   - assign an SSID Name
   - disable SSID broadcast
   - enable security mode
   - enabled the MAC filter
3. Edit Security Mode:
   - Navigate to Wireless > Basic Setting
   - Select a Wireless SSID to edit the security mode
   - Click Security Setting Mode
   - In the form for required security parameters, follow the guidance for enabling WPA2 Enterprise and Encryption AES
4. Edit MAC Filtering to block devices with MAC addresses that are not registered in the AP
   - Use the path Wireless > Basic Setting
   - Select a Wireless SSID to edit the security mode
   - Click Edit MAC Filtering and Add
   - Follow the form to add the MAC addresses that you want the AP to control

3.3.3.3 Cisco RV220 AP RADIUS Server Settings

NOTE: References to the RADIUS server are synonymous with the Cisco ISE server. The radius server is a subcomponent of the Cisco ISE AAA services (Authentication, Authorization, and Accounting).

1. Navigate to the path from the Configuration Utility Portal: *Security* > *RADIUS* Server to setup the AP to communicate with the authentication server
2. Fill out details in the RADIUS configuration pages, which normally includes:
   - Authentication Server IP address – the IP address of the authenticating RADIUS server (e.g. 10.10.101.101)
   - Authentication Port – the RADIUS authentication server's port number used to send RADIUS traffic (e.g. 1812)
   - Enter the pre-shared secret that will be used between the AP and the RADIUS authenticator server
   - Timeout – the timeout interval (in seconds) after which the RV220W re-authenticates with the RADIUS server

- Retries – the number of retries for the RV220W to re-authenticate with the RADIUS server. If the number of retries is exceeded, authentication of this device with the RADIUS server has failed

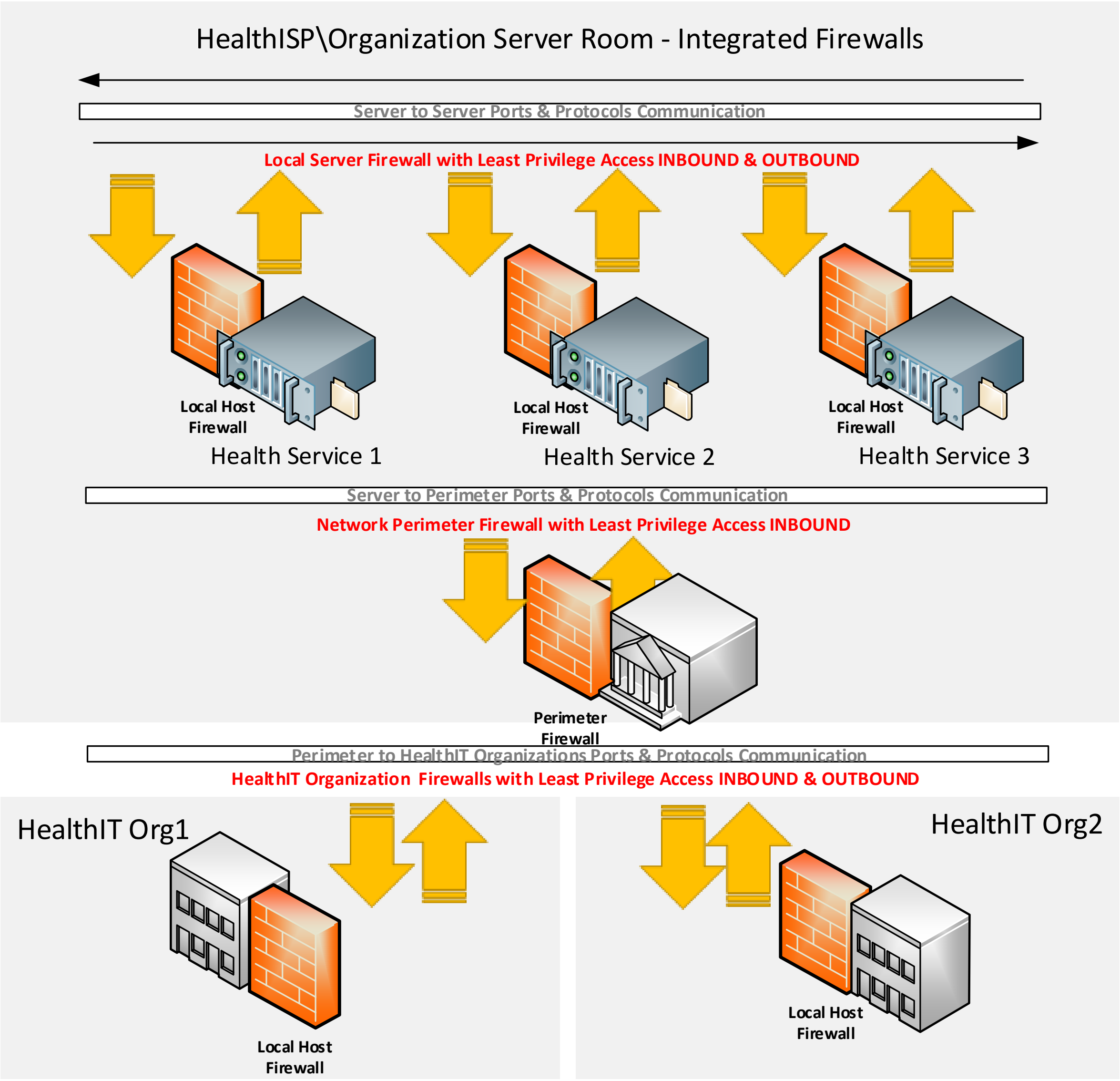
After the setup, you can use the diagnostic tools provided in the RV220W admin portal to test the connectivity between the AP and the RADIUS authentication server.

The firewall on the APs were set to the default setting for this install. This blocked all inbound traffic with exception to Internet Control Message Protocol (ICMP) traffic. All outbound traffic was allowed from internal clients. If the authentication server is installed in the cloud behind the corporate or AP firewall, you can use port forwarding to allow the AP to properly communicate with the RADIUS server. In this case, use the firewall network address as the authentication server IP address.

3.4 Firewalls: IPTables

A firewall is used to control egress and ingress network traffic between multiple subnets and or systems. A firewall will determine what traffic goes in which direction based on ip, tcp/ip or udp/ip ports and protocols. A firewall uses rules to allow or disallow traffic based on an organization’s security policy. The IPTables firewall is a Linux based firewall that uses stateful inspection to protect ports.

Each subnet and server host on this build has a firewall. The servers have local firewalls that follow a least privilege access approach for outbound and inbound traffic. Each subnet cross point between other subnets has a firewall to protect Internet traffic from traversing inbound to the internal network.


HealthISP\Organization Server Room - Integrated Firewalls
Server to Server Ports & Protocols Communication
Local Server Firewall with Least Privilege Access INBOUND & OUTBOUND
Local Host Firewall
Health Service 1
Local Host Firewall
Health Service 2
Local Host Firewall
Health Service 3
Server to Perimeter Ports & Protocols Communication
Network Perimeter Firewall with Least Privilege Access INBOUND
Perimeter Firewall
Perimeter to HealthIT Organizations Ports & Protocols Communication
HealthIT Organization Firewalls with Least Privilege Access INBOUND & OUTBOUND
HealthIT Org1
Local Host Firewall
HealthIT Org2
Local Host Firewall

System requirements

- Linux Operating System
- IPTables application installed (installed by default on most Linux systems)
- Most intel-based systems will support IPtables and Linux (see your Linux version hardware compatibility (HCL) list for more)
- If this is a system that protects multiple subnets then multiple network interface cards (NIC) for each subnet will be needed. (see your Linux OS HCL for more on multiple NIC compatibility)

You will also need the following parts of this guide:

- Section 11.2.2, Linux Post-Installation Tasks
- Section 3.1, Hostnames

IPTables Setup

Puppet Enterprise ensured the installation of IPTables and all Linux-based external firewalls for this build. No action is needed to install the local firewalls if the Puppet prerequisite has been followed below. Section 3.4 lists the files that contain the firewall rules for each Linux system used in our build.

4 Backup

The backup system is an important part of security as it assists with ensuring the architecture survives in the event of a disaster. Regular full and incremental backups provide a means of recovery in the event of a disaster. Remote online backups provide even more security as offsite backups are harder to tamper or lose in a local disaster to the architecture.

This section will show you how to install an online back-up system using URBackup.

4.1 URBackup

As described, URBackup is a remote backup system that will facilitate both full and incremental backups. It's a Web-based system designed to allow multiple administrators to manage backups to all Windows and Linux based systems

System requirements

Processor	Minimum 1.4 GHz 64-bit processor
RAM	Minimum 8G
Disk space	Minimum 150 GB

You will also need the following parts of this guide:

- Section 11.2, Linux Installation and Hardening
- Section 3.1, Hostnames
- Section 5.2, Puppet Enterprise Configuration

URBackup Setup

Follow these instructions to build, install, and set up UrBackup on Fedora20 Linux systems.

If you want the URBackup Server itself to be backed up, follow this same guidance for the URBackup Server.

1. Follow Section 11.2, Linux Installation and Hardening.
2. Install the dependencies UrBackup needs:
   - If installing on Fedora 20, there is a WxWidgets app already installed. Please verify that its version is higher than 3.0.
   - On Fedora 20, you will use *yum* as your installer.
3. Input the following commands:

For this install, make sure you have allowed outbound port 80 and 443 only.

```
> yum install gcc-c++
> yum remove wxBase or wxBase3 # removes any current yum instantiations
of wxBase3 so no conflicts
> yum install wxGTK3
> yum install wxGTK3-devel
> yum install wxBase3
> ln -s /usr/libexec/wxGTK3/wx-config /usr/bin/wx-config
> yum install cryptopp-devel
> wx-config # just to test if it works
> mkdir /usr/local/urbackup
> cd /usr/local/urbackup
> wget
http://sourceforge.net/projects/urbackup/files/Client/1.4.7/urbackup-
client-1.4.7.tar.gz/download
> mv download /usr/local/urbackup/urbackup-client-1.4.7.tar.gz
> cd /usr/local/urbackup/
> tar zxvf urbackup-client-1.4.7.tar.gz
> cd urbackup-client-1.4.7/
> ./configure --enable-headless # enable headless if you want to use
the main server vs GUI on the client
```

4. Build the UrBackup client and install it:

```
> make
> make install
```

The program will return the following:

```
POST INSTALL NOTICE:
----------------------------------------------------------------------
Libraries have been installed in:
 /usr/local/lib
If you ever happen to want to link against installed libraries
in a given directory, LIBDIR, you must either use libtool, and
specify the full pathname of the library, or use the `-LLIBDIR'
flag during linking and do at least one of the following:
 - add LIBDIR to the `LD_LIBRARY_PATH' environment variable
 during execution
 - add LIBDIR to the `LD_RUN_PATH' environment variable
 during linking
 - use the `-Wl,-rpath -Wl,LIBDIR' linker flag
 - have your system administrator add LIBDIR to `/etc/ld.so.conf'

See any operating system documentation about shared libraries for
more information, such as the ld(1) and ld.so(8) manual pages.
----------------------------------------------------------------------
/usr/bin/install -c -m 644 -D "./backup_client.db"
"/usr/local/var/urbackup/backup_client.db.template"
touch "/usr/local/var/urbackup/new.txt"
make[2]: Leaving directory `/usr/local/urbackup/urbackup-client-
1.4.7/urbackupclient'
make[1]: Leaving directory `/usr/local/urbackup/urbackup-client-
1.4.7/urbackupclient'
```

5. Setup communication with the server by opening *vi /usr/local/var/urbackup/data/settings.cfg* and add the following:

   Make sure there are no spaces at the end of the line when you cut and paste this into the file.

```
internet_server=healthitbackup.healthisp.com
internet_server_port=55415
computername=<your backup client hostname>.healthisp.com
internet_authkey=foobar # See Note 2 in section 4 about this; remove this
                  comment when you cut and paste it in the file
internet_mode_enabled=true
```

6. Make sure that the UrBackup client can communicate with the server correctly. (Don't worry when you see authentication errors. We are only testing the ability for the client to communicate properly.)

```
> start_urbackup_client --loglevel debug --no_daemon --internetonly
```

   It should connect and say "Successfully Connected" after a series of lines that fly by on the screen.

   You will receive an authentication error that looks like the following:

```
2015-01-29 09:41:54: Successfully connected.
2015-01-29 09:41:54: ERROR: Internet server auth failed. Error: Unknown
client (healthitconfman.healthisp.com)
2015-01-29 09:41:54: InternetClient: Had an auth error
```

```
2015-01-29 09:41:54: ERROR: Internet server auth failed. Error: Unknown
client (healthitconfman.healthisp.com)
```

```
2015-01-29 09:41:54: InternetClient: Had an auth error
```

`> CTRL-C` to exit

Here is the fix:

UrBackup also allows manually adding clients and manually configuring the shared key. Follow these steps to add such a client:

- Log into the URBackup server via the Web link *http://yourhost.yourdomain.com:55414*
- Go to the “Status” screen.
- Under “Internet clients” enter the FQDN name of the laptop/PC you want to add. This must be the fully qualified computer name (i.e. the one you see in the advanced system settings) or the computer name configured on the client.
- After pressing “add” there will be a new client in the “Status” screen. Go to the "Settings" section then use the drop down "Client" menu to select the newly added client there.
- In the Internet settings view the authentication key for that client. Copy the key and go back to the client then edit the */usr/local/var/urbackup/data/settings.cfg* file on the client. Add the authentication key to the setting in that file.
- The server and client should now connect to each other. If it does not work the client shows what went wrong in the “Status” window.
- Test the fully authenticated connection again:

  ```
  > sudo start_urbackup_client --loglevel debug --no_daemon --
  internetonly
  ```

You should now see a success message. Just `CTRL-C` out of it and move to the next step.

7. Start the UrBackup client backend on startup using the following for Fedora20:

   ```
   > vi /lib/systemd/system/urbackup-client-backend.service
   ```

   Add the following to the file *urbackup-client-backend.service*

   ```
   [Unit]
   Description=Starting backend client services for URBackup client
   After=syslog.target network.target

   [Service]
   Type=forking
   NotifyAccess=all
   PIDFile=/run/urbackup_client.pid
   ExecStart=/usr/local/sbin/start_urbackup_client
   ExecStop=/usr/local/sbin/stop_urbackup_client
   ```

```
[Install]
WantedBy=multi-user.target
```

Change Permissions

```
> chmod 755 /lib/systemd/system/urbackup-client-backend.service
```

Create Stop Client Process File

```
> vi /usr/local/sbin/stop_urbackup_client
```

Add the following to the stop_urbackup_client file

```
#!/bin/bash

if [ -f /var/run/urbackup_client.pid ]; then
        /usr/bin/kill `cat /var/run/urbackup_client.pid`
else
        echo ""
         echo "URBackup Client is not running!!!"
         echo ""
fi
```

Make symbolic link

```
> cd /etc/systemd/system/
> ln -s /lib/systemd/system/urbackup-client-backend.service
```

Make systemd take notice of it

```
> systemctl daemon-reload
```

Activate a service immediately

```
> service urbackup-client-backend start
```

Or

```
> systemctl start urbackup-client-backend.service
```

Enable a service to be started on bootup

```
> chkconfig urbackup-client-backend on
```

Or

```
> systemctl enable urbackup-client-backend.service
```

8. Start the UrBackup client backend on startup using the following for CentOS and other Linux OSs that still use init scripts:

   Edit rc.local

   ```
   > vi /etc/rc.d/rc.local
   ```

Paste the following into that file

/usr/local/sbin/start_urbackup_client

To start immediately, run

```
> start_urbackup_client
```

9. Configure the client backup files, images, time intervals and increments, and custom backup locations and other settings for each client:
   - Log into the URBackup server Web portal.
   - Use the client dropdown menu and select the client you want to set custom settings for this configuration.
   - Select the "Separate settings for this client" radio button and begin edits.
   - Save your settings after each section you edit.

10. Make sure local client firewall rules allow inbound and outbound for URBackup. Fedora 20 server clients and `iptables` command:

```
      /sbin/iptables -A OUTPUT -p tcp --dport 55415 -m state --state NEW -d
192.168.200.99 -j ACCEPT

      /sbin/iptables -A INPUT -p tcp --dport 35621 -m state --state NEW -s
192.168.200.99 -j ACCEPT

      /sbin/iptables -A INPUT -p tcp --dport 35623 -m state --state NEW -s
192.168.200.99 -j ACCEPT

      iptables -A INPUT -p icmp --icmp-type 8 -s 0/0 -m state --state
NEW,ESTABLISHED,RELATED -j    ACCEPT
```

11. Make sure URBackup Server has firewall rules to allow inbound and outbound rules

```
      /sbin/iptables -A OUTPUT -p tcp --dport 35621 -m state --state NEW -d
192.168.200.0/24 -j ACCEPT

      /sbin/iptables -A OUTPUT -p tcp --dport 35623 -m state --state NEW -d
192.168.200.0/24 -j ACCEPT

      /sbin/iptables -A INPUT -p tcp --dport 55415 -m state --state NEW -j
ACCEPT

      /sbin/iptables -A INPUT -p tcp --dport 55414 -m state --state NEW -j
ACCEPT
```

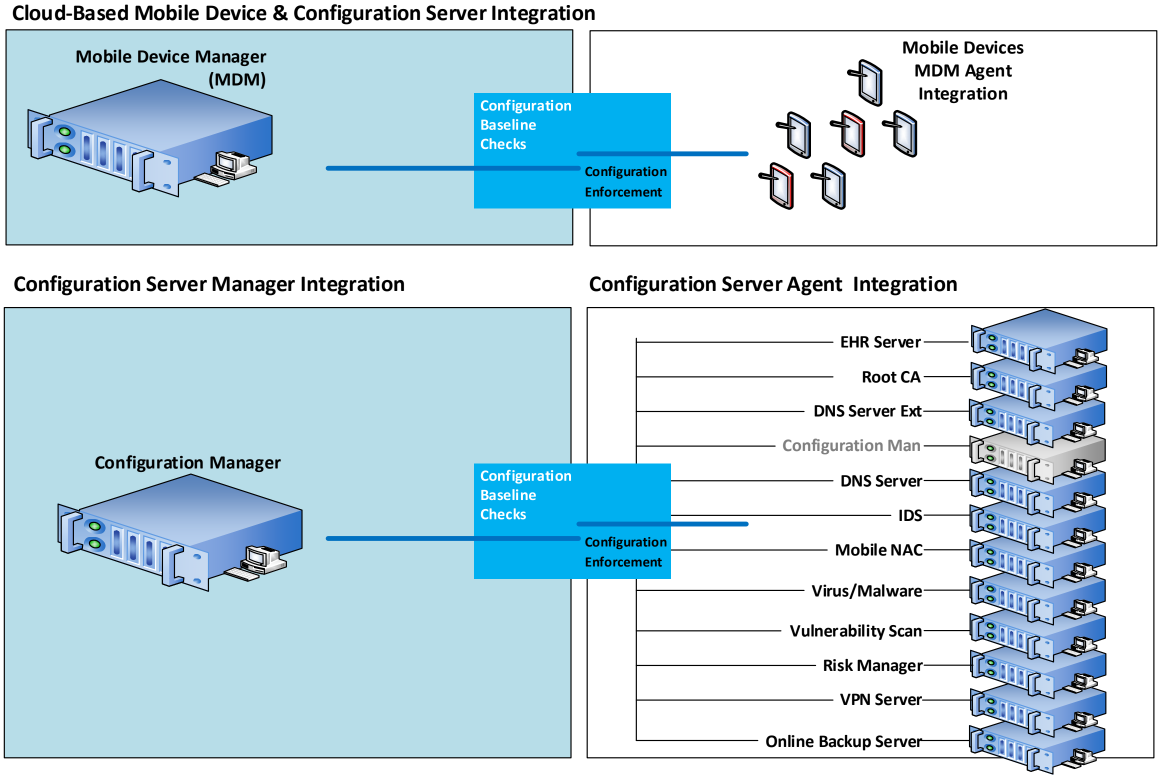
5 Configuration Management

Understanding, implementing and maintaining a secure baseline for all systems that process and store PHI is critical to its security. In the event that a configuration becomes corrupt or unusable the configuration management tool provides recovery capabilities. In addition the tool can periodically validate that a configuration is correct or unchanged from its known configuration. The configuration management tool selected for this build offers the following options:

- Secure Configuration Baseline Creation
- Automated Secure Configuration Baseline Maintenance

- Automated Secure Configuration Baseline Compliance
- Secure Configuration Baseline Reporting

System Security Baseline and Configuration Management System


Cloud-Based Mobile Device & Configuration Server Integration
Mobile Device Manager (MDM)
Configuration Baseline Checks
Configuration Enforcement
Mobile Devices MDM Agent Integration
Configuration Server Manager Integration
Configuration Server Agent Integration
Configuration Manager
Configuration Baseline Checks
Configuration Enforcement
EHR Server
Root CA
DNS Server Ext
Configuration Man
DNS Server
IDS
Mobile NAC
Virus/Malware
Vulnerability Scan
Risk Manager
VPN Server
Online Backup Server

System requirements

- Processor Minimum 1.4 GHz 64-bit processor
- RAM Minimum 8G
- Disk space Minimum 150 GB

You will also need the following parts of this guide:

- Section 11.2, Linux Installation and Hardening
- Section 3.1, Hostnames

5.1 Puppet Setup

This build uses an agent/master configuration with the default <puppet> hostname for the Puppet Master. We used the Web-based report interface in this build, although it is not normally installed with Puppet.

5.1.1 Pre-Install Tasks

Puppet Enterprise has some preparation tasks that need to be completed prior to install. For the steps to follow, see *https://docs.puppetlabs.com/guides/install_puppet/pre_install.html*

5.1.2 Install Instructions

This build used Puppet Enterprise on Fedora 20 Linux. Find install instructions for Fedora 20 at *https://docs.puppetlabs.com/guides/install_puppet/install_fedora.html*

5.1.3 Post-Install Tasks

Puppet has several post-installation tasks, including setting up its manifests, modules, and other files. Before starting the Puppet Master, follow the guidance in Section 5.2, Puppet Enterprise Configuration. We give specific guidance in Section 5.1.3 regarding changes to the Puppet Enterprise post-install documentation.

According to the post-install guidance in the Puppet Enterprise documentation, the following components can be installed as options.

> We recommend that you do NOT set up the following post-installs unless you are familiar with the security implications and advanced features.

- Automatic Puppet Master Certificate Processing – this has security implications. See note above
- Load Balancing – not needed unless your organization has a large group of agents to manage
- Puppet Manifests and Modules – This task will be completed later, but you should read this section in the Puppet Enterprise post-install documentation for the location of the directories and files needed to set up Puppet
- Configure Production Ready Web Server – this will be covered in Section 5.2.5 Puppet Enterprise Web-Based Reporting Installation and Configuration and Section 5.3, Production Web Server

5.2 Puppet Enterprise Configuration

> Puppet uses the *g* file, manifests, and modules to configure itself and other systems. While there are other files that assist with configuration of Puppet, these are the main areas where specific system configuration control is executed. This build also made use of Puppet templates to assist with creation of Linux-based files to be used in configuration management and secure baseline controls.

5.2.1 Puppet.conf

The *puppet.conf* file for the Puppet Master is in the */etc/puppet* directory. This build requires the following configuration. Cut and paste the Puppet Master *puppet.conf* configuration below into */etc/puppet/puppet.conf.*

```
 [main]
        # The Puppet log directory.
        # The default value is '$vardir/log'.
        logdir = /var/log/puppet

        # Where Puppet PID files are kept.
        # The default value is '$vardir/run'.
        rundir = /var/run/puppet

        # Where TLS certificates are kept.
        # The default value is '$confdir/tls'.
        tlsdir = $vardir/tls
              server = puppet.healthisp.com
[agent]
        # The file in which puppet stores a list of the classes
        # associated with the retrieved configuration. Can be loaded in
        # the separate ``puppet`` executable using the ``--loadclasses``
        # option.
        # The default value is '$confdir/classes.txt'.
        classfile = $vardir/classes.txt

        # Where puppetd caches the local configuration. An
        # extension indicating the cache format is added automatically.
        # The default value is '$confdir/localconfig'.
        localconfig = $vardir/localconfig
       report=true
[master]
       reports=store,http
       reporturl=http://puppet.healthisp.com:3000/reports/upload
```

5.2.2 Manifests

Manifests are files that consist of Puppet application code language. Those familiar with functions and classes in other programming languages may find the code in Puppet familiar.

Learn more about manifests at *https://docs.puppetlabs.com/pe/latest/puppet_modules_manifests.html*

The following list describes each manifest used in this build. The specific files can be found in the online file repository for this use case at *https://nccoe.nist.gov/sites/default/files/nccoe/manifests.zip*.

Once downloaded, the files should be moved to the */etc/puppet/manifests* directory of Puppet Master. The files will not work if the hostnames for each system have been changed from the hostnames provided in the Section 3.1, Hostnames.

The following customized Puppet enterprise manifests were configured and installed in this build:

site.pp – this is the main configuration file for Puppet. This is the launch point for all other manifests. There are custom class entries in this file for specific Windows configurations. However, most of this file consists of manifests imports and calls to predefined classes created in each manifest.

- *accounts.pp* - this allows control over users who can log in and also controls the password. If an attacker changes any of the information in the *passwd* file then Puppet will change back based on the entries in this file.
- *crontabconfig.pp* - this file creates tasks that run automatically at set intervals. In this case there are four tasks that are executed to secure Linux.
  - *Logoutall.sh* - this task will run every few seconds and kill all other user tasks with exception of root. This effectively removes normal users from all the Linux systems while they are in production mode
  - *puppetagent.config.base.sh* – this task will periodically run the Puppet agent to update any changes to the configuration of the local system based on a remote Puppet Master configuration change.
  - *yum.config.base.sh* – this task will force the local system to update itself during set a time every day.
  - *harden.os.single.commands.sh* – this is a series of single commands to ensure changes to permissions on critical system files, disable root console or other one line commands are issued.
- *firewall_rules.pp* - this creates and enforces individual *iptables* rules on each local Linux host in accordance with the least access needed in or out of the system.
- *grub2fedora20.pp* - this build implemented versions of Fedora 20 with the Grub2 bootloader. The bootloader assists with starting the Linux operating system and allowing the operator to make special configurations prior to the system boot process. This access can be dangerous because it will allow an attacker to boot the system into single user mode or make other changes prior to the boot process. The changes made with this Puppet manifest file create a Grub2 password challenge.
- *openemr.pp* - this will use both the `apache` and `concat` modules to configure the EHR OpenEMR Web server. It will enable TLS and OCSP.
- *openemrconcat.pp* – this file augments the *openemr.pp* file by setting up the ModSecurity Web application firewall.
- *packages.pp* - this ensures that less secure applications are removed and only the applications needed to run the service are installed on the local system.

- *passwdfile.pp* - this cleans the *passwd* file of standard users that come with the Fedora 20 Linux distro. It also cleans the group file.
- *puppet.pp* – this sets up the Puppet reporting feature.
- *securettyfile.pp* - this creates a new *securetty* file in the local system that prevents root from logging into a console session.
- *ssh.pp* - this hardens the encrypted remote management service for Linux.
- *time.pp* - this forces the local system to use a time server for accurate time. This creates accurately time-stamped logs.
- *warningbanners.pp* - this creates warning banners at the console and remote login sessions that warn users that their sessions should be authorized and monitored. This banner should act as a deterrent for good people accidentally doing bad things. It will in no way stop a determined attacker under any circumstances.

5.2.3 *Templates*

Puppet templates are used in this build to create configuration files for systems. As an example, if the *sshd_config* file already existed on a Linux system running *ssh*, Puppet would recreate the *sshd_config* file according to our templates. Another example is that all of the local system and Health ISP perimeter firewall rules are in the templates directory. If new rules or policies for all systems managed by Puppet need to be changed, the templates can be updated in one central location. Puppet templates can be configured with the *erb* Puppet language. This build used simple text commands that are native to the application configured by the template. For example, the *iptables* template uses *iptables* configuration language to configure the firewall on each system.

All of the templates used this this build can be downloaded from the following link: *https://nccoe.nist.gov/sites/default/files/nccoe/templates.zip*.

Once you download the templates, move them to the */var/lib/puppet/templates* directory. The templates directory may need to be created using the `mkdir` command.

The following list provides descriptions of each template file.

- puppet agent cron – periodic tasks to run Puppet agent
  - *puppetagent_config_base.erb*
  - *logoutall_CENTOS_config_base.erb*
  - *logoutall_config_base.erb*
  - *logoutall_daytime_config_base.erb*
  - *government_motd_motd_file.erb*
  - *government_motd_issue_file.erb*
  - *passwd_group_file_edit_data.erb*
- account lockout – locks out certain non-root users during production run time
- message of the day - unauthorized use warning banner
- password file clean up – removes default users and groups from Linux
  - *passwd_group_remove_script.erb*

- boot lockdown – adds grub password to system boot up and prevents single sign-on ability
    - *grub_lockdown_password.erb*
    - *grub2_lockdown_password.erb*
- single line hardening commands - a series of permissions and other changes to the system to harden it against attacks
    - *harden_os_single_commands.erb*
- local and perimeter firewall rules – all firewall rules for each system used in this build
    - *dns_firewall_base_rules.erb*
    - *dnse_firewall_base_rules.erb*
    - *healthitbackup_firewall_base_rules.erb*
    - *openemr1_firewall_base_rules.erb*
    - *puppet_firewall_base_rules.erb*
    - *healthitca_firewall_base_rules.erb*
    - *healthitfirewall_firewall_base_rules.erb*
- root console login deny – prevents root from logging in at the local console and an attacker from attempting a brute-force attack at the console
    - *securetty_devicelogin_config.erb*
- linux system updates - creates script for *cron* to run *yum* updates to Linux systems
    - *yum_config_base.erb*

5.2.4 Modules

Multiple manifests combine to make up modules in Puppet. There are communities of people who maintain a large array of Puppet modules. When installed via the following process, Modules are stored in the */etc/puppet/modules* directory.

They can be found at *https://forge.puppetlabs.com/.*

Modules can also be viewed, downloaded, and installed by the Puppet Master using the following commands at the Puppet Master command line interface:

```
> puppet module list
# Lists all installed modules

> puppet module search apache
# puppet will search and list Apache modules.

> puppet module install puppetlabs-apache –version
# puppet will install here
```

Learn more about Modules at *https://docs.puppetlabs.com/pe/latest/puppet_modules_manifests.html*

Our example solution used the following Puppet modules. Use the commands above to install them.

- *puppetlabs-apache* – streamlined creation of Web services using Apache

- *puppetlabs-mysql* – streamlined edits of *mysql* with minimal configuration
- *puppetlabs-concat* - allows creation of configuration files based on concatenation
- *puppetlabs-ntp* – provides an ability to manage standard time on systems
- *puppetlabs-registry* – allows edits to the Windows registry for configuration
- *puppetlabs-stdlib* – this is the standard library for resources on Puppet

5.2.5 Puppet Enterprise Web-Based Reporting Installation and Configuration

Find the full installation documentation at *https://docs.puppetlabs.com/dashboard/manual/1.2/configuring.html*

Short Version:

Run the following on your Puppet Master:

```
> yum install puppet-dashboard
```

Add the following to *puppet.conf* on each Puppet Agent:

```
[agent]
        report = true
```

Add the following to *puppet.conf* on the Puppet Master

```
[master]
 reports = store, http
 reporturl = http://dashboard.example.com:3000/reports/upload
```

Run the following commands on the Puppet Master:

```
> puppet-dashboard rake cert:create_key_pair
> puppet-dashboard rake cert:request
> puppet-dashboard rake cert:retrieve
```

5.3 Production Web Server

These instructions are for a non-production environment like ours. Because a production-ready reporting server is a best practice, it may be beneficial to learn more about that once you become familiar with Puppet Enterprise. Visit the following link: *https://docs.puppetlabs.com/guides/install_puppet/post_install.html#configure-a-production-ready-web-server.*

6 Intrusion Detection System (IDS)

An Intrusion Detection Server monitors a network for known threats to an organizations network. It will examine every packet it sees, then deconstruct the packet looking for header and/or payload threats. Usually, most IDS servers will utilize a packet reassembly mechanism to limit the effects of fragmented attacks as well as normal TCP transmission analysis.

6.1 Security Onion

Security Onion is the IDS selected for this build. It was selected based on its track record in the open source community for its support to SNORT and built in Web-based administration functions.

IDS Supporting Applications and Services

- **Squert** – a Web application that is used to query and view event data stored in a Sguil database (typically IDS alert data). Squert is a visual tool that attempts to provide additional context to events through the use of metadata, time series representations and weighted and logically grouped result sets. The hope is that these views will prompt questions that otherwise may not have been asked.
- **Sguil** – used as a database for IDS alerts
- **ELSA** – adds and ability to normalize logs and assists in searching a large set of alerts
- **Snorby** – integrates with Snort and allows reporting of sensor data on a daily, weekly and monthly basis.

System requirements

- The Security Onion IDS runs on Ubuntu Linux
- Hardware requirements can be found at https://code.google.com/p/security-onion/wiki/Hardware
- Find the ISO image full version at https://code.google.com/p/security-onion/wiki/QuickISOImage
- Find the Install Version for Ubuntu Linux at https://code.google.com/p/security-onion/wiki/InstallingOnUbuntu

You will also need the following parts of this guide:

- Section 11.2, Linux Installation and Hardening
- Section 3.1, Hostnames

Security Onion Setup

We followed the documentation provided by Security Onion:

- Introduction *https://code.google.com/p/security-onion/wiki/IntroductionToSecurityOnion*
- Production install steps *https://code.google.com/p/security-onion/wiki/ProductionDeployment*

- Booting issues
  https://code.google.com/p/security-onion/wiki/TroubleBooting
- Post-Installation
  https://code.google.com/p/security-onion/wiki/PostInstallation

7 Certificate Authority

The certificate authority uses the OpenSSL cryptographic libraries to create then sign soft certificates for use in identifying mobile devices that would ultimately connect to both the AP and the OpenEMR server. The certificate authority is also the trusted signatory of the OpenEMR Web server certificate. In a transaction where a certificate is used as an identity, all participants must ultimately trust the signatory of the presented certificate. This build relies heavily on a certificate authority. Using a Public Key Infrastructure approach is among the strongest methods to assure proper identity and access control for PHI.

7.1 Fedora PKI

The certificate authority used for this build is based on a Linux PKI Manger used in Fedora, RedHat Enterprise and other production class Linux distros.

System requirements

Processor	Minimum 1.4 GHz 64-bit processor
RAM	Minimum 8G
Disk space	Minimum 150 GB

You will also need the following parts of this guide:

- Section 11.2, Linux Installation and Hardening
- Section 3.1, Hostnames
- Section 3.2, Bind DNS and DNSE Installation and Hardening
- Section 5.2, Puppet Enterprise Configuration

Fedora PKI Installation

Fedora PKI Manager Installation instructions can be found at *http://pki.fedoraproject.org/wiki/Quick_Start*

7.2 Post-Installation

Fedora PKI Manager Administrator set-up instructions can be found at *http://pki.fedoraproject.org/wiki/CA_Admin_Setup*.

To manually create user/device certificates, follow the steps in Section 8, Mobile Device Manager, or the instructions at *http://pki.fedoraproject.org/wiki/User_Certificate*.

To approve the certificate request, use the Web administrator's interface, as described below. You can use the command line, instead, if you are familiar with that method.

1. Navigate to Web Approval at *https://<your certificate authority host.domain>.com:8443*
2. Go to *Admin Services* > *Agent Services*
3. This should default to the List Requests tab. If not, click that tab on the left navigation pane.

4. Click the Find button. Once the Find page loads, there were be a list of pending requests. Select the number to approve the request.
5. Scroll to the bottom of the page, then approve or deny the request.

To retrieve the client/device certificate:

1. Navigate to *http://<your certificate authority host.domain>.com:8080*
2. Click on End Users Services.
3. Click on Retrieval Tab. This will connect to the Check Request Status Tab.
4. Enter in your certificate request reference number created during the registration request process.
5. Scroll to the bottom of the page and download

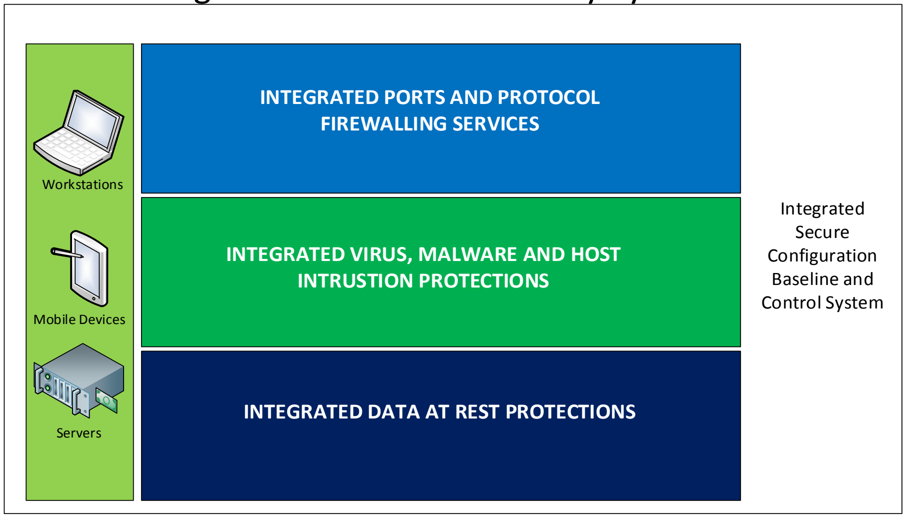
   OR

   Copy and paste the certificate information to the mobile device desktop and follow Section 8, "Mobile Device Management" for details on how to install the certificate.

8 Hosts and Mobile Device Security

Hosts and Mobile Devices combine with the basic network architecture to create the HealthIT environment used to move PHI to and from its origin. Each host on the build network is a server that provides a specific service to either secure or facilitate authorized PHI data sharing. Mobile devices are used by authorized health care professionals and patients to add, change, read or remove PHI.

Integrated Host Based Security System


Workstations
Mobile Devices
Servers
INTEGRATED PORTS AND PROTOCOL FIREWALLING SERVICES
INTEGRATED VIRUS, MALWARE AND HOST INTRUSTION PROTECTIONS
INTEGRATED DATA AT REST PROTECTIONS
Integrated Secure Configuration Baseline and Control System

This section will show you how to build and configure hosts and mobile devices securely.

8.1 Mobile Devices

The main purpose of this Practice Guide is to demonstrate how mobile devices can be used in a practical and effective cybersecurity architecture with PHI. The mobile devices in this build allow an authorized user to remotely access to PHI from anywhere. These devices must be secured so that they both protect themselves and the PHI data transmitted or stored on them.

This section will show you how to configure both Apple and Android mobile devices to successfully connect and securely protect PHI. This section will also show you how to setup the mobile devices to communicate and their security policy configurations managed by the Maas360 MDM.

System requirements

- Android device: Android operating system 4.1 and up, screen size 7" and up, and Wi-Fi enabled
- Apple devices: Apple iOS 7 and up, screen size 7" and up, with Wi-Fi enabled

You will also need the following parts of this guide:

- Section 3.3, Access Point: Cisco RV220W
- Section 7.1, Fedora PKI
- Section 8.2.1, MDM Setup
- Section 9.1, Cisco Identity Services Engine

8.1.1 Mobile Device Setup

This guide assumes that MaaS360 has been configured and applicable policies and rules for Android devices have been established. We also assumed that you have the corporate identifier for your MaaS360 and your Google account name and Google account password.

8.1.1.1 Register Device to MDM (Fiberlink MaaS360)

Prepare Mobile Device for MDM enrollment

1. Perform factory reset - This step is optional. If factory reset is necessary for an Android device, be sure to check the options for backing up and restoring your data (*https://support.google.com/android-one/answer/2819582*). Follow these steps to perform the factory reset:
    - On your mobile device, open the Settings menu.
    - Under Personal, tap on Backup & Reset.
    - Under Personal data, tap on Factory Data Reset.
    - After pressing Reset Device, the device will start to reboot into recovery mode and begin to wipe the tablet and return the device to its factory conditions.
    - Startup the device and follow the instructions on the screen to set up the device for a new user. Be sure the Date and Time setting is correct. Otherwise, the wrong date and time could affect the process for validating the certificates for authentication.
2. Passcode protection - Passcode protection is required for Android devices to be encrypted and enroll into the MDM. To set the passcode, follow these steps:
    - On your mobile device, open the Setting menu.
    - Under Personal, touch Security.
    - Under Screen Security, navigate to Screen Lock.

- Select the Password option.
- Follow the instructions on the screen to complete the passcode set up and record it in a safe location.

3. Device encryption - Our NCCoE security policy defined in the MDM requires the device to be encrypted for protecting data at rest. It is recommended that the device is encrypted before enrolling the device to MDM. Perform encryption using these steps:

   - Plug in the device to a power cable and allow the battery to charge. Keep the power cable connected during the encryption process.
   - On your mobile device, open the Settings menu.
   - Under Personal, touch Security.
   - Scroll to the Encrypt Tablet option.
   - Press the Encrypt Tablet button.
   - The device will reboot several times during the encryption process.
   - On completion, the device will prompt you to enter your password.

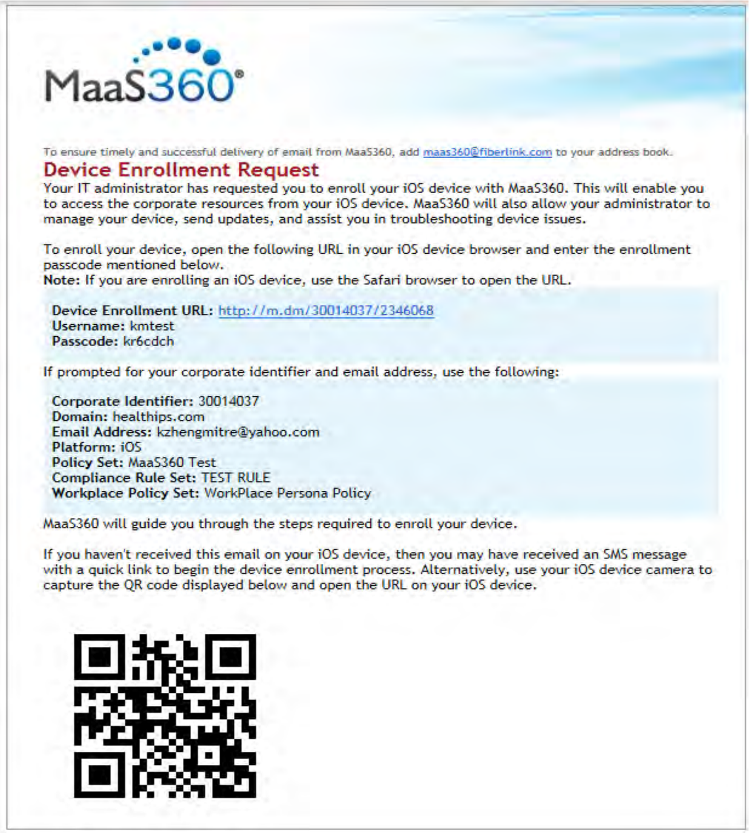
4. Wi-Fi configuration - In our NCCoE build, a dedicated Wi-Fi with SSID HealthITOrg1Reg was established in the wireless access point to allow the device to connect to the Internet for MDM enrollment and for connecting to the Certificate Authority server for requesting and importing device certificates. This Wi-Fi is protected using the WPA2 security protocol. This Wi-Fi SSID is not broadcast. Configure the device to connect to Wi-Fi using these steps:

   - On your mobile device, open the Settings menu.
   - Go to Wireless & Networks.
   - If Wi-Fi is unchecked, tap the empty box.
   - Since the SSID is not broadcast, use Add New Action to create a new Wi-Fi connection.
   - Type in all the details and be sure to select the WPA2 as the protocol and enter the correct password.
   - Check Internet connection using a public Web site such as http://*www.google.com*.

MDM enrollment - It is assumed that the device enrollment request has been done and the enrollment notification has been received via email.

1. For enrollment application:

   - Use your device to open the enrollment email as shown below:



To ensure timely and successful delivery of email from MaaS360, add maas360@fiberlink.com to your address book.

Device Enrollment Request

Your IT administrator has requested you to enroll your iOS device with MaaS360. This will enable you to access the corporate resources from your iOS device. MaaS360 will also allow your administrator to manage your device, send updates, and assist you in troubleshooting device issues.

To enroll your device, open the following URL in your iOS device browser and enter the enrollment passcode mentioned below.
Note: If you are enrolling an iOS device, use the Safari browser to open the URL.

Device Enrollment URL: http://m.dm/30014037/2346068
Username: kmtest
Passcode: kr6cdch

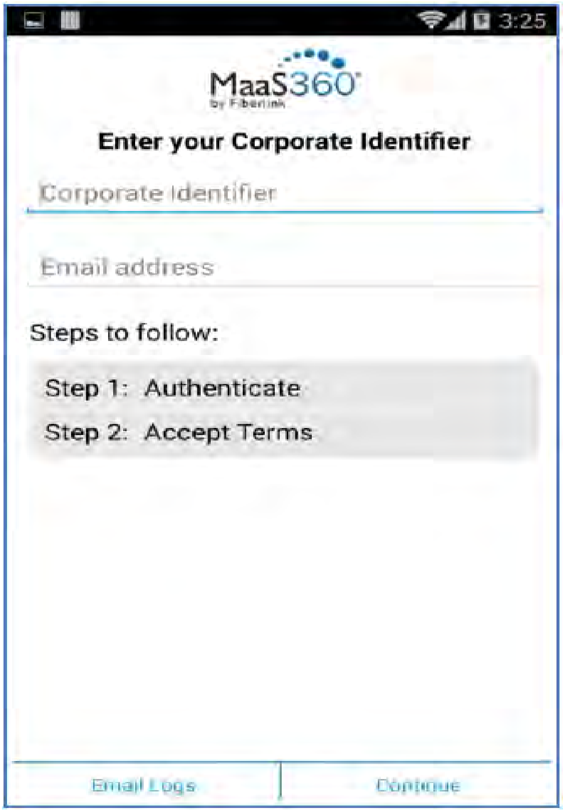
If prompted for your corporate identifier and email address, use the following:

Corporate Identifier: 30014037
Domain: healthips.com
Email Address: kzhengmitre@yahoo.com
Platform: iOS
Policy Set: MaaS360 Test
Compliance Rule Set: TEST RULE
Workplace Policy Set: WorkPlace Persona Policy

MaaS360 will guide you through the steps required to enroll your device.

If you haven't received this email on your iOS device, then you may have received an SMS message with a quick link to begin the device enrollment process. Alternatively, use your iOS device camera to capture the QR code displayed below and open the URL on your iOS device.

- Click the Device Enrollment URL to start the enrollment process, which includes these steps:
  - Download and install the MaaS360 MDM for Android app to the device.
  - Click to open the MaaS360 MDM for Android app



MaaS360 by Fiberlink

Enter your Corporate Identifier

Corporate Identifier

Email address

Steps to follow:

Step 1: Authenticate

Step 2: Accept Terms

- Fill in the Corporate Identifier and Email address as shown in the device enrollment request email.
- Press Continue to open the agreement page and select the Checkbox and press to continue.
- Press Activate to enroll the device to MDM.
- Install all the required apps.
- Apply policy and rule - Make sure the correct version of policy and rule are applied to the device.
- Verify compliance - Verify the device is compliant with all the security requirements. If not, from the Uncompliant list, click the uncompliant item to correct the problem.

8.1.1.2 Register Device in AP for MAC Address Filtering

Add MAC address and set the static IP address. Make sure the device MAC address is registered in the AP for MAC filtering service. Follow Section 3.3, Access Point: Cisco RV220W for adding a Device MAC address for MAC filtering service.

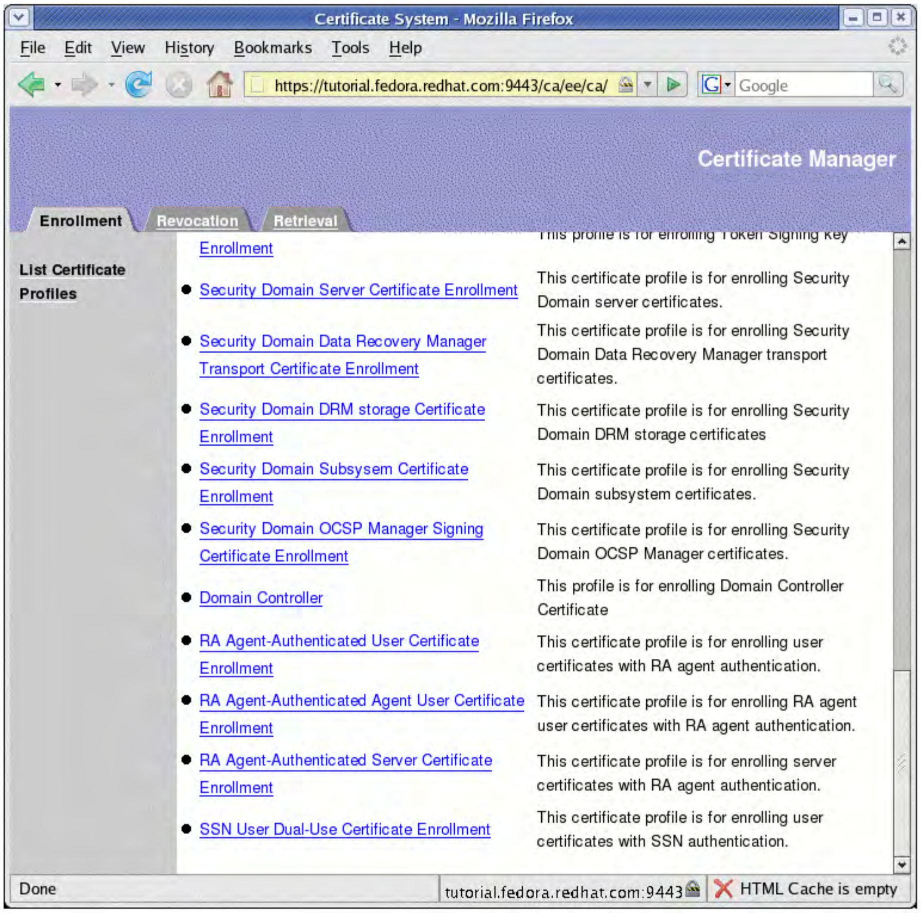
8.1.1.3 Install CA Trusted Certificates

Import certificates on Android devices - Most Android devices will import certificates from an internal or external SD card. Android OS has Credential Storage under the Settings/Security. Some old Android versions cannot recognize certain certificate formats, so additional steps are required to convert the certificate to the format being recognized by the device. For some newer versions of Android devices, directly importing and installing the certificate using a supported support browsers is possible. Below is the list of options that can be used to install a PKI certificate to the device.

Option 1. Directly install the certificate from a browser

The CA Certificate Authority server provides a browser-based interface for requesting and retrieving device certificates.

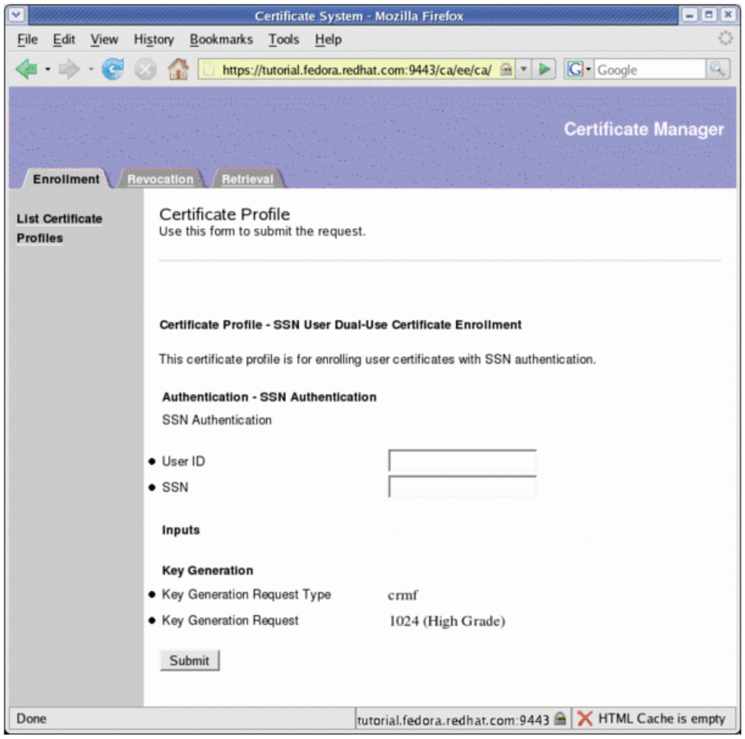
- From your device, launch a browser
- Type the URL *https://<PKI hostname>:<PKI secure EE port>* into the browser to list the CA Certificate Profiles:


Certificate System - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
https://tutorial.fedora.redhat.com:9443/ca/ee/ca/
Google
Certificate Manager
Enrollment
Revocation
Retrieval
List Certificate Profiles

Enrollment	This profile is for enrolling Token Signing key
● Security Domain Server Certificate Enrollment	This certificate profile is for enrolling Security Domain server certificates.
● Security Domain Data Recovery Manager Transport Certificate Enrollment	This certificate profile is for enrolling Security Domain Data Recovery Manager transport certificates.
● Security Domain DRM storage Certificate Enrollment	This certificate profile is for enrolling Security Domain DRM storage certificates
● Security Domain Subsysem Certificate Enrollment	This certificate profile is for enrolling Security Domain subsystem certificates.
● Security Domain OCSP Manager Signing Certificate Enrollment	This certificate profile is for enrolling Security Domain OCSP Manager certificates.
● Domain Controller	This profile is for enrolling Domain Controller Certificate
● RA Agent-Authenticated User Certificate Enrollment	This certificate profile is for enrolling user certificates with RA agent authentication.
● RA Agent-Authenticated Agent User Certificate Enrollment	This certificate profile is for enrolling RA agent user certificates with RA agent authentication.
● RA Agent-Authenticated Server Certificate Enrollment	This certificate profile is for enrolling server certificates with RA agent authentication.
● SSN User Dual-Use Certificate Enrollment	This certificate profile is for enrolling user certificates with SSN authentication.

Done | tutorial.fedora.redhat.com:9443 | HTML Cache is empty

- Select an Enrollment link and fill in the device identity in the Common Name field as shown the in page below:


Certificate System - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://tutorial.fedora.redhat.com:9443/ca/ee/ca/
Google
Certificate Manager
Enrollment
Revocation
Retrieval
List Certificate Profiles
Submit
Done
tutorial.fedora.redhat.com:9443
HTML Cache is empty

Certificate Profile
Use this form to submit the request.

Certificate Profile - SSN User Dual-Use Certificate Enrollment

This certificate profile is for enrolling user certificates with SSN authentication.

Authentication - SSN Authentication
SSN Authentication

- User ID
- SSN

Inputs

Key Generation

- Key Generation Request Type crmf
- Key Generation Request 1024 (High Grade)

- Press Submit to request the device certificate
- If successful, a request number will be given. Record this number for later use
- The CA Authority Administrator will use the Certificate system to approve or disapprove the request. (Refer to Section 7 for details.)
- Once approved, use the same interface as shown to select the Retrieval Tab.
- Enter the request number to retrieve the certificate. If successful, the certificate will be displayed on the screen with the Import button for importing the certificate to the device.
- If successful, a valid certificate will be installed to the Android device in the location at *Setting/Security/Trusted Credentials*.

> The retrieving interface provides an IMPORT action button for importing and installing the certificate to the device directly. You should use the same browser that you used for submitting the certificate request to perform this importing since the private key generally accompanies the browser.

Option 2. Use internal storage or an external SD card to install the certificate

Download an exported certificate to internal storage or an external SD card and install the certificate from there.

The exported certificate can be copied or downloaded to the internal storage or an external SD card of the device. Android devices provide a tool in the Settings/Security for installing the certificate from internal or external storage. This method will be suitable for installing the root certificate to the device.

- Go to the Settings of your Android device.
- Select Security.
- From the Credentials Storage, select Install from Storage Device to install the certificate.

Option 3. Use OpenSSL utility tool

If Option 1 or 2 does not work, there is a possibility that the specific Android device requires a special certificate format. You can use tools such as OpenSSL to generate a proper certificate and copy it to the SD card for installation. The TLS protocol utility functions provided by the open source OpenSSL may be used to handle conversion of the certificate from one format to another suitable format.

The process for acquiring the CA signed certificate using the OpenSSL command line tool is (Using CN=nccoe525 as an example):

1. Use a Linux server where the OpenSSL Utility is installed
2. Generate a new private key and Certificate Signing Request:

   openssl req –newkey rsa:4096 –days 365 keyout nccoe525.key –out nccoe525.csr –subj “/CN=nccoe525”

3. Have CA sign the certificate. The certificate request you just created in the file "*certreq.tx*" will have a blob of data looking something like this: “-----BEGIN NEW CERTIFICATE REQUEST----- ……. -----END NEW CERTIFICATE REQUEST-----“. Copy the Blob to a clipboard
4. Proceed to the CA main page at *https://example.host.com:9443/ca/services* and click on “SSL End Users Services”.
5. Select the certificate profile “Manual Administrator Certificate Enrollment”.
6. Paste the blob to the large edit box while accepting the default format ‘PKCS#10”.
7. Add the subject name: example, *CN=nccoe525*
8. Click Submit**.**
9. If successful, a request number will be displayed for future retrieval of the approved certificate.
10. CA admin will verify the request and approve the certificate.
11. Retrieve the approved certificate using the Retrieval tab in the CA main page and save it as a certificate file. In the Retrieval tab, fill in the request number and submit it to get the certificate content. From the opening Certificate content, copy this under the Base 64 encoded certificate from the line “-----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----“.
12. Use the copied blob to create a certificate file, e.g *nccoe525.crt*. If there is a *.txt* extension associated with this file, remove it.
13. Move this file to the Linux server in the location where the private key file is located.
14. Use the OpenSSL command to bind the signed certificate with the private key file and convert the certificate to a p12 file so that it may be installed in most browsers:

```
openssl pkcs12 -export -clcerts -in nccoe525.crt -inkey
   nccoe526.key -out nccoe526.p12
```

15. Save this file and transfer it to the device's internal or external storage.
16. Install the certificate as shown in Option 2.

8.1.1.4 Configure Wi-Fi for EAP-TLS authentication

With the certificates in place, you are ready to connect to the wireless network that requires the certificate as the authentication mechanism. Use the following steps to setup Wi-Fi in an Android device with EAP-TLS authentication:

1. Go to Wi-Fi settings for the Android device
2. Enter the following items:
   - EAP method: TLS
   - Phase 2 authentication: None
   - CA certificate: Name of your RootCA
   - User certificate: Name of your device certificate
3. Click Save. You should be now connected to the network using EAP-TLS authentication.
4. In this build, we used a protected website, *https://www.healthisp.com*, to verify whether the EAP-TLS authentication was successful or not.

8.1.2 Setup Apple Mobile Devices to Support EAP-TLS Authentication

It is assumed that the MaaS360 has been configured and applicable policies and rules for Apple iOS devices have been established. It is also assumed that you have the corporate identifier for your MaaS360 and your Apple ID for the device.

8.1.2.1 Register Device to MDM (Fiberlink MaaS360)

Prepare Device for MDM enrollment

1. Perform factory reset - This step sets the device to its factory default setting for a new owner and erases the original settings, data, and applications to prevent unknown and harmful applications remaining on the device. If a factory reset is necessary for an Apple device, be sure to check options for backing up and restoring your data (*https://support.apple.com/en-us/HT203977*). Following these steps to perform the factory reset:
   - On your Apple device, open the Settings menu.
   - Under General, tap on Reset.
   - Under Reset, tap on Erase All Content and Settings.
   - You will have to confirm your selection to set your device to the factory default.
   - After you confirm your choice, the device will begin the reset process.
   - Restart your device and follow the on screen instructions to setup the device for a new owner.
2. Passcode protection and device encryption **-** Passcode code protection is required for iOS devices to be encrypted and enroll into the MDM. Setting a passcode in the iOS device will also enable encryption on the device. To set the passcode, follow

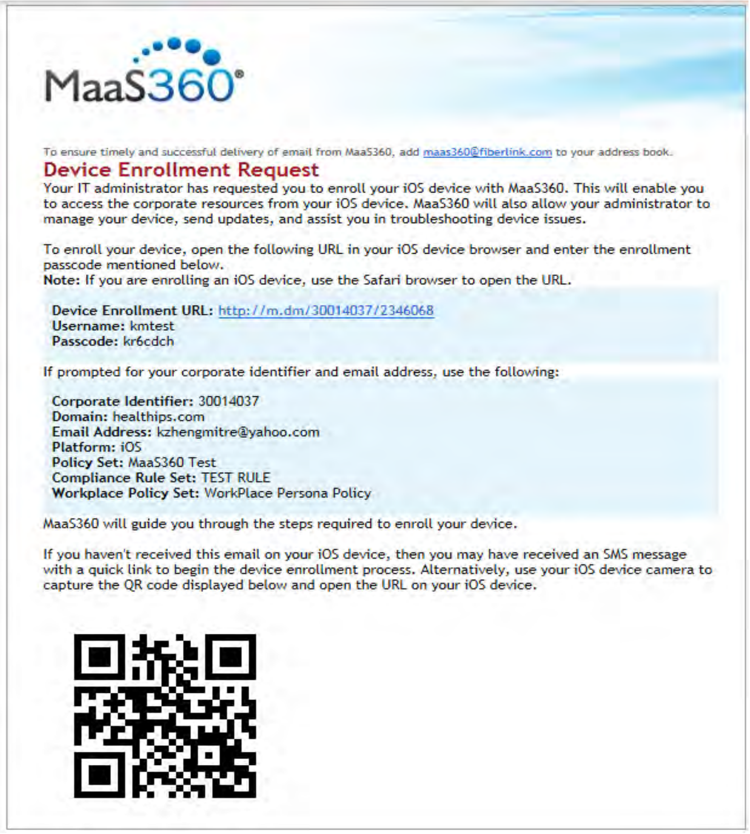
these steps:

- On your mobile device, open the Settings menu.
- Under General, go to Passcode Lock and press Turn Passcode On.
- Under Screen Security, navigate to Screen Lock.
- When you turn on the passcode, you also enable encryption on your iOS devices.

3. Wi-Fi configuration - In our NCCoE build, a dedicated Wi-Fi with SSID HealthITOrg1Reg was established in the wireless Access Point to allow a device to connect to the Internet for MDM enrollment and to the CA certificate Authority server to request and import device certificates. This Wi-Fi is protected using the WPA2 security protocol. This Wi-Fi SSID is not broadcast. Configure the device to connect to Wi-Fi using these steps:
    - On your mobile device, open the Settings menu.
    - Tap Wi-Fi.
    - When Wi-Fi is on, the device will automatically search for available Wi-Fi networks.
    - Join the hidden Wi-Fi network with no broadcast SSID: Under the Choose a Network section, tap on Other.
    - In Name, put the exact Wi-Fi network SSID you want to connect.
    - Tap on Security and choose the type of network encryption used. (For the NCCoE build, WPA2 is used).
    - Return back to the primary connection screen.
    - Enter the Wi-Fi SSID password and tap on Join to connect to the hidden wireless network.

MDM Enrollment - It is assumed that the device enrollment request has been completed and the enrollment notification has been received via email.

1. For enrollment application
    - Enroll your iOS device using the URL provided to you via the enrollment email from MaaS360 (an example is shown below). Click the URL provided. Alternatively, you can open the Safari browser on the device and enter the URL manually.



To ensure timely and successful delivery of email from MaaS360, add maas360@fiberlink.com to your address book.

Device Enrollment Request

Your IT administrator has requested you to enroll your iOS device with MaaS360. This will enable you to access the corporate resources from your iOS device. MaaS360 will also allow your administrator to manage your device, send updates, and assist you in troubleshooting device issues.

To enroll your device, open the following URL in your iOS device browser and enter the enrollment passcode mentioned below.
Note: If you are enrolling an iOS device, use the Safari browser to open the URL.

Device Enrollment URL: http://m.dm/30014037/2346068
Username: kmtest
Passcode: kr6cdch

If prompted for your corporate identifier and email address, use the following:

Corporate Identifier: 30014037
Domain: healthips.com
Email Address: kzhengmitre@yahoo.com
Platform: iOS
Policy Set: MaaS360 Test
Compliance Rule Set: TEST RULE
Workplace Policy Set: WorkPlace Persona Policy

MaaS360 will guide you through the steps required to enroll your device.

If you haven't received this email on your iOS device, then you may have received an SMS message with a quick link to begin the device enrollment process. Alternatively, use your iOS device camera to capture the QR code displayed below and open the URL on your iOS device.

- Clicking the Device Enrollment URL will start the enrollment process.
- The enrollment steps include Authenticate, Accept Terms, Download & Install Profile, and Install MaaS360 for iOS App to the device.
- Click Continue to proceed and follow the instructions to provide necessary authentication information from the enrollment email, such as passcode and Corporation Identifier.
- Accept terms. You must agree to the Fiberlink end user agreement to enroll your device.
- The device will start to install the MDM Profile. Press Continue. The profile will enable the MaaS360 Administrator to manage the device using MaaS360. Click Install to install the profile and accept any prompts for profile installation to continue with the enrollment.
- After the profile is installed, you will be prompted to install the required MaaS360 app from the Apple App Store.
- Return to the home screen and locate the MaaS360 app. Tap the MaaS360 icon to install the Fiberlink MDM for iOS app.
- The installation may request permission to use your location information and your permission to send you push notifications. Accept these requests by clicking the OK button.
- You device is enrolled in MaaS360 now.

- Apply policy and rule - From the home screen, locate the MaaS360 icon. Tap on it to display the device general information and the device policy. Make sure the correct versions of policy and rules are applied to the device.
- Verify compliance - Verify the device is compliant with all the security requirements. If not, from the uncompliant list, click the uncompliant item to correct the problem.

8.1.2.2 Register Device in AP for MAC Address Filtering

Add MAC address and set the static IP address. Make sure the device MAC address is registered in the AP for MAC filtering service. Follow Section 3.3, Access Point: Cisco RV220WM for adding a Device MAC address for MAC filtering service.

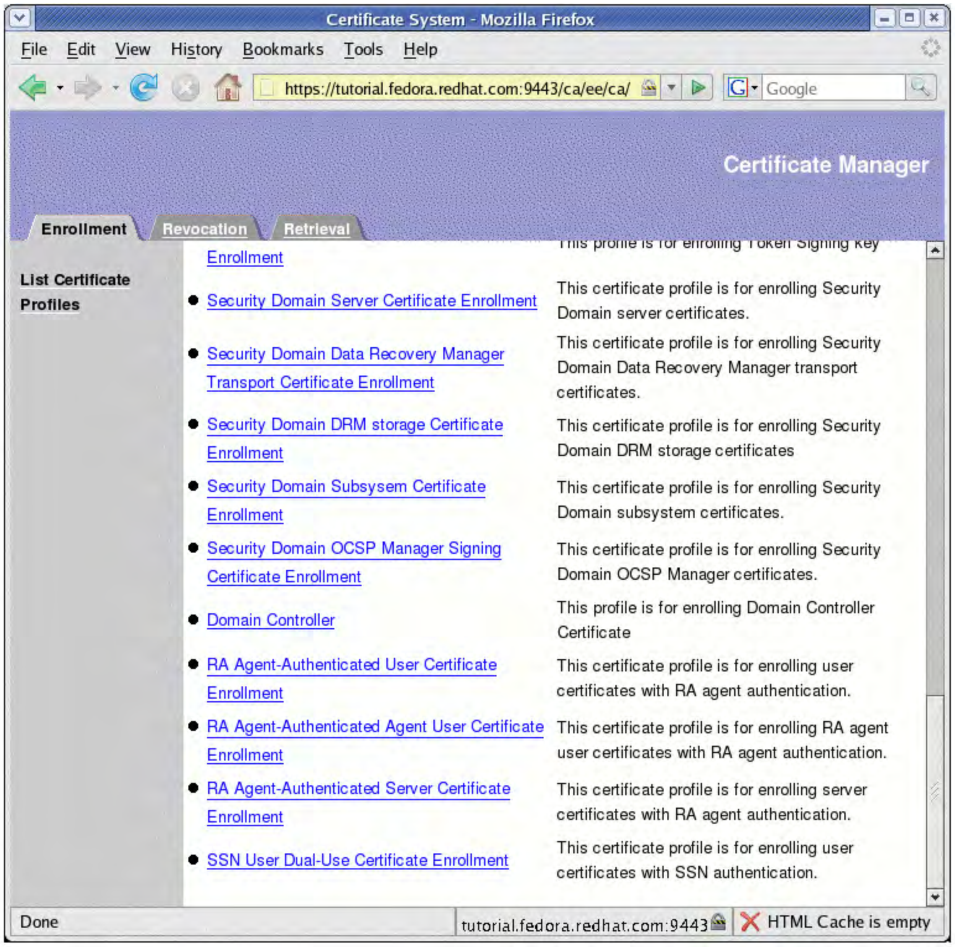
8.1.2.3 Install CA Trusted Certificates

Import certificates on iOS Devices - Most of the iOS devices will import certificates from *.*p12* or **pfx* files sent to your device as an attachment in an email. We recommend this email is encrypted using TLS. Below is the list of options that can be used to install a PKI certificate to the device.

Option 1. Directly install the certificate from browser

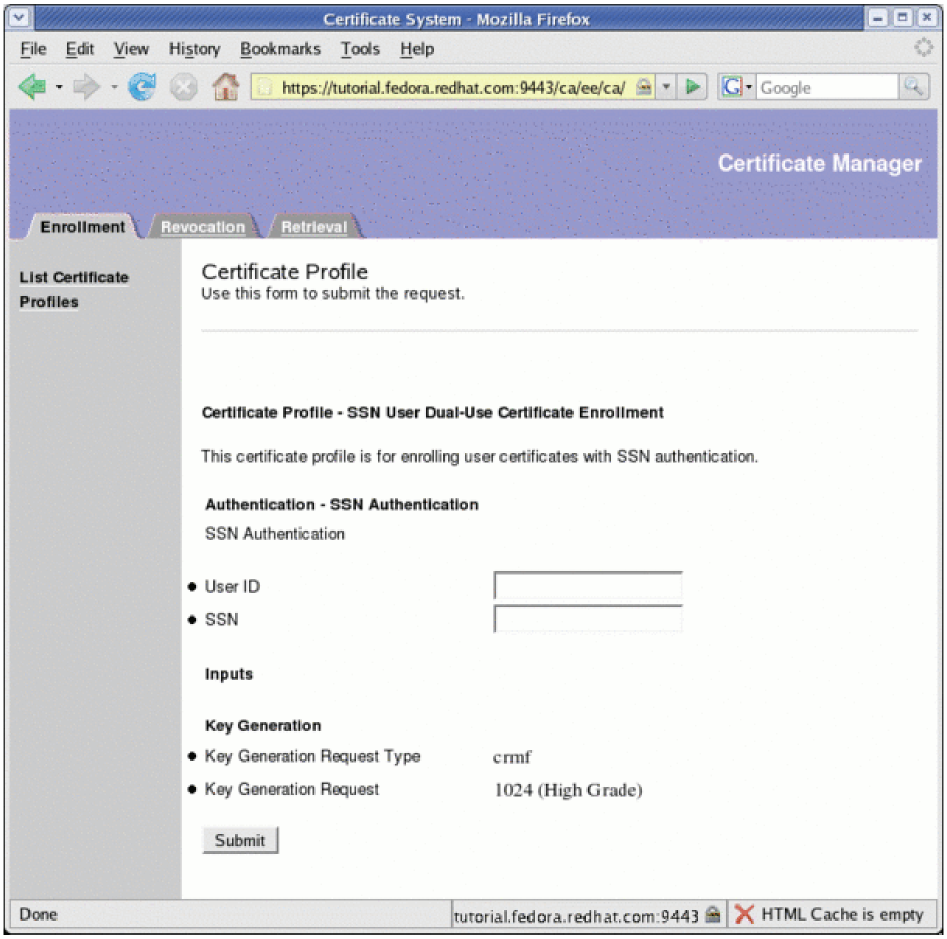
The CA Certificate Authority server provides a browser-based interface for requesting and retrieving device certificates.

- From your device, launch a browser
- Type the URL *https://<PKI hostname>:<PKI secure EE port>* into the browser to list the CA Certificate Profiles:


Certificate System - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://tutorial.fedora.redhat.com:9443/ca/ee/ca/
Google
Certificate Manager
Enrollment
Revocation
Retrieval
List Certificate Profiles
Done
tutorial.fedora.redhat.com:9443
HTML Cache is empty

Enrollment	This profile is for enrolling Token Signing key
● Security Domain Server Certificate Enrollment	This certificate profile is for enrolling Security Domain server certificates.
● Security Domain Data Recovery Manager Transport Certificate Enrollment	This certificate profile is for enrolling Security Domain Data Recovery Manager transport certificates.
● Security Domain DRM storage Certificate Enrollment	This certificate profile is for enrolling Security Domain DRM storage certificates
● Security Domain Subsysem Certificate Enrollment	This certificate profile is for enrolling Security Domain subsystem certificates.
● Security Domain OCSP Manager Signing Certificate Enrollment	This certificate profile is for enrolling Security Domain OCSP Manager certificates.
● Domain Controller	This profile is for enrolling Domain Controller Certificate
● RA Agent-Authenticated User Certificate Enrollment	This certificate profile is for enrolling user certificates with RA agent authentication.
● RA Agent-Authenticated Agent User Certificate Enrollment	This certificate profile is for enrolling RA agent user certificates with RA agent authentication.
● RA Agent-Authenticated Server Certificate Enrollment	This certificate profile is for enrolling server certificates with RA agent authentication.
● SSN User Dual-Use Certificate Enrollment	This certificate profile is for enrolling user certificates with SSN authentication.

- Select an Enrollment link and fill in the device identity in the Common Name field as shown the in page below:


Certificate System - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://tutorial.fedora.redhat.com:9443/ca/ee/ca/
Google
Certificate Manager
Enrollment
Revocation
Retrieval
List Certificate Profiles
Submit
Done
tutorial.fedora.redhat.com:9443
HTML Cache is empty

Certificate Profile
Use this form to submit the request.

Certificate Profile - SSN User Dual-Use Certificate Enrollment

This certificate profile is for enrolling user certificates with SSN authentication.

Authentication - SSN Authentication

SSN Authentication

- User ID
- SSN

Inputs

Key Generation

• Key Generation Request Type	crmf
• Key Generation Request	1024 (High Grade)

- Then press Submit to request the device certificate.
- If successful, a request number will be given. Record this number for later use.
- The CA Authority Administrator will use the Certificate system to approve or disapprove the request. (Refer to Section 7 for details.)
- Once approved, use the same interface as shown to select the Retrieval Tab.
- Enter the request number to retrieve the certificate. If successful, the certificate will be displayed on the screen with the Import button for importing the certificate to the device.
- If successful, a valid certificate will be installed to the iOS device in the location at *Setting/General/Profile & Device Management*.

The retrieving interface provides an IMPORT action button for importing and installing the certificate to the device directly. You should use the same browser as you used for submitting the certificate request to perform this importing since the private key generally accompanies the browser.

Option 2. Use email attachment to install the certificate

- Open the certificate file from an email with the certificate as the attachment. The install process will start.
- At the Install Profile screen, press the Install button.
- If you are prompted with a warning messaging saying: "Installing this profile will change settings on your iPhone," press the Install Now button.
- You may need to enter the passcode that you set for the device.
- Once the certificate installation has finished, you will see a screen showing your certificate.
- Press Done to exit the installation process.

Option 3. Use OpenSSL utility tool

You can use tools such as OpenSSL to generate a proper certificate and copy it to the SD for installation. In case the above methods do not work, there is a possibility that the specific device requires a special certificate format. The TLS protocol utility functions provided by the open source OpenSSL may be used to handle conversion of the certificate from one format to another suitable format so installation of a certificate on this device becomes possible.

The process for acquiring the CA signed certificate using the OpenSSL command line tool is (using CN=nccoe525 as an example) :

1. Use a Linux server where the OpenSSL Utility is installed
2. Generate a new private key and Certificate Signing Request:

   openssl req –newkey rsa:4096 –days 365 keyout nccoe525.key –out nccoe525.csr –subj "/CN=nccoe525"

3. Have CA sign the certificate. The certificate request you just created in the file "certreq.tx" will have a blob of data looking something like this: "-----BEGIN NEW CERTIFICATE REQUEST----- ……. -----END NEW CERTIFICATE REQUEST-----". Copy the Blob to a clipboard
4. Proceed to the CA main page at *https://example.host.com:9443/ca/services* and click on "SSL End Users Services".
5. Select the certificate profile "Manual Administrator Certificate Enrollment".
6. Paste the blob to the large edit box while accepting the default format 'PKCS#10".
7. Add the subject name: example, *CN=nccoe525*
8. Click Submit**.**
9. If successful, a request number will be displayed for future retrieval of the approved certificate.
10. CA admin will verify the request and approve the certificate.

11. Retrieve the approved certificate using the Retrieval tab in the CA main page and save it as a certificate file. In the Retrieval tab, fill in the request number and submit it to get the certificate content. From the opening Certificate content, copy this under the Base 64 encoded certificate from the line “-----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----“.
12. Use the copied blob to create a certificate file, e.g *nccoe525.crt*. If there is a *.txt* extension associated with this file, remove it.
13. Move this file to the Linux server in the location where the private key file is located.
14. Using the OpenSSL command to bind the signed certificate with the private key file and convert the certificate to a p12 file so that it may be installed in most browsers:

```
openssl pkcs12 -export -clcerts -in nccoe525.crt -inkey
   nccoe526.key -out nccoe526.p12
```

15. Save this file and transfer it to the iOS device using secure email.
16. Install the certificate as shown in Option 2.

8.1.2.4 Configure Wi-Fi for EAP-TLS Authentication

With the certificates in place (CA Root certificate and the device certificate), you are ready to connect your iOS device to the wireless network that requires the certificate as the authentication mechanism. Use the following steps to setup Wi-Fi in an iOS device with EAP-TLS authentication

1. Go to the Wi-Fi settings for the iOS device
2. Click Other Network to enter the following items:
    - Name of the SSID
    - Security: WPA2 Enterprise
    - Return to Other Network page
    - Click Mode
    - Select EAP-TLS as the Mode
    - Return to Other Network page
    - Enter the Username that has been assigned to this device
    - Click Identify to list all the certificates
    - Select the one registered for the device
    - Click Join to connect to the network
3. You should be now connected to the network using EAP-TLS authentication
4. In this build, we used the protected website *https://www.healthisp.com* to verify if the EAP-TLS authentication was successful

8.2 MaaS360

The MDM selected for this build is based on the MaaS360 product. Maas360 is a cloud based solution that is responsible for managing polices on each mobile device. An administrator can enforce the corporate mobile policies without logging into each device. This action will manage one or more centralized policies for distribution to all devices with the Maas360 agent installed. MaaS360 can group policies, users, and mobile devices, then distribute unique policies based on their roles.

This section will show you how to install one of our predefined policies

System Requirements

- A computer system for accessing the cloud version of MaaS360 Administration Portal
- Internet connectivity and Internet browsers installed
- Windows Phone Company Hub certificate

You will also need the following parts of this guide:

- Section 3.3, Access Point: Cisco RV220W
- Section 7.1, Fedora PKI
- Section 8.2.1, MDM Setup
- Section 9.1, Cisco Identity Services Engine

8.2.1 MDM Setup

8.2.1.1 Enable Mobile Device Management Service

It is assumed that a MaaS360 account has been established with Fiberlink. If no account has been established, contact Fiberlink for more information on how to request a user account (*http://www.maas360.com/*). It is also assumed that the required Windows Phone Company Hub and the Apple APNS certificates have been acquired. For detailed information on how to acquire these required certificates, please refer to the document *(http://content.maas360.com/www/support/mdm/assets/APNS_CertRenewalGuide.pdf*) for Apple MDM certificate and the document (*http://content.maas360.com/www/pdf/Win%20Phone%208%20Company%20Hub.pdf*) for MaaS360 Windows Phone 8 Company Hub Certificate.

1. Add the Apple MDM Certificate for managing Apple devices
    - Log on to MaaS360 dashboard using *https://logon.maas360.com*
    - Navigate to *Setup* > *Services***,** click *Mobile Device Management***.**
    - Click Apple MDM Certificate and use the Browser to load the certificate file.
2. Add Windows Phone Company Hub certificate for managing Windows Phones
    - Log on to MaaS360 dashboard using *https://logon.maas360.com*
    - Navigate to *Setup* > *Services*, click *Mobile Device Management*.
    - Expand the Windows Phone Company Hub certificate by pressing the "+" symbol.
    - Use the browser to load and install the certificate to the MDM.

8.2.1.2 Enable Security Policies for Mobile Devices

1. Create a new policy for a type of device

- Log on to the MaaS360 dashboard using *https://logon.maas360.com*
- Navigate to *Security* > *Polices*, click *Add Policy*
- Add a Name, e.g**.** Lab_Only_ISO
- Add Description
- Select a Type from the dropdown list: (e.g. IOS MDM)
- Use a Start From dropdown list to copy an existing policy for this new policy
- Click Continue to create a new policy for the type of device.

2. Edit and refine the created policies
   - Log on to MaaS360 dashboard using *https://logon.maas360.com*
   - Navigate to Setup > Policies.
   - From the Policy list, click View to view a selected Policy.
   - Review each item in the policy to make sure they are set per your security policy and business requirement.
   - If the policy settings do not meet your security requirement, click the Edit button to enter the edit mode.
   - Change the values to your desired values.
   - Click Save to save the changes or click Save and Publish to save and publish the new policy.
   - Enter the password and press Continue.
   - Click Confirm Publish to complete this edition and the new policy will be assigned with a new version number. You can use this version number to verify that the devices controlled by this policy are enforced by this version of the policy.

If the policy is set to be extremely restrictive, it can lock you out of the mobile device and make it very difficult to unlock.

8.2.1.3 Enable Security Compliance Rule for Mobile Devices

1. Create a new rule set
   - Log on to MaaS360 dashboard using *https://logon.maas360.com*
   - Navigate to *Security* > *Compliance Rules*, click *Add Rule Set*
   - Add a Name, e.g. HIT-RULE
   - Copy an existing rule set for the new rule from the Copy From dropdown list
   - Click Continue to create a new rule.
2. Edit and refine the newly created rule
   - Log on to theMaaS360 dashboard using *https://logon.maas360.com*

- Navigate to *Security* > *Compliance Rules*
- Click Edit for the selected rule you want to review and edit
- From the Basic Settings, under Select Applicable Platforms, check the checkbox next to an OS's name to Enable the Real-Time Compliance for OS's.
- In the Event Notification Recipients fill in the emails you want to notified in case of noncompliance.
- Use the navigation tree to view and set other rules per your security and operational requirements.
- Click Save to save the newly set rules.

8.2.1.4 Add Applications to be Distributed to Mobile Devices

1. Add App to App Catalog
    - Log on to MaaS360 dashboard using *https://logon.maas360.com*
    - Navigate to *APPS* > *Catalog***,** click *Add* to select Apps from different app stores.
    - In the popup page, type a key word for the App in the search box to list the available Apps.
    - Select the app you want and click Add button to add the app into the category.
2. Add App to Bundles for Distribution
    - Log on to the MaaS360 dashboard using *https://logon.maas360.com*
    - Navigate to *APPS* > *Bundles*, click *Add App Bundles* to open the App Bundle window.
    - In the popup page, enter a Bundle Name and Description for the bundle. Then enter the App Names in the App Name field. Use a comma to separate the apps.
    - Click Add button to add the App Bundle.
    - From the App Bundle list, click Distribute button to set the distribution Target.

8.2.1.5 Add Device Group to Manage Mobile Devices

1. Add Device Group
    - Log on to MaaS360 dashboard using *https://logon.maas360.com*
    - Navigate to *Users* > *Groups***,** click *Create Device Group* to create a new Group.
    - Enter a group name and description from the Device Group Details window and specify the group Type.
    - Click Save to save the setting.
2. Configure Group
    - The group can be configured to include devices, policy, rules, etc. Devices in the same group will share the same settings as configured for the group.

- Detailed settings for group properties can be referenced in the MDM manual. *http://content.fiberlink.com/www/support/assets/MaaS360ServicesUserGuide.pdf*

8.2.1.6 Device Enrollment

- iOS MDM Enrollment is described in Section 0
- Android MDM Enrollment is described in Section 8.2.1.6

8.3 Host Based Security

Both the notional Data Center and the HealthIT Organizations in this build have systems that need protection from viruses and malware. As with most of the capabilities selected for this build, the Symantec Endpoint Protection service provides an enterprise class ability to manage host security policy for multiple systems. These managed systems could be local to the server or remotely across the world. An organization with the proper skilled resources on staff could manage traditional servers and hosts or allow an ISP like the notional Data Center in this build.

8.3.1 Symantec Endpoint Protection Suite

The Symantec Endpoint Protection server provides the following options:

- Local Host Intrusion Prevention System(IPS) will block traffic before it traverses the network
- Utilizes a global intelligence network service to remain current on threats
- Supports Windows, Linux and Mac systems
- Centralized management console

The Data Center in this build only manages the local servers in the Data Center. Symantec will be working with the NCCOE team in future iterations of this build to integrate mobile device malware and virus management with its Endpoint Protection product.

System requirements

Processor	Minimum 1.4 GHz 64-bit processor
RAM	Minimum 8G
Disk space	Minimum 150 GB

You will also need the following parts of this guide:

- Section 11.1, Windows Installation and Hardening
- Section 3.1, Hostnames

Symantec Setup

To set up Symantec Endpoint Protection, follow the installation and Administration guide at *https://support.symantec.com/en_US/article.DOC7698.html*

9 Identity and Access Control

This build utilizes a radius server integrated with our CA and AP which combines to create the full identity and access control function. A radius server uses the AAA protocol to manage network access via authentication, authorization and accounting. Authentication and authorization are of particular focus in the identity and access process used in this build. The authentication mechanism is integrated with the root certificate authority as a recipient of a signed root cert and OCSP communication. The authorization mechanism is integrated with the MDM to check mobile device policy for compliance.

9.1 Cisco Identity Services Engine

The Cisco Identity Services Engine (ISE) provides the ability to do the following:

- Centralize and unify identity and access policy management
- Visibility and more assured device identification through certificate challenges
- Organizations can use business rules to segment access to sections of the network
- Even with more assured and stronger authentication, the user experience during the challenge process is made seamless

System requirements

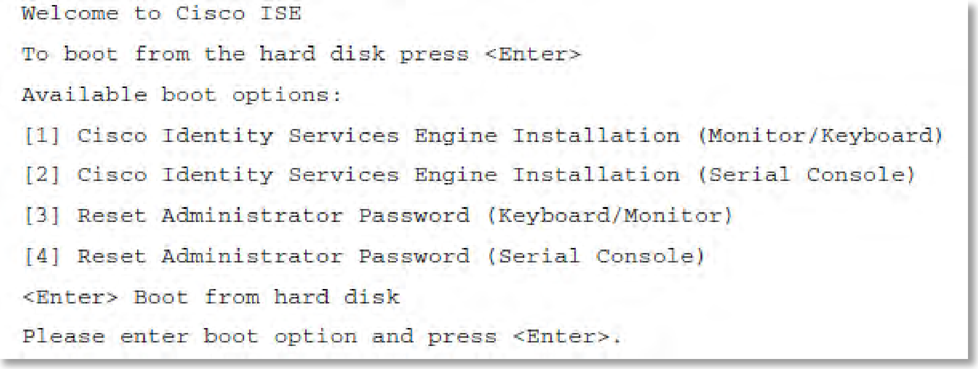
- Virtual Hypervisor (VH) capable of housing virtual machines (VMs)
- VM with CPU: Single Quad-core; 2.0 GHz or faster
- VM with minimum 4 GB memory
- VM with minimum 200 GB disk space

You will also need the following parts of this guide:

- Section 7.1, Fedora PKI
- Section 8.2.1, MDM Setup

Cisco ISE Setup

1. Download the Cisco ISE 1.2 ISO from *https://software.cisco.com/download/release.html?mdfid=283801620&softwareid=283802505&release=1.2*. Either use the ISO image or burn the ISO image on a DVD, and use it to install Cisco ISE 1.2 on a virtual machine
2. Follow the guidance from your VM vendor to boot the DVD or ISO and start the install process
3. Once the system boots up, follow the console display to select one of the installation options shown below:



```
Welcome to Cisco ISE
To boot from the hard disk press <Enter>
Available boot options:
[1] Cisco Identity Services Engine Installation (Monitor/Keyboard)
[2] Cisco Identity Services Engine Installation (Serial Console)
[3] Reset Administrator Password (Keyboard/Monitor)
[4] Reset Administrator Password (Serial Console)
<Enter> Boot from hard disk
Please enter boot option and press <Enter>.
```

4. Select Option 1 to start the installation.
5. Once the installation is complete, the system prompts for the network setup through the

command-line interface (CLI).

6. Enter the required parameters, below, to configure the network. If you would like to use our IP and hostname address scheme, refer to Section 3.1, Hostnames.
   - Hostname
   - Ethernet interface address
   - Default gateway
   - DNS domain name
   - Primary name server
   - Username and Password for use for the command line interface (CLI) and the admin portal access are provided by the Cisco ISE

More detailed procedures for installing the Cisco ISE is available from the installation guide provided by Cisco, available at *http://www.cisco.com/c/en/us/td/docs/security/ise/1-2/installation_guide/ise_ig/ ise_vmware.html#pgfId-1057864*

9.2 Cisco ISE Post-Installation Tasks

> Management of the Cisco ISE should be executed with a web browser unless you intend to administer via command line. All instructions in this guide for managing the Cisco ISE product relate to use of the graphical user interface.

1. Using a web browser and the Cisco ISE host address, log on to the Cisco ISE Administration Portal. You will use the credentials (username and password) created during the installation procedure.
2. From the Administration Portal, click the Setup Assistant.
3. Follow the wizard interface to set up the basic operating configuration and default settings for authentication, authorization, profiling, posture, client provisioning, guest services, and support for personal devices.

9.3 Configure CISCO ISE to Support EAP-TLS Authentication

9.3.1 Set ISE to support RADIUS authentication

The following steps are used to set up a communication connection from Cisco ISE to the network device (Access Point) used as the authenticator in the RADIUS authentication:

1. From the Admin Portal, navigate to the path: *Administration* > *Network Resources* > *Network Devices*. Then select *Add*.
2. Fill out the required parameters as indicated in the form:
   - The name of the network device,
   - The IP Address of the device with its subnet mask,
   - Select the RADIUS protocol as the selected protocol, and
   - Enter the shared secret that is configured on the network device.

There are many advanced optional RADIUS settings in the ISE network device definition. For example, KeyWrap helps increase RADIUS communication security via use of the AES KeyWrap algorithm. However, you should be experienced with Cisco ISE and confident that your network device supports this configuration.

9.3.2 Enable PKI in Cisco ISE

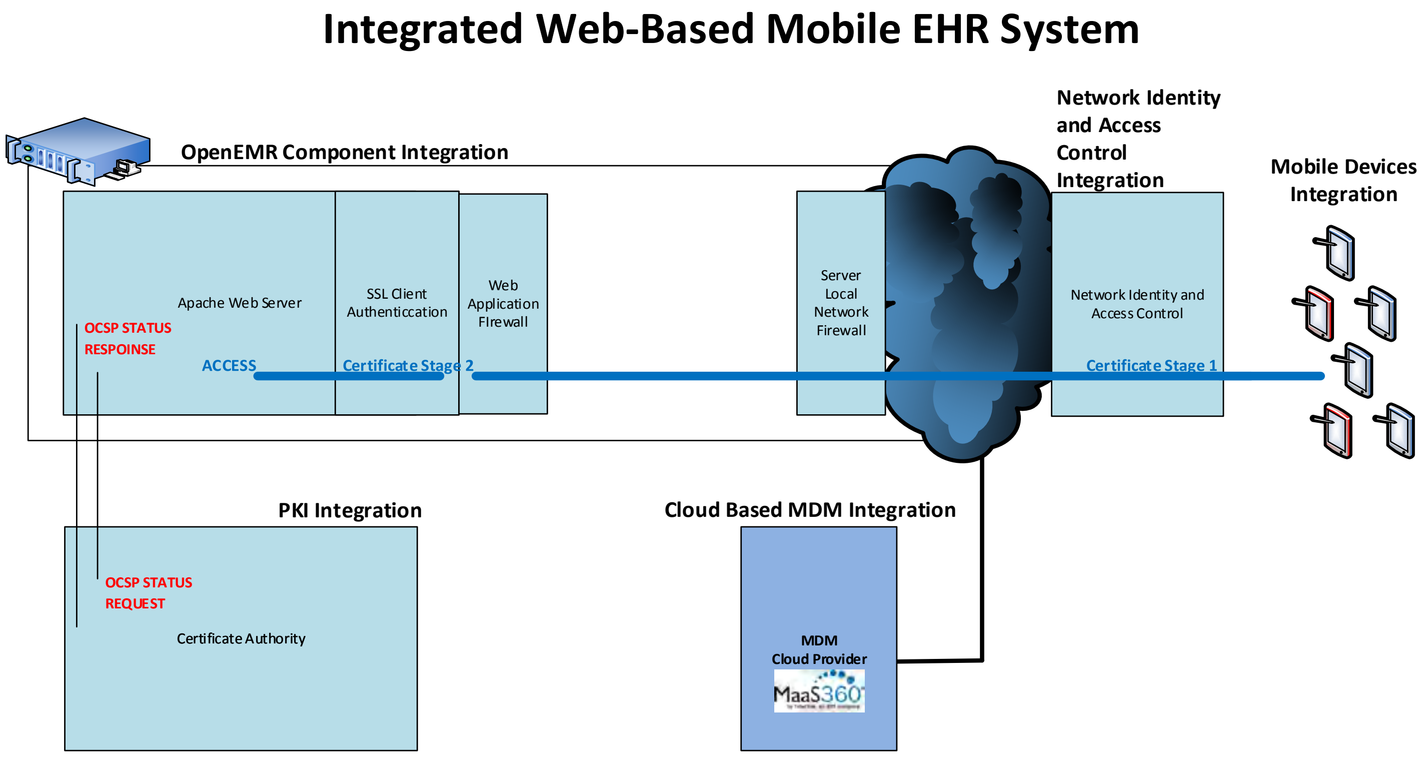
We replaced the Cisco ISE default self-signed certificate with the CA-signed certificate issued through our Certificate Authority. The steps are:

1. Generate a certificate signing request (CSR) through the Cisco ISE navigation path *Administration > System > Certificates > Local Certificates*.

Ensure the CN field matches the Fully Qualified Domain Name of the Cisco ISE server.

2. Export the Certificate Signing Request from the navigation path *Administration > System > Certificates >Certificate Signing Requests,* then select *Export*
3. Save and submit the Certificate Signing Request file to a Certificate Authority. From there, the content of the CSR described in the text from "-----BEGIN CERTIFICATE REQUEST-----" through "-----END CERTIFICATE REQUEST-----." is used for generating the signed certificate in CA for the specific server.
4. The process for signing the CSR is described in Section 7, Certificate Authority
5. Use the ISE Administration interface to bind the acquired CA-signed certificate with its private key using the path *Administration > System > Certificates > Local Certificates then Add>Bind CA Signed Certificate*

If you intend to use this certificate for client EA-TLS authentication, as we did in the NCCoE build, designate the certificate for EAP-TLS use when binding the certificate. The client needs this certificate to identify the Cisco ISE server for EAP protocols.



Architecture

9.3.3 Populate Certificate Store with Required CA-signed Certificates

The CA-signed root certificate, as well as the certificate for Fiberlink MaaS360 MDM server, are required by the Certificate Store. You will need to have the CA root certificate in PEM or DER format.

To import the CA-signed root certificates to the certificate store:

1. Obtain a CA-signed root certificate from the Trusted CA Administrator. The procedure for generating the root cert is described in Section 7, Certificate Authority
2. From the ISE Administration Portal, use the navigation path *Administration* > *System* > *Certificates* > *Certificate Store* to perform the import action.

Follow Steps 1 and 2 to import the Fiberlink MaaS360 MDM certificate to Cisco ISE so that ISE can communicate with Fiberlink MaaS360 MDM.

9.3.4 Set Identity Source for Client Certificate **Authentication**

No internal or external identity source is required for the EAP-TLS certificate-based authentication method, since the identity is validated based on the trusted certificate in the PKI. However, you must set up the Certificate Authentication Profile in the ISE as the external identity source. Instead of authenticating via the traditional username and password, Cisco ISE compares a certificate received from a client with one in the server to verify the authenticity of a user or device. Note that although internal or external identity sources are not needed for TLS authentication, internal or external identity sources can be added and used for authorization of a policy condition, if desired.

To create a Certificate Authentication Profile:

1. Use the Administration Portal to navigate to the path *Administration* > *Identity Management* > *External Identity Sources* > *Certificate Authentication Profile* and click *Add*.
2. Fill out the form with proper parameters. Be sure to select the Subject Name as the Principal Username X509 attribute because it is the field that will be used to validate the authenticity of the client.

9.3.5 Set Authentication Protocols

Cisco ISE uses authentication protocols to communicate with external identity sources. Cisco ISE supports many authentication protocols such as the Password Authentication Protocol (PAP), Protected Extensible Authentication Protocol (PEAP), and the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). For this build, we used the EAP-TLS protocol for user and machine authentication.

To specify the allowed protocols services in Cisco ISE:

1. From the Administration Portal navigate to the path *Policy >Policy Elements* > *Results >Authentication* > *Allowed Protocols* > *Add*
2. Select the preferred protocol or list of protocols. In this build, the *EAP_TLS* is selected as the allowed authentication protocol.

9.3.6 Configure Cisco ISE to Integrate with Fiberlink MaaS360

1. Establish basic connectivity between the Cisco ISE server and the Fiberlink MaaS360 MDM server. As indicated in the architecture diagram, firewalls are installed between the

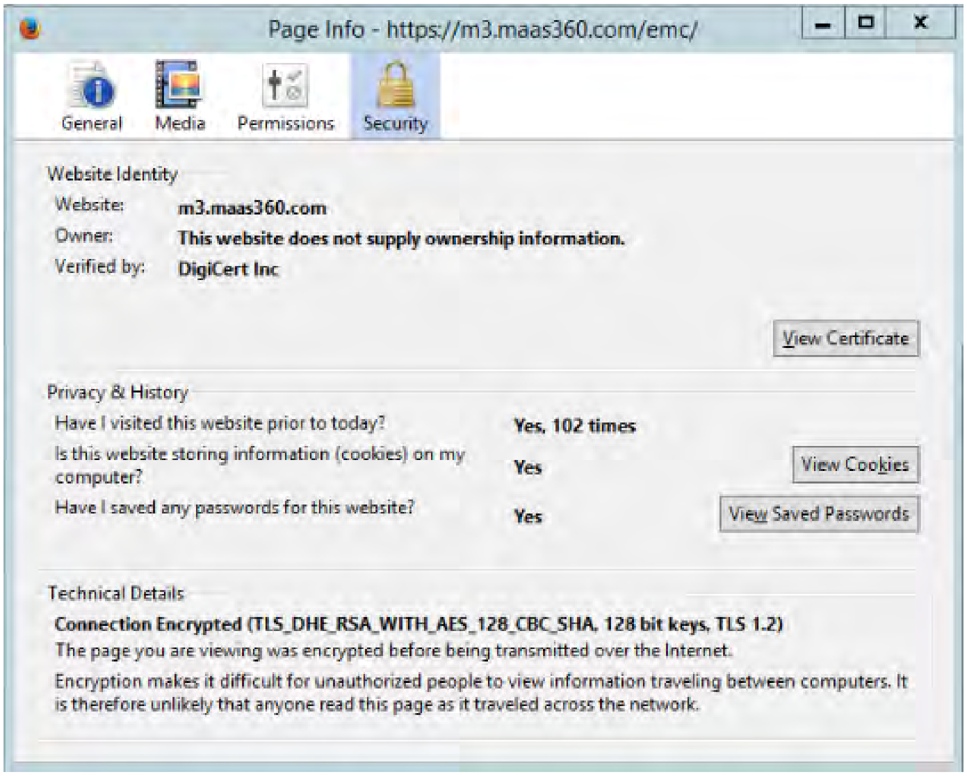
ISE and the Fiberlink MaaS360 in the cloud. The firewall should be configured to allow an HTTPS session from the ISE to the Fiberlink MaaS360 server located in the public Internet. The session is established outbound from ISE towards the MDM, where ISE takes the client role.

2. Import the MDM digital certificate for ISE

3. Export the MDM site digital certificate. One simple approach is to use one of the Internet browsers to do this. Depending on the browser selected, the importing and exporting procedures are slightly different. Here the Firefox browser is used.

   - From the browser, log on to the MaaS360: *https://logon.maas360.com*

   - In the Browser next to the URL, there is a lock symbol. Click that symbol. Open a security information page as shown below:



Website Identity

Website: m3.maas360.com

Owner: This website does not supply ownership information.

Verified by: DigiCert Inc

Privacy & History

Have I visited this website prior to today? Yes, 102 times

Is this website storing information (cookies) on my computer? Yes

Have I saved any passwords for this website? Yes

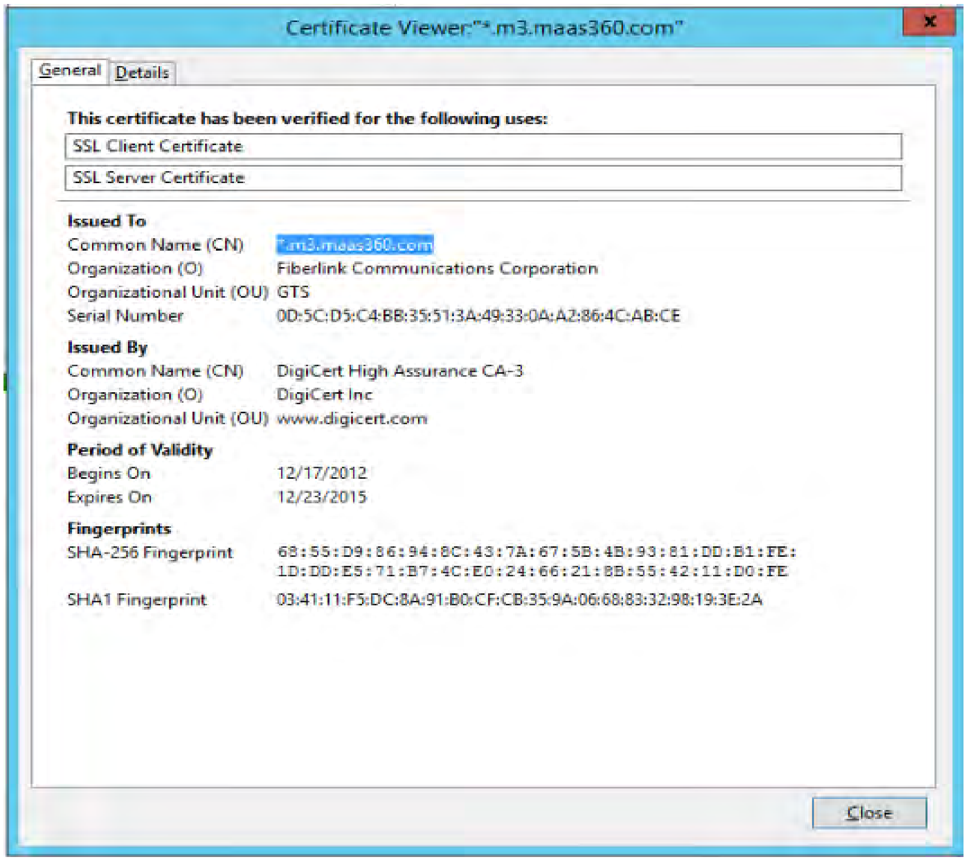
Technical Details

Connection Encrypted (TLS_DHE_RSA_WITH_AES_128_CBC_SHA, 128 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

- Click the View Certificate button to view the certificate



Certificate Viewer:"*.m3.maas360.com"

This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Issued To

Common Name (CN)	*.m3.maas360.com
Organization (O)	Fiberlink Communications Corporation
Organizational Unit (OU)	GTS
Serial Number	0D:5C:D5:C4:BB:35:51:3A:49:33:0A:A2:86:4C:AB:CE

Issued By

Common Name (CN)	DigiCert High Assurance CA-3
Organization (O)	DigiCert Inc
Organizational Unit (OU)	www.digicert.com

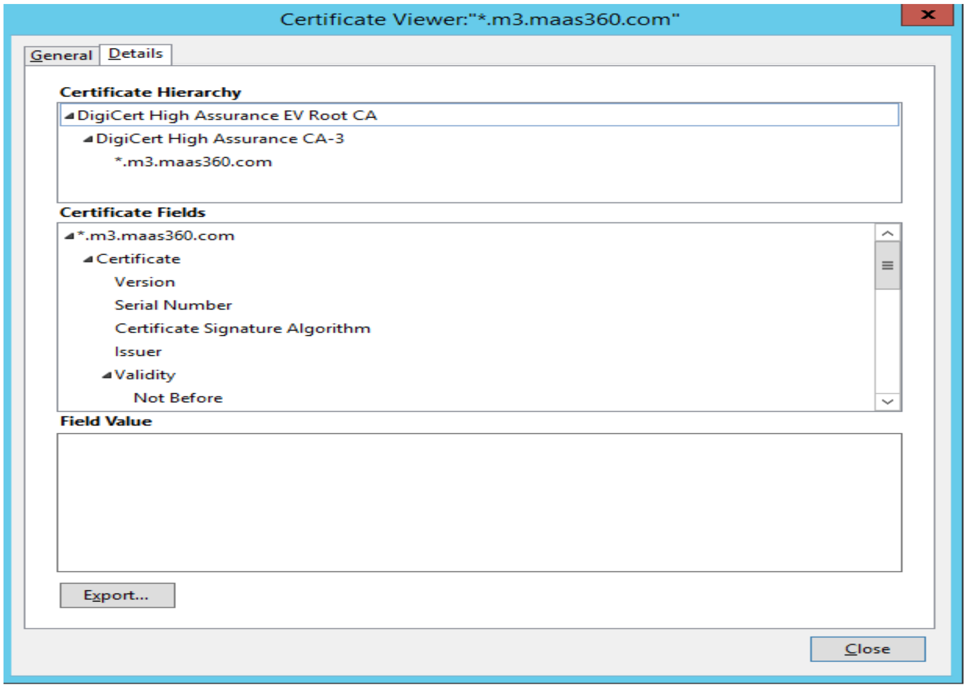
Period of Validity

Begins On	12/17/2012
Expires On	12/23/2015

Fingerprints

SHA-256 Fingerprint	68:55:D9:86:94:8C:43:7A:67:5B:4B:93:81:DD:B1:FE: 1D:DD:E5:71:B7:4C:E0:24:66:21:8B:55:42:11:D0:FE
SHA1 Fingerprint	03:41:11:F5:DC:8A:91:B0:CF:CB:35:9A:06:68:83:32:98:19:3E:2A

- Select the Detail to view the detail certificate information and from there you should have an Export button to export the certificate.



Certificate Viewer:"*.m3.maas360.com"

Certificate Hierarchy

```
◢DigiCert High Assurance EV Root CA
  ◢DigiCert High Assurance CA-3
      *.m3.maas360.com
```

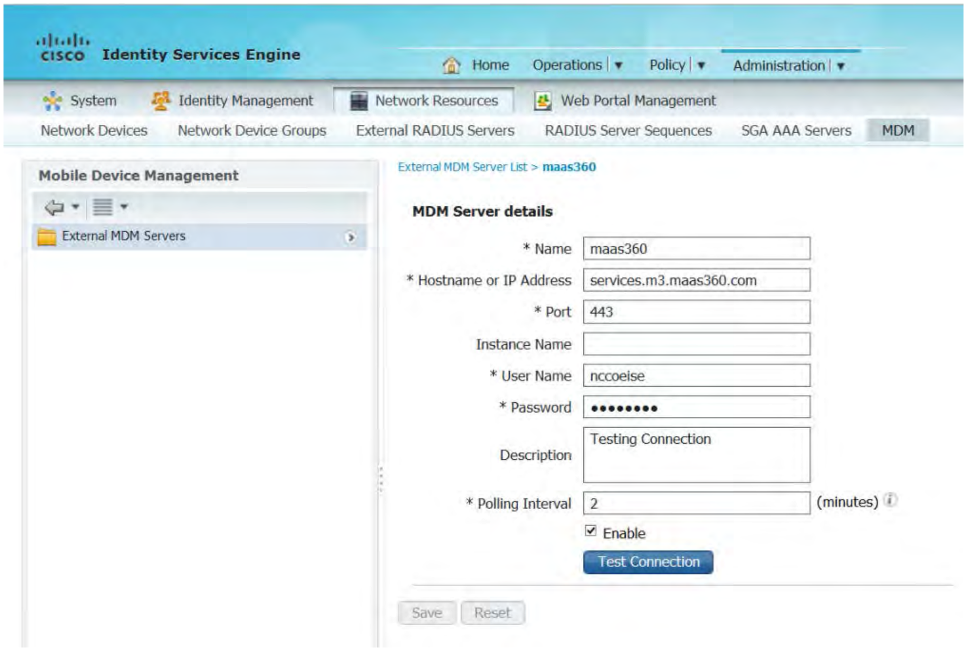
Certificate Fields

```
◢*.m3.maas360.com
  ◢Certificate
      Version
      Serial Number
      Certificate Signature Algorithm
      Issuer
    ◢Validity
        Not Before
```

Field Value

- Save the certificate to a file.

4. Import the certificate into the local cert store in ISE.
   - From the ISE Administration Portal, use the navigation path *Administration* > *System* > *Certificates* > *Certificate Store* to perform the import action.
   - Grant ISE Access to the Fiberlink MaaS360 API
5. Create a Fiberlink MaaS360 administrator account with an API role
   - Log on the MaaS360 with an Administrator Account
   - Navigate to *Setup* > *Administrators* and click Add Administrator.
   - Enter the new user name and a corporate email address and click Next
   - Enter Roles for the newly created administrator and click Next
   - Verify the setting and press Save.
6. Add MDM Server to ISE
   - Use the MaaS360 MDM admin account created above
   - Configure Cisco ISE to integrate with the MaaS360: *Administration* > *MDM* > *External MDM Server*, then click *Add*.
   - Fill out the required information using the account created in Step 5 and the hostname or IP address provided by Fiberlink. A sample result is given below:



MDM Server details

* Name: maas360
* Hostname or IP Address: services.m3.maas360.com
* Port: 443
Instance Name:
* User Name: nccoeise
* Password: ••••••••
Description: Testing Connection
* Polling Interval: 2 (minutes)
☑ Enable

   - The Test Connection button can be used to test the connection between the Cisco ISE and the cloud MaaS360. A successful message will be displayed if connection succeeds.

9.3.7 Configure Cisco ISE to Authorization Policy

Configure ISE Authorization Policies to include an MDM Compliance Check.

1. Configure Cisco ISE to allow network access for registered and compliant mobile devices
   - From the Cisco Administration Portal, navigate to *Policy* > *Authorization*
   - Create the rule as

     Name: *MDM Registered_Compliant*
     Condition: *If MDM:DeviceCompliantStatus Equals Compliant*
     And
     MDM:DeviceRegisterStatus Equals Registered
     Permissions: PermitAccess

2. Configure Cisco ISE to deny network access for unregistered or uncompliant mobile devices
   - From the Cisco Administration Portal, navigate to *Policy* > *Authorization*
   - Create a second rule as

     Name: *MDM UnRegistered_UnCompliant*
     Condition: *If MDM:DeviceCompliantStatus Equals UnCompliant*
     Or
     MDM:DeviceRegisterStatus Equals UnRegistered
     Permissions: *DenyAccess*

3. Configure Cisco ISE to deny network access for all Others
   - From the Cisco Administration Portal, navigate to *Policy* > *Authorization*
   - Create a third rule as

     Name: *Default*
     Condition: *If no matches*
     Permissions: *DenyAccess*

10 Governance, Risk, and Compliance (GRC)

Governance, Risk, and Compliance (GRC) allows an organization to link strategy and risk, adjusting strategy when risk changes, while remaining in compliance with laws and regulations. We used RSA Archer GRC to perform risk assessment and management.

10.1 RSA Archer GRC

10.1.1 System Requirements

This build requires the user to install a single-host RSA Archer GRC Platform node on a VMware virtual machine with the Microsoft Windows Server 2012R2 operating system to provide the risk management services needed.

> All components, features, and configurations presented in this guide reflect what we used based on vendors' best practices and requirements. Please refer to vendors' official documentation for complete instruction for other options.

10.1.2 Pre-installation

We chose the single-host deployment option for installing and configuring the GRC platform on a single VM under the Microsoft Windows Server 2012R2. All components, the Web application, services, and instance databases are running under a single server. Below are the pre-installation tasks that we performed prior the RSA Archer installation:

- Operating System: Windows Server 2012R2 Enterprise
  - Refer to Section 11.1, Windows Installation and Hardening for system requirements and installation.
- Database: Microsoft SQL Server 2012 Enterprise (x64)

Follow Microsoft's installation guidelines and steps to install the SQL Server Database Engine and SQL Server Management tools. Refer *to https://msdn.microsoft.com/en-us/library/bb500395(v=sql.110).aspx* for additional details.

We used the following configuration settings during the installation and configuration process. We also created the required database instances and users for the RSA Archer installation. Test the database instances by using different users to verify the login permissions on all database instances and configuration databases to ensure database owners have sufficient privileges and correct user mappings.

Setting	Value
Collation Settings set to case insensitive for instance database	SQL_Latin1_general_CP1_CI_AS
SQL Compatibility level set appropriately	SQL Server 2012 110
Locale set	English (United States)
Database server time zone	EST
Platform language	English
Create both the instance and configuration databases. For migration, create only the configuration database.	Database names: *grc-content* grc-config
User Account set to Database Owner role	*grc-content-user* grc-config-user
Recovery Model	Simple (configuration and instance databases)
Auto Shrink	False (configuration database)
Auto-Growth	Set it for (instance database)
Max Degree of Parallelism	1 (configuration and instance databases)

Web and Services

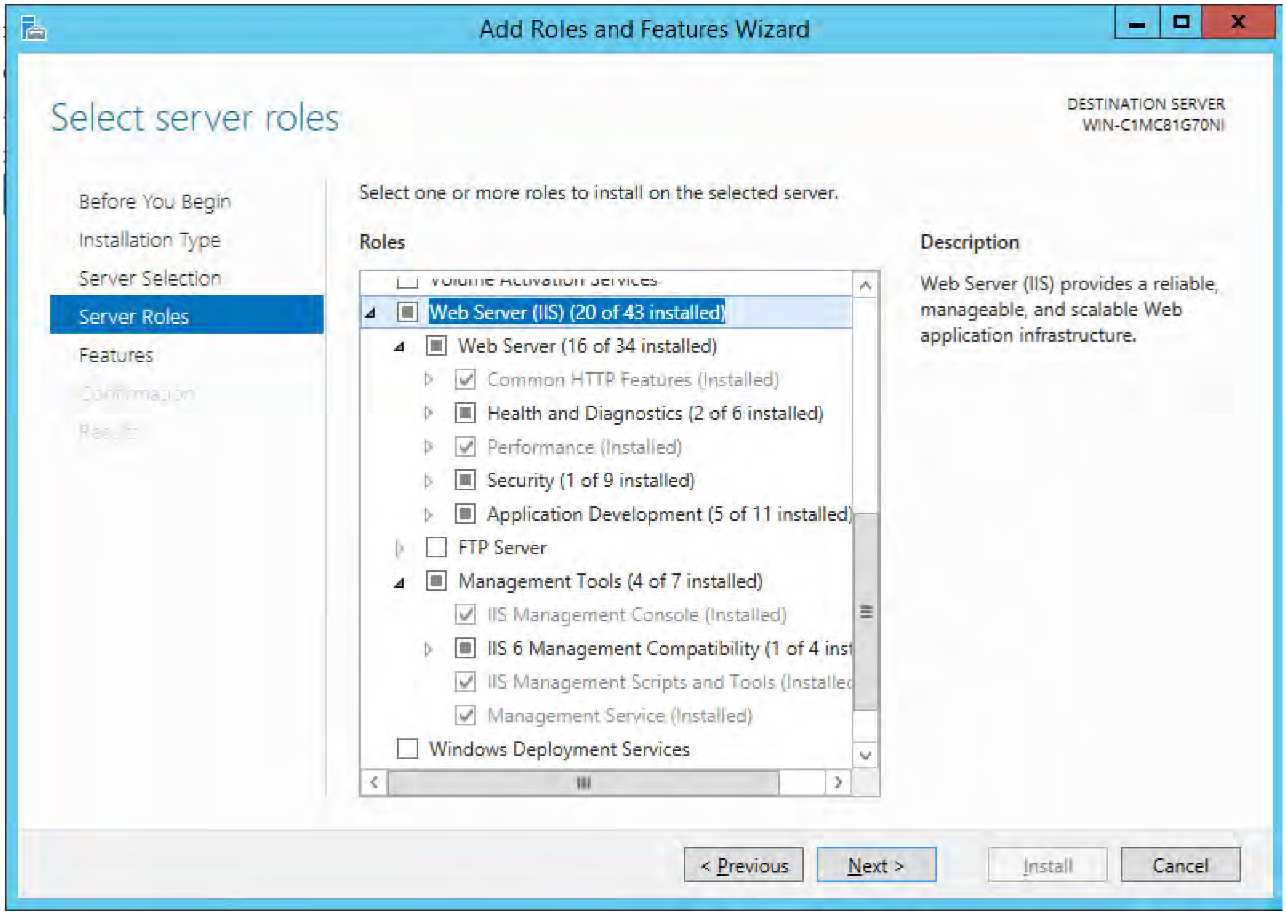
- Microsoft Internet Information Services (IIS) 8
- Microsoft .NET Framework 4.5

Use Server Manager for installing IIS and *.NET* Framework, referring to *http://www.iis.net/learn/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012* for detailed steps and corresponding screenshots.

Please install IIS first and then install the *.NET* Framework.

The table below summarizes the required IIS components and *.NET* Framework features followed by the screenshots.

Required Option	Value
IIS	
Common HTTP Features	Default Document Directory Browsing HTTP Errors Static Content
Health and Diagnostics	HTTP Logging
Application Development	.NET Extensibility 4.5 ASP .NET 4.5 ISAPI Extensions ISAPI Filters
Security	Request Filtering
Management Tools	IIS Management Console
.NET Framework	
.NET Framework 4.5 Features	.NET Framework 4.5 ASP.NET 4.5
WCF Services	HTTP Activation TCP Port Sharing



Select server roles

DESTINATION SERVER
WIN-C1MC81G70NI

Select one or more roles to install on the selected server.

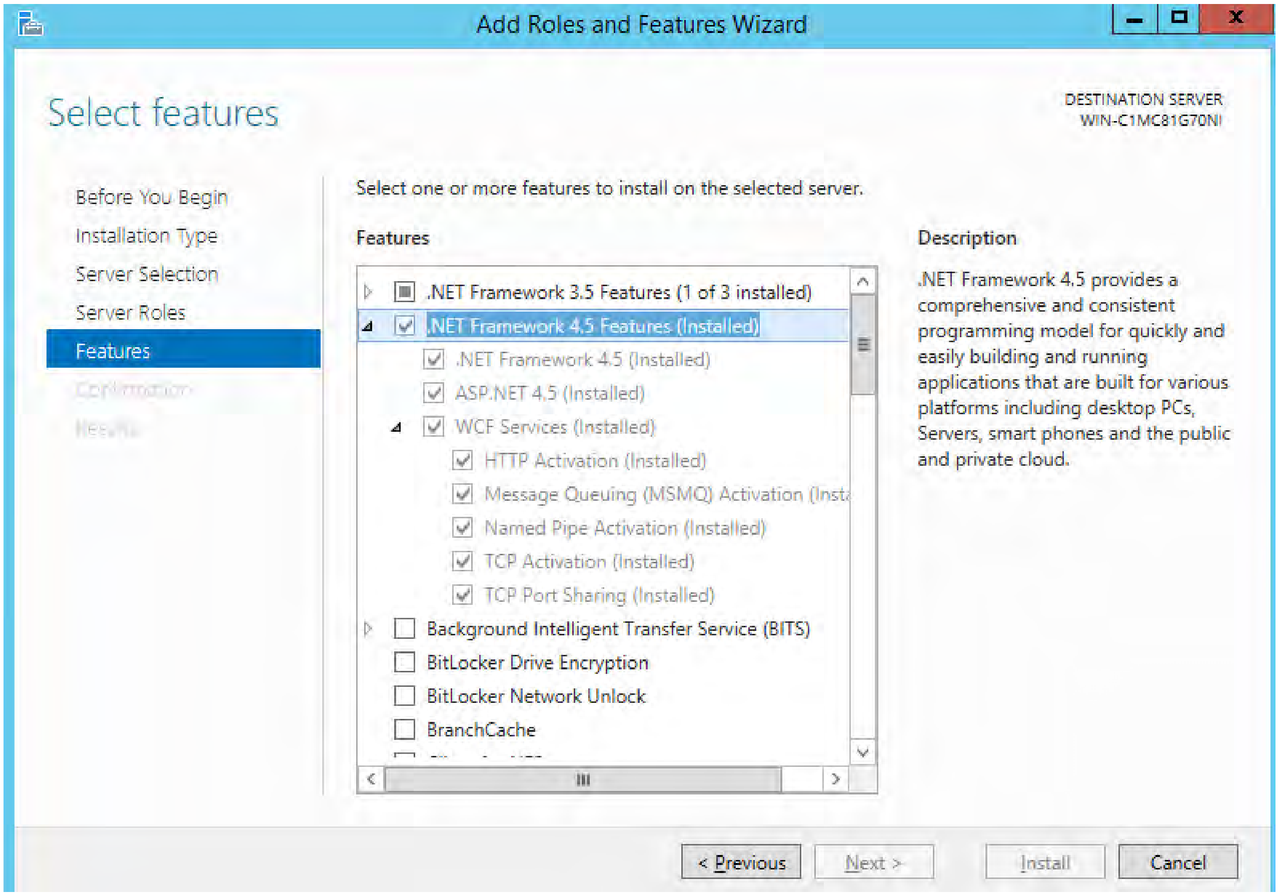
Roles

- □ Volume Activation Services
- ■ Web Server (IIS) (20 of 43 installed)
  - ■ Web Server (16 of 34 installed)
    - ☑ Common HTTP Features (Installed)
    - ■ Health and Diagnostics (2 of 6 installed)
    - ☑ Performance (Installed)
    - ■ Security (1 of 9 installed)
    - ■ Application Development (5 of 11 installed)
  - □ FTP Server
  - ■ Management Tools (4 of 7 installed)
    - ☑ IIS Management Console (Installed)
    - ■ IIS 6 Management Compatibility (1 of 4 inst
    - ☑ IIS Management Scripts and Tools (Installed
    - ☑ Management Service (Installed)
- □ Windows Deployment Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Figure 1: Web Server (IIS) Components Selection Screenshot



Select features

DESTINATION SERVER
WIN-C1MC81G70NI

Select one or more features to install on the selected server.

Features

- ■ .NET Framework 3.5 Features (1 of 3 installed)
- ☑ .NET Framework 4.5 Features (Installed)
  - ☑ .NET Framework 4.5 (Installed)
  - ☑ ASP.NET 4.5 (Installed)
  - ☑ WCF Services (Installed)
    - ☑ HTTP Activation (Installed)
    - ☑ Message Queuing (MSMQ) Activation (Insta
    - ☑ Named Pipe Activation (Installed)
    - ☑ TCP Activation (Installed)
    - ☑ TCP Port Sharing (Installed)
- ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BitLocker Network Unlock
- ☐ BranchCache

Description

.NET Framework 4.5 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud.

Figure 2: .NET Framework 4.5 Features Selection Screenshot

Microsoft Office 2013 Filter Packs

Download it from Microsoft website (*http://www.microsoft.com/en-us/download/details.aspx?id=40229*) and install it.

Java Runtime Environment (JRE) 8

Download and install JRE 8 refer to *http://www.oracle.com/technetwork/java/javase/install-windows-64-142952.html* for details.

> All pre-installation software must be installed and configured before installing RSA Archer.

10.1.3 Installation

1. Create folders *C:\ArcherFiles\Indexes* and *C:\ArcherFiles\Logging*(will be used later).
2. Obtain/Download the installer package from RSA; extract the installation package.
3. Run installer
   - Open installation folder, right-click on *ArcherInstall.exe*

- Select Run as Administrator
- Click OK to Run the Installer
- Follow the prompts from the installer for each step, set the value and click Next
- Select all components (Web Application, Services, Instance Database) for installation; then click Next
- Specify the X.509 Certification by selecting it from the checklist (create new cert or use existing cert)
- Set the Configuration Database options with the following properties:

SQL Server:	local
Login Name:	######
Password:	######
Database:	*grc-config* (this is the configuration database we created during the pre-installation process)

- Set the Configuration Web Application options with the following properties:

Website:	Default Website
Destination Directory:	select "Install in an IIS application" option with "RSAarcher" as the value

- Set the Configuration of the Service Credentials

  Select "Use the Local System Account to Run All" option from the checklist

- Set the Services and Application Files paths with the following properties:

  Services: use the default value "*C:\Program Files\RSA Archer\Services\*"

  Application Files: use the default value "*C:\Program Files\RSA Archer*"

- Set the Log File Path to *C:\ArcherFiles\Logging*
- Perform the installation by clicking Install, wait for the installer to complete installing all components, then click Finish. The RSA Archer Control Panel opens.

10.1.4 Post-Installation

10.1.4.1 Configure the Installation Settings

Verify and set the configurations for the following by clicking on RSA Archer Control Panel > Installation Settings, then select corresponding sections:

1. Logging Section
   - Path: *Archer Files\Logging*
   - Level: Error
2. Locale and Time Zone Section
   - Locale: English (United States)
   - Time Zone: (UTC-05:00) Eastern Time (US & Canada)

On the Toolbar, click Save.

3. Create the Default GRC Platform Instance
   - Start the RSA Archer Queuing Service
   - *Server Manager > Local Services* or *All Services > Locate RSA Archer Queuing* in the list under the *"SERVICES" section > Right-click RSA Archer Queuing* and click Start
   - Add a new instance
   - *RSA Archer Control Panel > Instance Management > Add New Instance*, enter "EHR1" as the Instance Name, then click Go. Complete the properties as needed.
   - Configure the Database Connection Properties
   - *RSA Archer Control Panel > Instance Management > under All Instances*, click on EHR1
   - In the Database tab setup the following:
     - SQL Server: (local)
     - Login name: xxxxxx
     - Password: xxxxxx
     - Database: grc-config
4. Click on the "Test Connection" link to make sure the "Success" message appears.
5. Configure the General Properties
   - *RSA Archer Control Panel > Instance Management > under All Instances, click on EHR1*
   - In the General tab, setup the following:
     - File Repository section – Path *C:\ArcherFiles\Indexes*
     - Search Index section - Content Indexing:Check on Index design language only; Path: *C:\ArcherFiles\Indexes\EHR1*
6. Configure the Web Properties
   - *RSA Archer Control Panel > Instance Management >* under *All Instances*, click on EHR1
   - In the Web tab, setup the following:
     - Base URL: *http://localhost/RSAArcher/*
     - Authentication URL: *default.aspx*
7. Change SysAdmin and Service Account passwords
   - *RSA Archer Control Panel > Instance Management > under All Instances, click on EHR1*
   - Change the password on the page by using a strong password
   - Complete Default GRC Platform Instance Creation by clicking Save on the

toolbar.

8. Register the Instance
   - *RSA Archer Control Panel > Instance Management > under All Instances, right-click on EHR1, select Update Licensing, enter the following info, then click on Active*

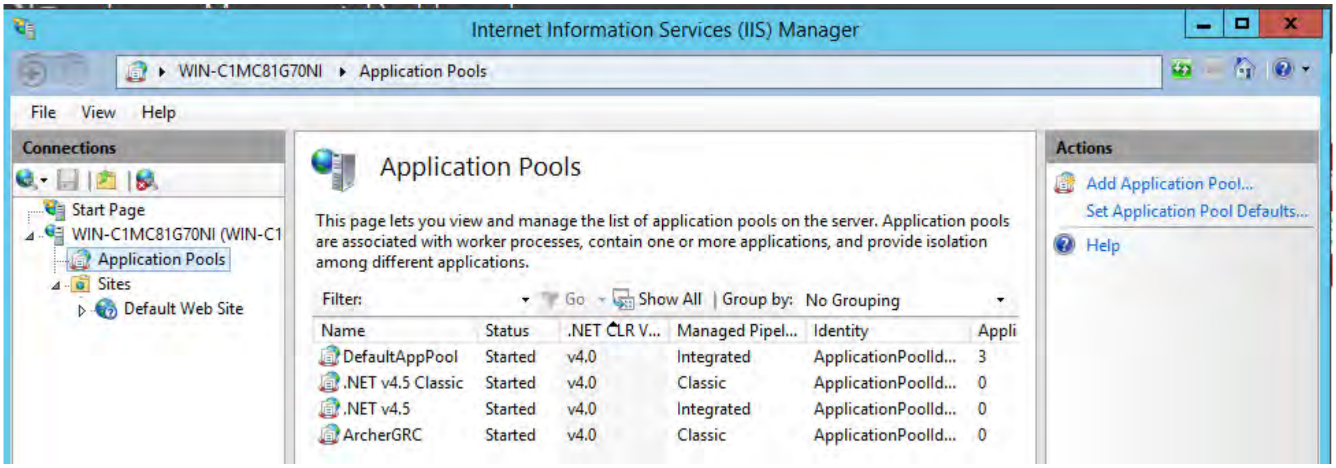
     Serial Number (obtained from RSA)

     Contact Info (First Name, Last Name, Company, etc)

     Activation Method (select Automated)

9. Activate the Archer Instance
   - Start the RSA Archer Services
   - *Server Manager > Local Services or All Services > Locate the following services > Right-click on that service and click Start*
     - RSA Archer Configuration
     - RSA Archer Job Engine
     - RSA Archer LDAP Synchronization
   - Restart the RSA Archer Queuing Service
   - *Server Manager > Local Services or All Services > Locate RSA Archer Queuing > Right-click RSA Archer Queuing and click Restart*
   - Rebuild the Archer Search Index
   - *RSA Archer Control Panel > Instance Management > under All Instances, right-click on EHR1, then click on Rebuild Search Index*

10. Configure and Activate the Web Role (IIS)
    - Setup Application Pools
    - *Server Manager > Tools > IIS Manager > Application Pools (in the left side bar) > right-click to add applications (.NET, ArcherGRC etc.),* example screenshot below



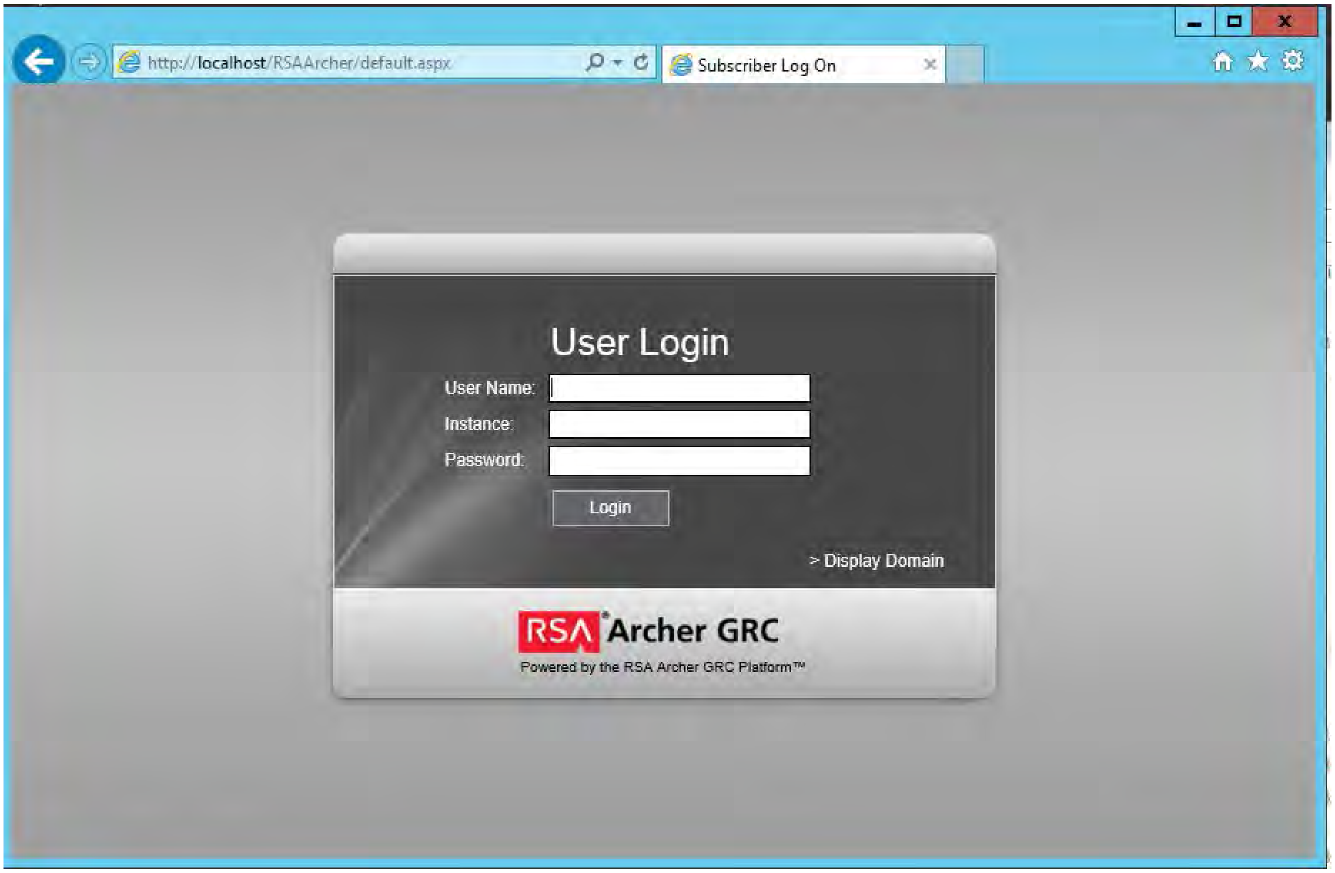
Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

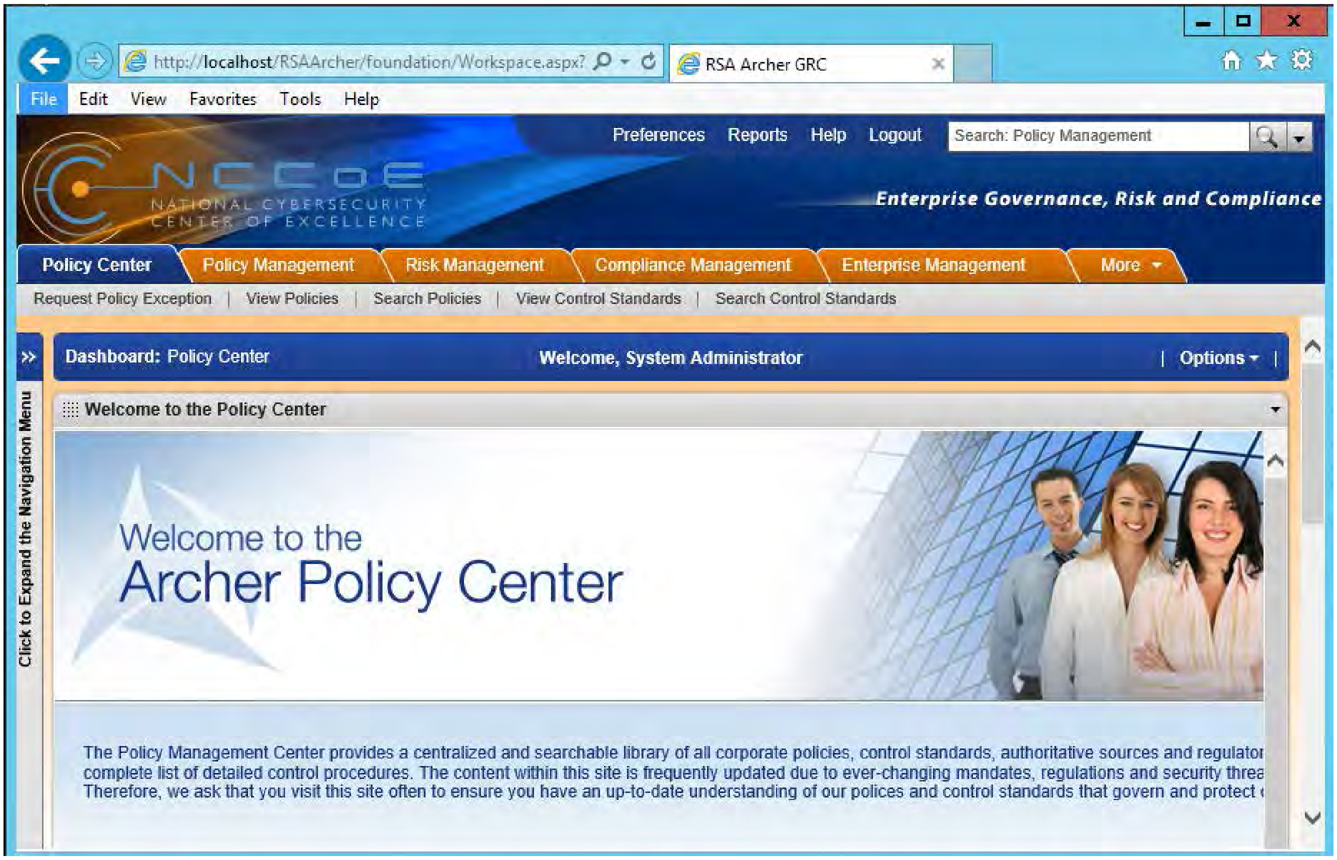
Name	Status	.NET CLR V...	Managed Pipel...	Identity	Appli
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolId...	3
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolId...	0
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolId...	0
ArcherGRC	Started	v4.0	Classic	ApplicationPoolId...	0

   - Restart IIS

11. Test Run for installed RSA Archer GRC and make sure you get the RSA Archer GRC Login screen.



12. Log in to EHR1 Instance.



The Policy Management Center provides a centralized and searchable library of all corporate policies, control standards, authoritative sources and regulator complete list of detailed control procedures. The content within this site is frequently updated due to ever-changing mandates, regulations and security threa Therefore, we ask that you visit this site often to ensure you have an up-to-date understanding of our polices and control standards that govern and protect

13. Now you are ready to set up the contents and establish the GRC processes detailed in the next section.

10.1.5 Content Setup for establishing GRC process

In order to demonstrate how to monitor and clearly communicate the relationship between technical risks and organizational risks, we used a GRC tool to aggregate and visualize data. We configured the RSA Archer GRC tool to ingest data from various sources and provide information about the implementation of security controls used to address the target security characteristics.

Table 1: Content Sources for GRC Tool

Source	Description
NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF)	• Used as the focal point for mapping the use case's security characteristics to Cybersecurity Standards and Best Practices (i.e., NIST SP-800-53r4) and Sector Specific Standards and Best Practices (i.e., HIPAA)
HIPAA Security Rule – Technical Safeguards	• Used as the core authoritative source for defining the objectives, policies, control standards and selecting the relevant control procedures
NIST SP 800-66 rev1	• Utilized the Security Rule Goals and Objectives in section 2.1.1 for defining the Corporate Objectives. • Used Table 4. HIPAA Standards and Implementation Specifications Catalog for defining the control standards and selecting the control procedures from SP 800-53

NIST SP 800-53r4	• Selected controls for HIPAA Security Rule – Technical Safeguards (based on NIST SP 800-66 mapping)
HHS-ONC SRA Tool Technical Safeguards	• Used Questionnaire for doing assessments
Results of Risk Assessment	• Used identified risks and their levels as the input for the risk register, a library of risks that can be utilized by the entire organization

RSA provided the NCCoE with all the core modules. However, this build uses the following modules:

- Enterprise Management
- Policy Management
- Risk Management
- Compliance Management

High Level Structure and Process Steps for NCCoE HIT Mobil Device Use Case GRC Program

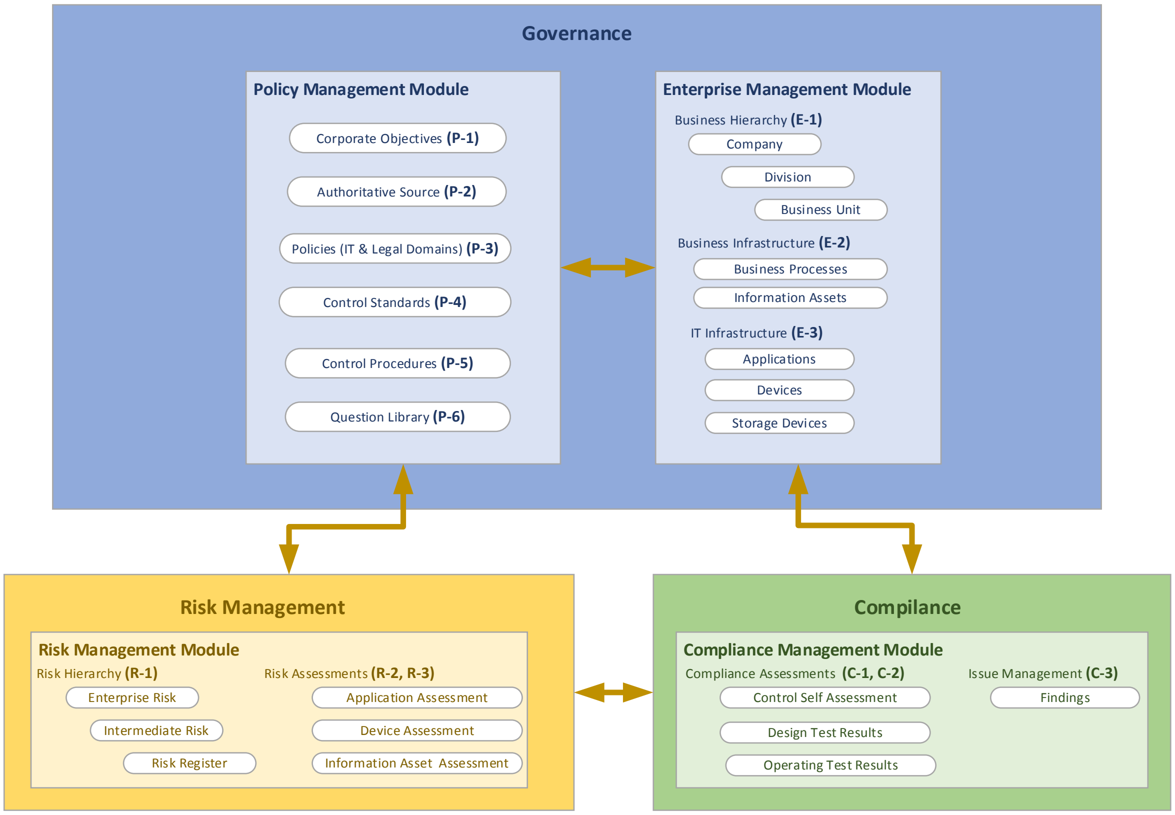


Table 2: High Level Process Steps summarizes the tasks that are conducted for this use case. For most of the tasks, the sequential order is not necessary. The task step is used as the content correlator within this guide. The techniques and relevant content sources are outlined as references. The column of "RM Tool Required?" is an indicator to the organizations, even

without an integrated risk management tool, accomplishes levels of risk management. Also, the manually prepared risk management contents (i.e., using spreadsheets) can be valuable inputs to the risk management tool, if an organization chooses to do so in a later stage.

Table 2: High Level Process Steps

Task Step #	Task	Description & Primary Source	Techniques / Steps in using Archer	RM Tool Required?
P-1	Define Corporate Objectives	Each organization has its own objectives for conducting the business. The objectives can be classified into different categories, such as strategic, operational, reporting and compliance etc. The objectives can be related to the defined policies and risks. Through those associations, Archer supports an organization to track policies and monitoring related risks and key performance indicators. For the demonstration purpose, this use case select a single objective from SP 800-66. **Primary Source:** NIST SP 800-66	**Archer Module:** Policy Management **Archer App:** Corporate Objectives **Actions:** use the Archer UI to create/update the corporate objectives and associate the objective to necessary existing policies, organizations, risks.	No
P-2	Select/Define Authoritative Source	In order to scope down the set of relevant controls, NCCoE takes the advantage of Archer's content library for the HIPAA Security as the authoritative source, but remap them to the set of control standards that are specifically created for HIPAA Security (P-4 & P-5). **Primary Source:** HIPAA/Archer content library, NCCoE	**Archer Module:** Policy Management **Archer App:** Authoritative Sources **Actions:** Created new report for Authoritative Sources for the target subset of the authoritative source. **To create new report:** Policy Management (tab) > Authoritative Source (side menu) > Reports > New > > Select reporting fields > Enter filters (for HIPAA security technical safeguards) > Enter sort option > Enter display option > Save report **To access to the new report:** Policy Management (tab) > Authoritative Source (side menu) > Records (side menu) > Reports (icon) > HIPAA Security Technical Safeguard Compliance (Select Report popup)	Yes
P-3	Select/Define related Policies			
P-4	Create relevant Control Standards	The NIST SP 800-66 is used as the guidance for NCCoE to create a set of Control Standards that are directly mapped to the HIPAA Security, Technical Safeguard (see Figure: Control Standards). Relevant SP 800-53r4 controls are also being created and mapped to the HIPAA related control standards (see Figure: Control Procedures – NCCoE) **Primary Source:** HIPAA Security, Technical Safeguards, NIST SP 800-	**Archer Module:** Policy Management **Archer App:** Control Standards **Actions:** use the Archer UI to create/update the control standards that corresponding to relevant source. **To create new control standard:** Policy Management (tab) > Control Standards (side menu) > New Record > enter data > Save **Archer App:** Control Procedures **Actions:** use the Archer UI to import pre-defined data from spreadsheet. **To import control procedures:**	No
P-5	Select SP800-53 control procedures			

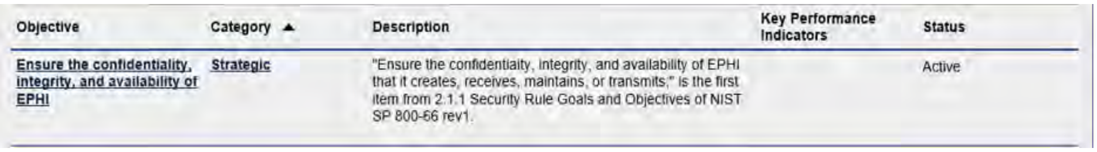
Task Step #	Task	Description & Primary Source	Techniques / Steps in using Archer	RM Tool Required?
		66, and NIST SP 800-53-r4	Policy Management (tab) > Control Procedures (side menu) > Data Import > Follow the Data Import Wizard to Select data file, select format option, perform data mapping, and import data.	
P-6	Create questionnaires by importing questions	The Security Risk Assessment Tool from the Office of the National Coordinator for Health Information Technology (ONC) is adopted for populating the questionnaires. **Primary Source:** HHS/ONC SRA tool	**Archer Module:** Policy Management **Archer App:** Question Library **Actions:** use the Archer UI to import pre-defined data from spreadsheet. **To import questionnaires:** Policy Management (tab) > Question Library (side menu) > Data Import > Follow the Data Import Wizard to Select data file, select format option, perform data mapping, and import data.	No
E-1	Define/Import Business Hierarchy	Pseudo organizations are used for presenting the organizations that defined in lab environment. **Primary Source:** NCCoE HIT EHR Mobile Device Use Case	**Archer Module:** Enterprise Management **Archer App:** Business Hierarchy **Actions:** use the Archer UI to create/update the business hierarchy and associate them to necessary existing policies, objectives, risks, and etc. **To create new company/division/business unit:** Enterprise Management (tab) > Business Hierarchy (side menu) > Company/Division/Business Unit > New Record.	No
E-2	Define/Import Business Infrastructure	With the pseudo organization and lab environment setting, this use case only defines Business Process and Information Assets in this group. **Primary Source:** NCCoE HIT EHR Mobile Device Use Case	**Archer Module:** Enterprise Management **Archer App:** Business Infrastructure **Actions:** use the Archer UI to create/update the Business Processes and Information Assets and associate them to necessary existing policies, organizations, objectives, risks, and etc. **To create new business processes/information assets:** Enterprise Management (tab) > Business Infrastructure (side menu) > Business Processes/Information Assets > New Record.	No
E-3	Define/Import IT Infrastructure	With the pseudo organization and lab environment setting, this use case defines Applications and Devices in this group. **Primary Source:** NCCoE HIT EHR Mobile Device Use Case (inventory list, device scanning list, etc.)	**Archer Module:** Enterprise Management **Archer App:** IT Infrastructure **Actions:** use the Archer UI to import pre-defined data from spreadsheets and then use Archer UI to associate them to necessary existing policies, organizations, objectives, risks, and etc. **To import applications/devices:** Enterprise Management (tab) > IT Infrastructure (side menu) > Applications/Devices > Data Import > Follow the Data Import Wizard to Select data file,	No

Task Step #	Task	Description & Primary Source	Techniques / Steps in using Archer	RM Tool Required?
			select format option, perform data mapping, and import data.	
R-1	Identify and rating risks and define risk hierarchy	Three-level Risk Hierarchy enables organization to roll-up their risk register from detailed risk records to an Intermediate summary level, and to an Enterprise level. Based on the NIST SP 800-30 (see diagram below), a study was conducted for identifying the risks in the NCCoE HIT Mobile Device use case environment based on the identified Threat Sources and Events, vulnerabilities, likelihood and impact. Refer to RAM section for details on the risk identification procedures. **Primary Source:** Identified Risks from the risk assessment exercise	**Archer Module:** Risk Management **Archer App:** Risk Hierarchy/Risk Register **Actions:** use the Archer UI to create risk hierarchy and risk register with all the risk assessment results. Then associate them to necessary existing policies, organizations, objectives, risks, devices, applications, and etc. **To create new risk hierarchy/risk register:** Risk Management (tab) > Risk Hierarchy/Risk Register (side menu) > New Record.	No
R-2	Design and conduct risk assessment for Applications, Devices and Info Asset	Modify the existing Archer assessment app for Application, Device and Information Asset by incorporating corresponding questionnaires form HHS/ONC SRA tool. Then conduct the assessments for required applications, devices, and information assets. The assessment results are aggregated and used throughout all associated objects (i.e., other asset type, business unit, business process, and objectives etc.) Business impacts can also be captured during the assessment process. **Primary Source:** HHS/ONC SRA tool and Archer Content Library	**Archer Module:** Risk Management **Archer App:** Risk Assessments **Actions:** use the Archer UI to modify existing assessment app; use the Archer UI to conduct assessments **To modify existing assessment apps:** Risk Management (tab) > Administration (side menu) > Manage Questionnaires (pop-up menu) > Application Assessment/Device Assessment/Information Asset Assessment (list on screen) > click Edit icon under Action > Field (tab) import ONC questionnaires > Layout (tab) to add additional sections with corresponding questions > Save. **To conduct risk assessment:** Risk Management (tab) > Risk Assessments (side menu) > Application Assessment/Device Assessment/Information Asset Assessment (side submenu) > select record > conduct assessment > Save.	Yes
R-3	Risk Assessment result/impact analysis and decision making	Various reports and charts can be accessed for viewing the assessment results and conducting the impact analysis at different levels and different modules. **Primary Source:** NCCoE	**Archer Module:** all used modules **Archer App:** any app that has risk management tab to be associated or reports that on the dashboard. **Actions:** various – see sample screenshots	Yes
C-1	Compliance Assessment	Various assessments can be used for checking the compliance to HIPAA, control standards, and control procedures **Primary Source:** HIPAA, HHS/ONC	**Archer Module:** Compliance Management **Archer App:** Compliance Assessments **Actions:** use the Archer UI to conduct assessments **To conduct compliance assessment:**	Yes

Task Step #	Task	Description & Primary Source	Techniques / Steps in using Archer	RM Tool Required?
		SRA tool, Archer content library	Compliance Management (tab) > Compliance Assessments (side menu) > Select type of assessment (side submenu) > select record > conduct assessment > Save.	
C-2	Compliance Assessment result/impact analysis and decision making	Create customized and use existing reports and charts to view assessment results and conducting the impact analysis at different levels and different modules. **Primary Source:** NCCoE	**Archer Module:** all used modules **Archer App:** any app that has compliance management tab to be associated or reports that on the dashboard. **Actions:** various – see sample screenshots	Yes
C-3	Issue Management	Issue Management module is embed in other modules, such as Risk Management, Compliance Management, and others. All related activities, such as assessments, imported scanning results and other tests produce “Findings”, which can be managed as issues. **Primary Source:** NCCoE	**Archer Module:** Issue Management **Archer App:** Findings. **Actions:** various – see sample screenshots **To access “Finding reports”:** Risk/Compliance Management (tab) > Issue Management (side menu) > Findings (side submenu) > Report icon > select report from drop-down list > view report (drill down to for other actions).	Yes
Final	Integrate with external data sources and customize reports and dashboards	Utilizing the Data Feed feature to setup the		Yes

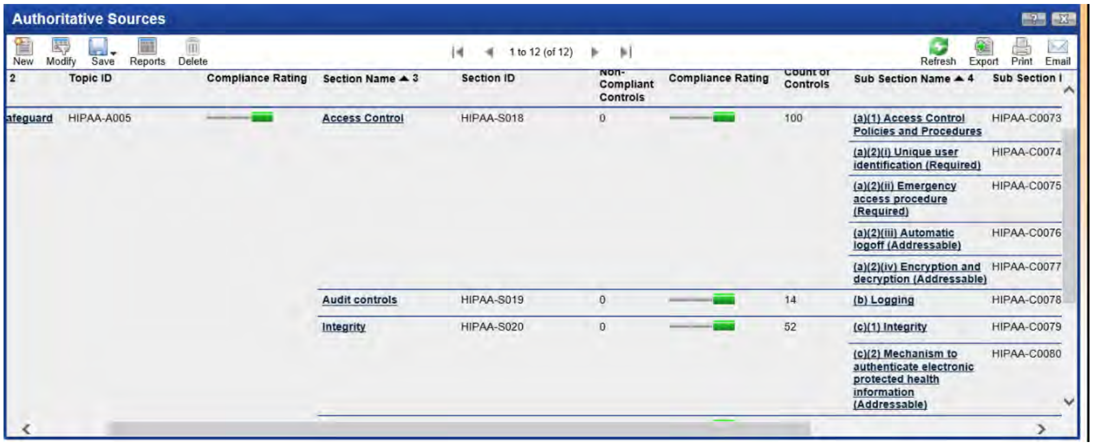
Below are sample screenshots for the steps defined in the table above:

P-1) Define Corporate Objectives



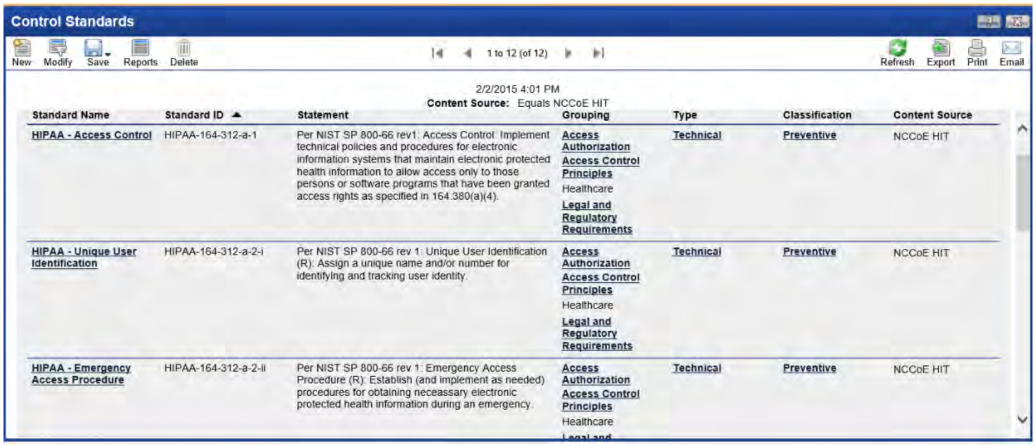
Objective	Category ▲	Description	Key Performance Indicators	Status
Ensure the confidentiality, integrity, and availability of EPHI	Strategic	"Ensure the confidentiaity, integrity, and availability of EPHI that it creates, receives, maintains, or transmits;" is the first item from 2.1.1 Security Rule Goals and Objectives of NIST SP 800-66 rev1.		Active

P-2) & P-3) Select/Define Authoritative Source (HIPAA Security) and related Policies



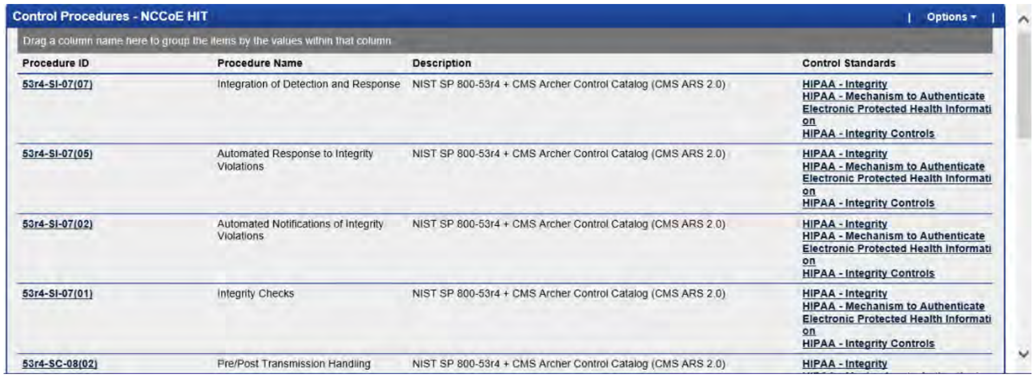
2	Topic ID	Compliance Rating	Section Name ▲ 3	Section ID	Non-Compliant Controls	Compliance Rating	Count of Controls	Sub Section Name ▲ 4	Sub Section I
afeguard	HIPAA-A005	🟩	Access Control	HIPAA-S018	0	🟩	100	(a)(1) Access Control Policies and Procedures	HIPAA-C0073
								(a)(2)(i) Unique user identification (Required)	HIPAA-C0074
								(a)(2)(ii) Emergency access procedure (Required)	HIPAA-C0075
								(a)(2)(iii) Automatic logoff (Addressable)	HIPAA-C0076
								(a)(2)(iv) Encryption and decryption (Addressable)	HIPAA-C0077
			Audit controls	HIPAA-S019	0	🟩	14	(b) Logging	HIPAA-C0078
			Integrity	HIPAA-S020	0	🟩	52	(c)(1) Integrity	HIPAA-C0079
								(c)(2) Mechanism to authenticate electronic protected health information (Addressable)	HIPAA-C0080

P-4) & P-5) Create relevant Control Standards and Select SP800-53 control procedures (focus on HIPAA Security, Technical Safeguards)



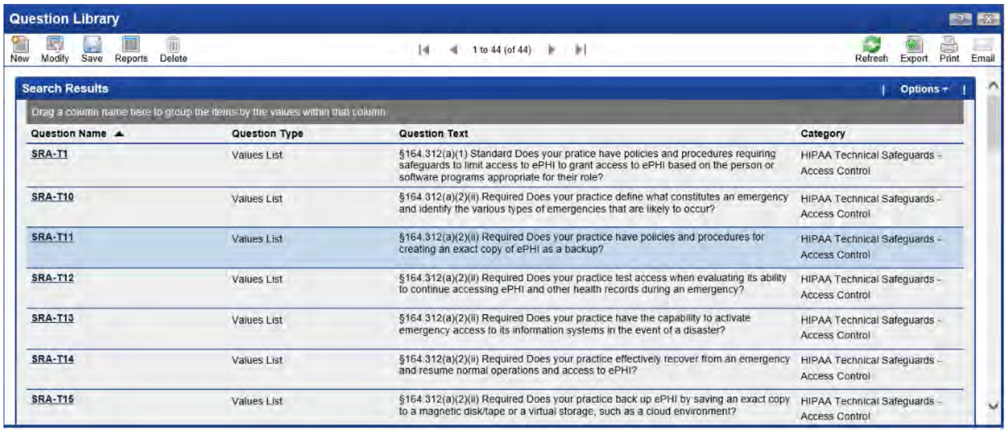
2/2/2015 4:01 PM
Content Source: Equals NCCoE HIT

Standard Name	Standard ID ▲	Statement	Grouping	Type	Classification	Content Source
HIPAA - Access Control	HIPAA-164-312-a-1	Per NIST SP 800-66 rev1: Access Control: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.380(a)(4).	Access Authorization Access Control Principles Healthcare Legal and Regulatory Requirements	Technical	Preventive	NCCoE HIT
HIPAA - Unique User Identification	HIPAA-164-312-a-2-i	Per NIST SP 800-66 rev 1: Unique User Identification (R): Assign a unique name and/or number for identifying and tracking user identity.	Access Authorization Access Control Principles Healthcare Legal and Regulatory Requirements	Technical	Preventive	NCCoE HIT
HIPAA - Emergency Access Procedure	HIPAA-164-312-a-2-ii	Per NIST SP 800-66 rev 1: Emergency Access Procedure (R): Establish (and implement as needed) procedures for obtaining neceassary electronic protected health information during an emergency.	Access Authorization Access Control Principles Healthcare Legal and	Technical	Preventive	NCCoE HIT


Control Procedures - NCCoE HIT
Options
Drag a column name here to group the items by the values within that column.

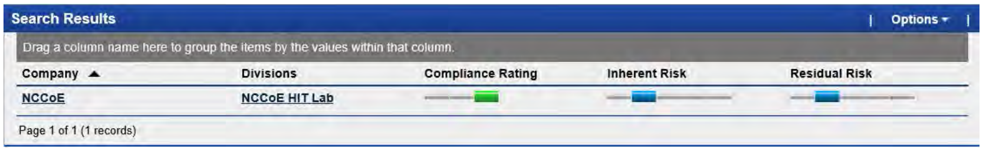
Procedure ID	Procedure Name	Description	Control Standards
53r4-SI-07(07)	Integration of Detection and Response	NIST SP 800-53r4 + CMS Archer Control Catalog (CMS ARS 2.0)	HIPAA - Integrity HIPAA - Mechanism to Authenticate Electronic Protected Health Informati on HIPAA - Integrity Controls
53r4-SI-07(05)	Automated Response to Integrity Violations	NIST SP 800-53r4 + CMS Archer Control Catalog (CMS ARS 2.0)	HIPAA - Integrity HIPAA - Mechanism to Authenticate Electronic Protected Health Informati on HIPAA - Integrity Controls
53r4-SI-07(02)	Automated Notifications of Integrity Violations	NIST SP 800-53r4 + CMS Archer Control Catalog (CMS ARS 2.0)	HIPAA - Integrity HIPAA - Mechanism to Authenticate Electronic Protected Health Informati on HIPAA - Integrity Controls
53r4-SI-07(01)	Integrity Checks	NIST SP 800-53r4 + CMS Archer Control Catalog (CMS ARS 2.0)	HIPAA - Integrity HIPAA - Mechanism to Authenticate Electronic Protected Health Informati on HIPAA - Integrity Controls
53r4-SC-08(02)	Pre/Post Transmission Handling	NIST SP 800-53r4 + CMS Archer Control Catalog (CMS ARS 2.0)	HIPAA - Integrity

P-6) Create questionnaires by importing questions from HHS/ONC SRA tool



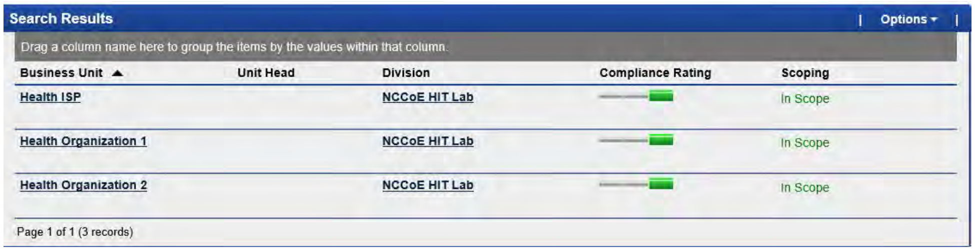
Question Name ▲	Question Type	Question Text	Category
SRA-T1	Values List	§164.312(a)(1) Standard Does your pratice have policies and procedures requiring safeguards to limit access to ePHI to grant access to ePHI based on the person or software programs appropriate for their role?	HIPAA Technical Safeguards - Access Control
SRA-T10	Values List	§164.312(a)(2)(ii) Required Does your practice define what constitutes an emergency and identify the various types of emergencies that are likely to occur?	HIPAA Technical Safeguards - Access Control
SRA-T11	Values List	§164.312(a)(2)(ii) Required Does your practice have policies and procedures for creating an exact copy of ePHI as a backup?	HIPAA Technical Safeguards - Access Control
SRA-T12	Values List	§164.312(a)(2)(ii) Required Does your practice test access when evaluating its ability to continue accessing ePHI and other health records during an emergency?	HIPAA Technical Safeguards - Access Control
SRA-T13	Values List	§164.312(a)(2)(ii) Required Does your practice have the capability to activate emergency access to its information systems in the event of a disaster?	HIPAA Technical Safeguards - Access Control
SRA-T14	Values List	§164.312(a)(2)(ii) Required Does your practice effectively recover from an emergency and resume normal operations and access to ePHI?	HIPAA Technical Safeguards - Access Control
SRA-T15	Values List	§164.312(a)(2)(ii) Required Does your practice back up ePHI by saving an exact copy to a magnetic disk/tape or a virtual storage, such as a cloud environment?	HIPAA Technical Safeguards - Access Control

E-1) Define/Import Business Hierarchy


Search Results
Options
Drag a column name here to group the items by the values within that column.

Company ▲	Divisions	Compliance Rating	Inherent Risk	Residual Risk
NCCoE	NCCoE HIT Lab	🟩	🟦	🟦

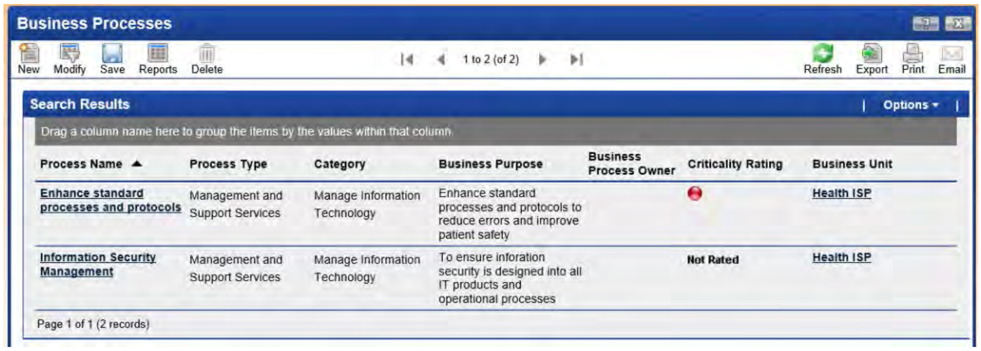
Page 1 of 1 (1 records)


Search Results
Options
Drag a column name here to group the items by the values within that column.

Business Unit ▲	Unit Head	Division	Compliance Rating	Scoping
Health ISP		NCCoE HIT Lab	🟩	In Scope
Health Organization 1		NCCoE HIT Lab	🟩	In Scope
Health Organization 2		NCCoE HIT Lab	🟩	In Scope

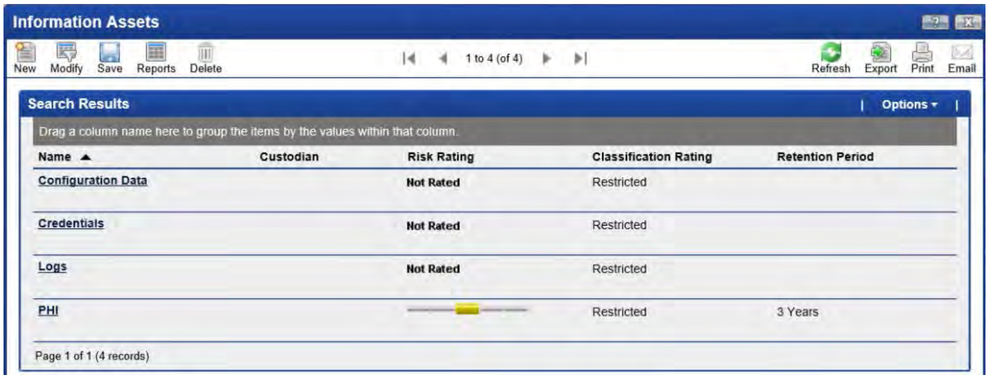
Page 1 of 1 (3 records)

E-2) Define/Import Business Infrastructure



Process Name ▲	Process Type	Category	Business Purpose	Business Process Owner	Criticality Rating	Business Unit
Enhance standard processes and protocols	Management and Support Services	Manage Information Technology	Enhance standard processes and protocols to reduce errors and improve patient safety		🔴	Health ISP
Information Security Management	Management and Support Services	Manage Information Technology	To ensure inforation security is designed into all IT products and operational processes		Not Rated	Health ISP

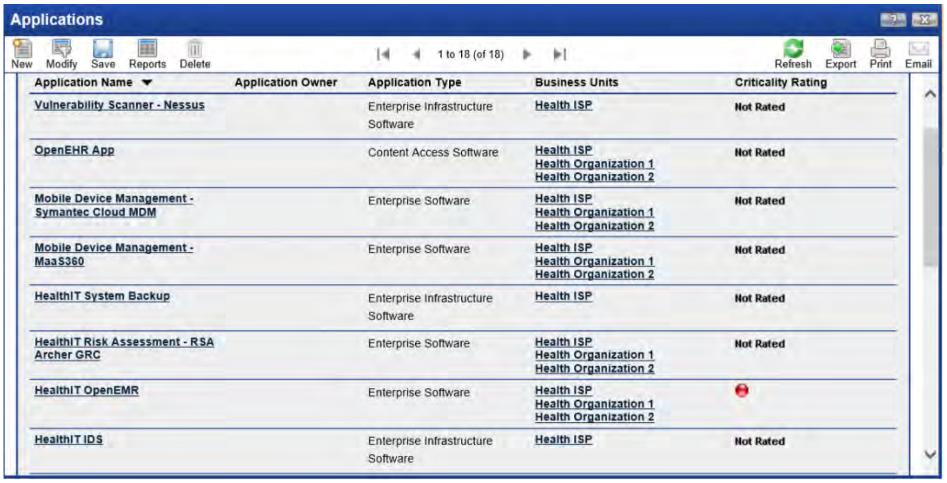
Page 1 of 1 (2 records)



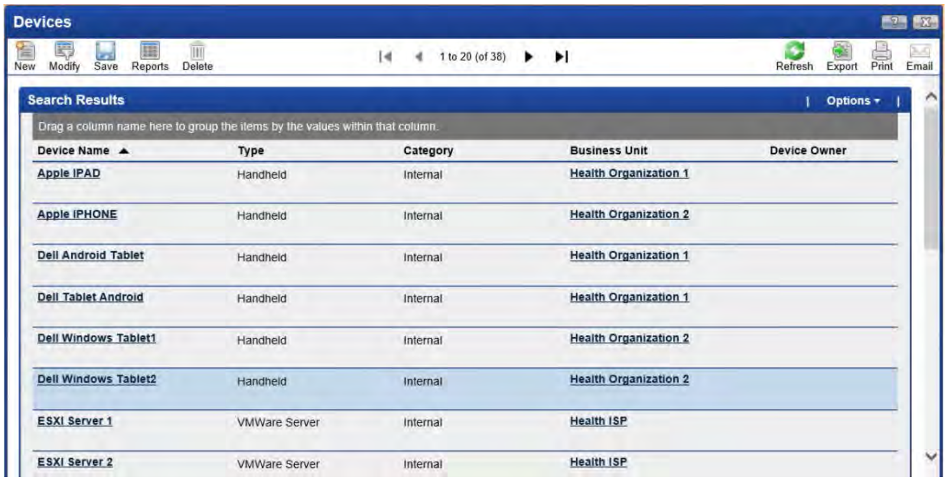
Name ▲	Custodian	Risk Rating	Classification Rating	Retention Period
Configuration Data		Not Rated	Restricted	
Credentials		Not Rated	Restricted	
Logs		Not Rated	Restricted	
PHI		🟨	Restricted	3 Years

Page 1 of 1 (4 records)

E-3) Define/Import IT Infrastructure

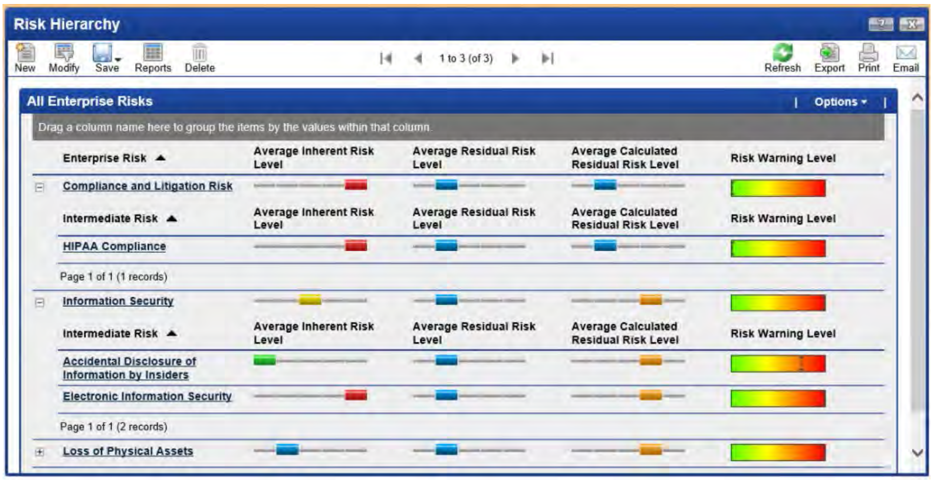


Application Name ▼	Application Owner	Application Type	Business Units	Criticality Rating
Vulnerability Scanner - Nessus		Enterprise Infrastructure Software	Health ISP	Not Rated
OpenEHR App		Content Access Software	Health ISP Health Organization 1 Health Organization 2	Not Rated
Mobile Device Management - Symantec Cloud MDM		Enterprise Software	Health ISP Health Organization 1 Health Organization 2	Not Rated
Mobile Device Management - MaaS360		Enterprise Software	Health ISP Health Organization 1 Health Organization 2	Not Rated
HealthIT System Backup		Enterprise Infrastructure Software	Health ISP	Not Rated
HealthIT Risk Assessment - RSA Archer GRC		Enterprise Software	Health ISP Health Organization 1 Health Organization 2	Not Rated
HealthIT OpenEMR		Enterprise Software	Health ISP Health Organization 1 Health Organization 2	●
HealthIT IDS		Enterprise Infrastructure Software	Health ISP	Not Rated



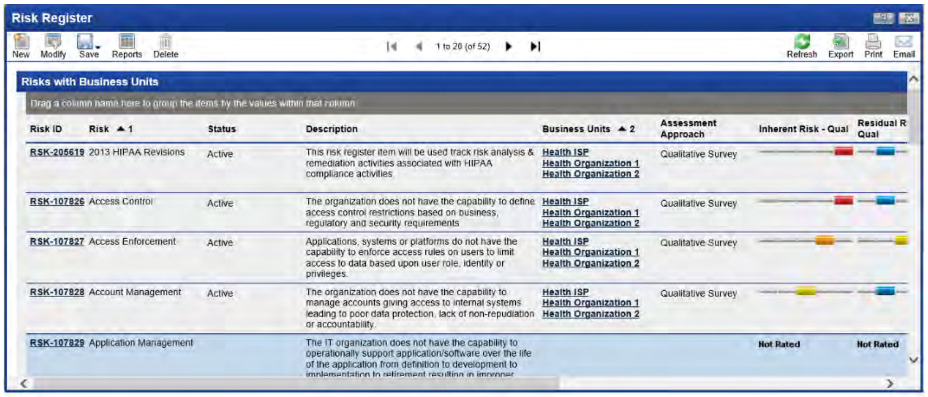
Device Name ▲	Type	Category	Business Unit	Device Owner
Apple IPAD	Handheld	Internal	Health Organization 1	
Apple IPHONE	Handheld	Internal	Health Organization 2	
Dell Android Tablet	Handheld	Internal	Health Organization 1	
Dell Tablet Android	Handheld	Internal	Health Organization 1	
Dell Windows Tablet1	Handheld	Internal	Health Organization 2	
Dell Windows Tablet2	Handheld	Internal	Health Organization 2	
ESXI Server 1	VMWare Server	Internal	Health ISP	
ESXI Server 2	VMWare Server	Internal	Health ISP	

R-1) Identify and rating risks and define risk hierarchy



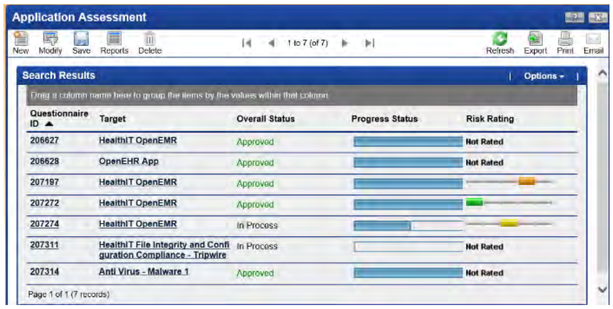
Enterprise Risk ▲	Average Inherent Risk Level	Average Residual Risk Level	Average Calculated Residual Risk Level	Risk Warning Level
⊟ Compliance and Litigation Risk	🟥	🟦	🟦	
Intermediate Risk ▲	Average Inherent Risk Level	Average Residual Risk Level	Average Calculated Residual Risk Level	Risk Warning Level
HIPAA Compliance	🟥	🟦	🟦	
Page 1 of 1 (1 records)				
⊟ Information Security	🟨	🟦	🟧	
Intermediate Risk ▲	Average Inherent Risk Level	Average Residual Risk Level	Average Calculated Residual Risk Level	Risk Warning Level
Accidental Disclosure of Information by Insiders	🟩	🟦	🟧	
Electronic Information Security	🟥	🟦	🟧	
Page 1 of 1 (2 records)				
⊞ Loss of Physical Assets	🟦	🟦	🟧	

Risk Register


Risk Register
New
Modify
Save
Reports
Delete
1 to 20 (of 52)
Refresh
Export
Print
Email
Risks with Business Units
Drag a column name here to group the items by the values within that column

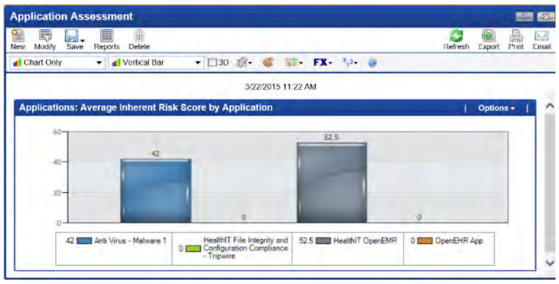
Risk ID	Risk ▲ 1	Status	Description	Business Units ▲ 2	Assessment Approach	Inherent Risk - Qual	Residual R Qual
RSK-205619	2013 HIPAA Revisions	Active	This risk register item will be used track risk analysis & remediation activities associated with HIPAA compliance activities	Health ISP Health Organization 1 Health Organization 2	Qualitative Survey	🟥	🟦
RSK-107826	Access Control	Active	The organization does not have the capability to define access control restrictions based on business, regulatory and security requirements	Health ISP Health Organization 1 Health Organization 2	Qualitative Survey	🟥	🟦
RSK-107827	Access Enforcement	Active	Applications, systems or platforms do not have the capability to enforce access rules on users to limit access to data based upon user role, identity or privileges.	Health ISP Health Organization 1 Health Organization 2	Qualitative Survey	🟧	🟨
RSK-107828	Account Management	Active	The organization does not have the capability to manage accounts giving access to internal systems leading to poor data protection, lack of non-repudiation or accountability.	Health ISP Health Organization 1 Health Organization 2	Qualitative Survey	🟨	🟦
RSK-107829	Application Management		The IT organization does not have the capability to operationally support application/software over the life of the application from definition to development to implementation to retirement resulting in improper			Not Rated	Not Rated

R-2) & R-3) Perform risk assessment, result/impact analysis and decision making for Applications, Devices and Info Asset



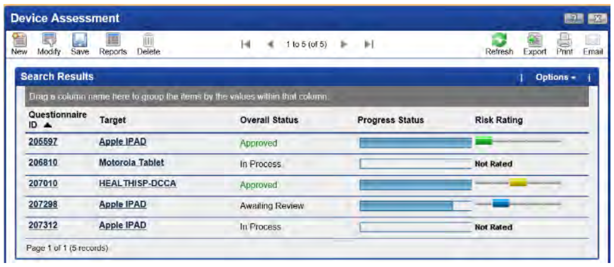
Questionnaire ID ▲	Target	Overall Status	Progress Status	Risk Rating
206627	HealthIT OpenEMR	Approved		Not Rated
206628	OpenEHR App	Approved		Not Rated
207197	HealthIT OpenEMR	Approved		🟧
207272	HealthIT OpenEMR	Approved		🟩
207274	HealthIT OpenEMR	In Process		🟨
207311	HealthIT File Integrity and Confi guration Compliance - Tripwire	In Process		Not Rated
207314	Anti Virus - Malware 1	Approved		Not Rated

Page 1 of 1 (7 records)



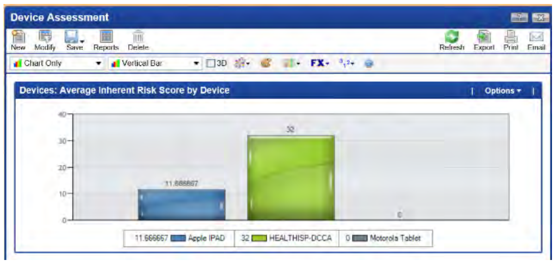
3/22/2015 11:22 AM

Applications: Average Inherent Risk Score by Application

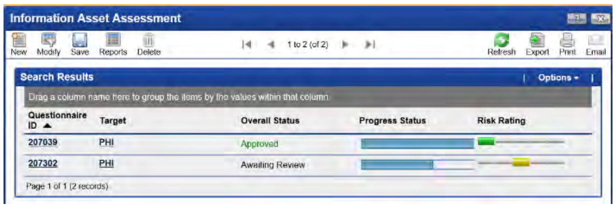


Questionnaire ID ▲	Target	Overall Status	Progress Status	Risk Rating
205597	Apple IPAD	Approved		🟩
206810	Motorola Tablet	In Process		Not Rated
207010	HEALTHISP-DCCA	Approved		🟨
207298	Apple IPAD	Awaiting Review		🟦
207312	Apple IPAD	In Process		Not Rated

Page 1 of 1 (5 records)

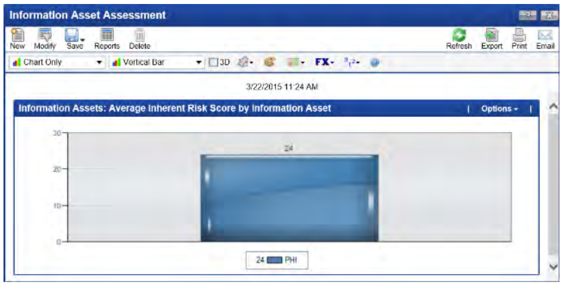


Devices: Average Inherent Risk Score by Device


Information Asset Assessment
New
Modify
Save
Reports
Delete
1 to 2 (of 2)
Refresh
Export
Print
Email
Search Results
Options
Drag a column name here to group the items by the values within that column.

Questionnaire ID ▲	Target	Overall Status	Progress Status	Risk Rating
207039	PHI	Approved		🟩
207302	PHI	Awaiting Review		🟨

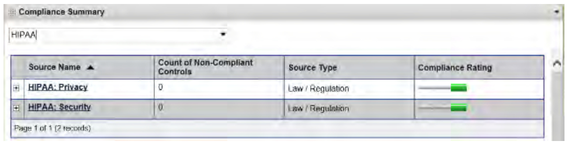
Page 1 of 1 (2 records)



3/22/2015 11:24 AM

Information Assets: Average Inherent Risk Score by Information Asset

C-1) & C-2) Perform compliance assessment, result/impact analysis and decision making

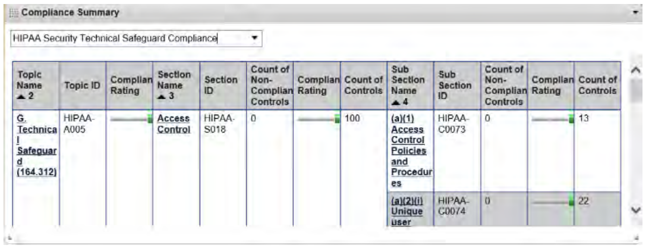


Compliance Summary

HIPAA

	Source Name ▲	Count of Non-Compliant Controls	Source Type	Compliance Rating
⊞	HIPAA: Privacy	0	Law / Regulation	
⊞	HIPAA: Security	0	Law / Regulation	

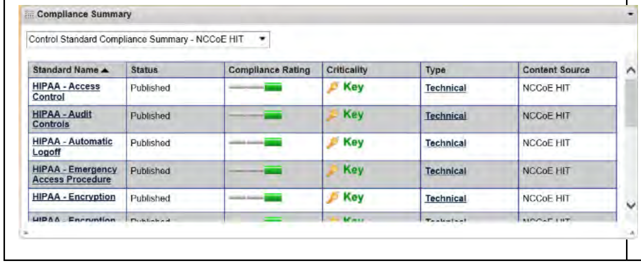
Page 1 of 1 (2 records)



Compliance Summary

HIPAA Security Technical Safeguard Compliance

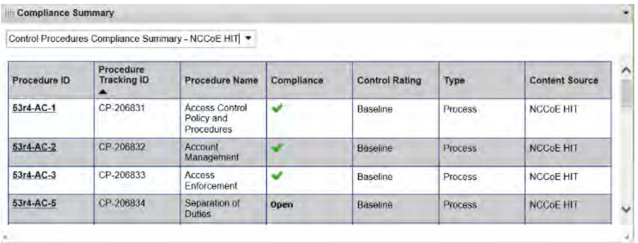
Topic Name ▲ 2	Topic ID	Complian Rating	Section Name ▲ 3	Section ID	Count of Non-Complian Controls	Complian Rating	Count of Controls	Sub Section Name ▲ 4	Sub Section ID	Count of Non-Complian Controls	Complian Rating	Count of Controls
G. Technical Safeguard (164.312)	HIPAA-A005		Access Control	HIPAA-S018	0		100	(a)(1) Access Control Policies and Procedures	HIPAA-C0073	0		13
								(a)(2)(i) Unique user	HIPAA-C0074	0		22



Compliance Summary

Control Standard Compliance Summary - NCCoE HIT

Standard Name ▲	Status	Compliance Rating	Criticality	Type	Content Source
HIPAA - Access Control	Published		Key	Technical	NCCoE HIT
HIPAA - Audit Controls	Published		Key	Technical	NCCoE HIT
HIPAA - Automatic Logoff	Published		Key	Technical	NCCoE HIT
HIPAA - Emergency Access Procedure	Published		Key	Technical	NCCoE HIT
HIPAA - Encryption	Published		Key	Technical	NCCoE HIT
HIPAA - Encryption	Published		Key	Technical	NCCoE HIT

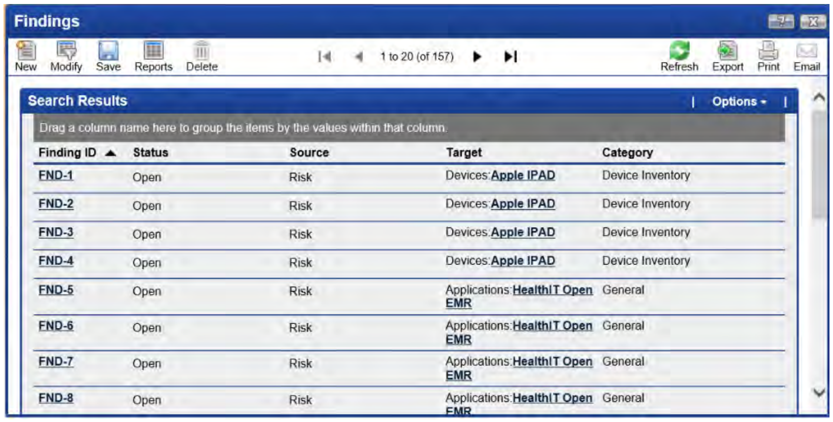


Compliance Summary

Control Procedures Compliance Summary - NCCoE HIT

Procedure ID	Procedure Tracking ID ▲	Procedure Name	Compliance	Control Rating	Type	Content Source
53r4-AC-1	CP-206831	Access Control Policy and Procedures	✓	Baseline	Process	NCCoE HIT
53r4-AC-2	CP-206832	Account Management	✓	Baseline	Process	NCCoE HIT
53r4-AC-3	CP-206833	Access Enforcement	✓	Baseline	Process	NCCoE HIT
53r4-AC-5	CP-206834	Separation of Duties	Open	Baseline	Process	NCCoE HIT

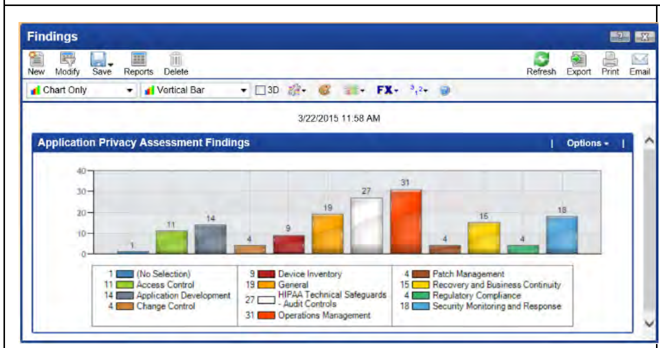
C-3) Manage Issues (Findings)

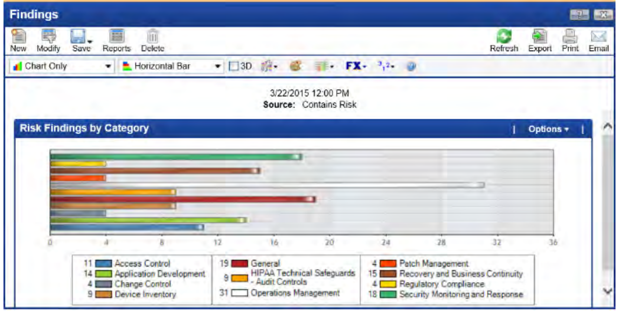


Search Results

Drag a column name here to group the items by the values within that column.

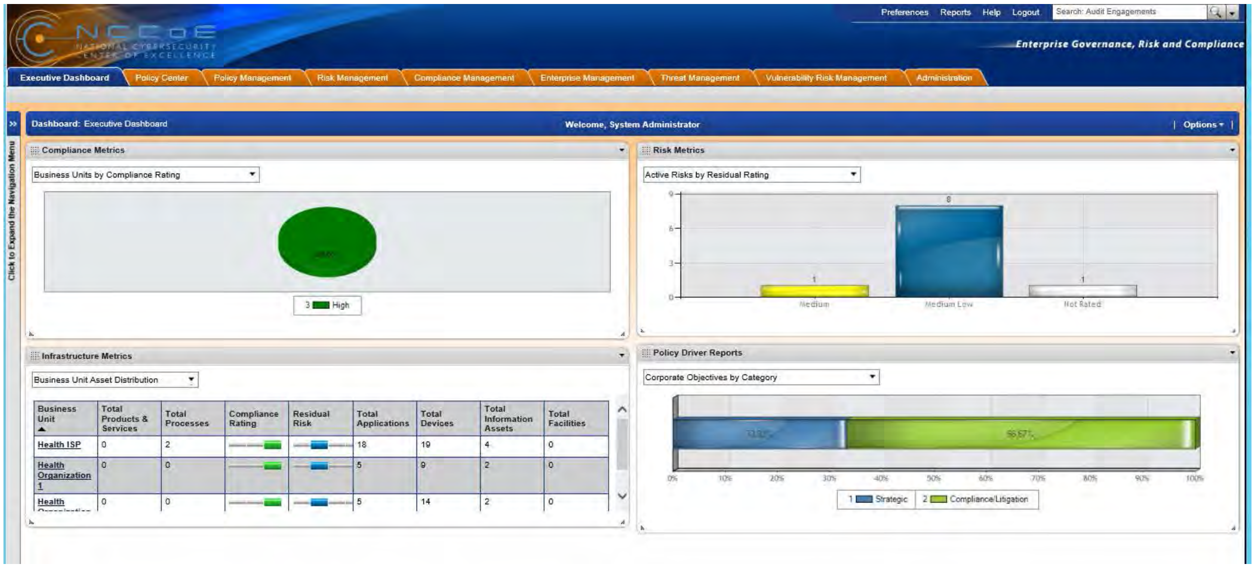
Finding ID ▲	Status	Source	Target	Category
FND-1	Open	Risk	Devices:Apple IPAD	Device Inventory
FND-2	Open	Risk	Devices:Apple IPAD	Device Inventory
FND-3	Open	Risk	Devices:Apple IPAD	Device Inventory
FND-4	Open	Risk	Devices:Apple IPAD	Device Inventory
FND-5	Open	Risk	Applications:HealthIT Open EMR	General
FND-6	Open	Risk	Applications:HealthIT Open EMR	General
FND-7	Open	Risk	Applications:HealthIT Open EMR	General
FND-8	Open	Risk	Applications:HealthIT Open EMR	General





Final) Customized reports and dashboards creation samples

Executive Dashboard



Preferences | Reports | Help | Logout
Search: Audit Engagements
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
Enterprise Governance, Risk and Compliance
Executive Dashboard
Policy Center
Policy Management
Risk Management
Compliance Management
Enterprise Management
Threat Management
Vulnerability Risk Management
Administration
Click to Expand the Navigation Menu
Options ▾
Compliance Metrics
Business Units by Compliance Rating ▾
3 🟩 High
Risk Metrics
Active Risks by Residual Rating ▾
9
6
3
0
1
8
1
Medium
Medium Low
Not Rated
Policy Driver Reports
Corporate Objectives by Category ▾
33.33%
66.67%
0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
1 ▬ Strategic
2 ▬ Compliance/Litigation

Dashboard: Executive Dashboard

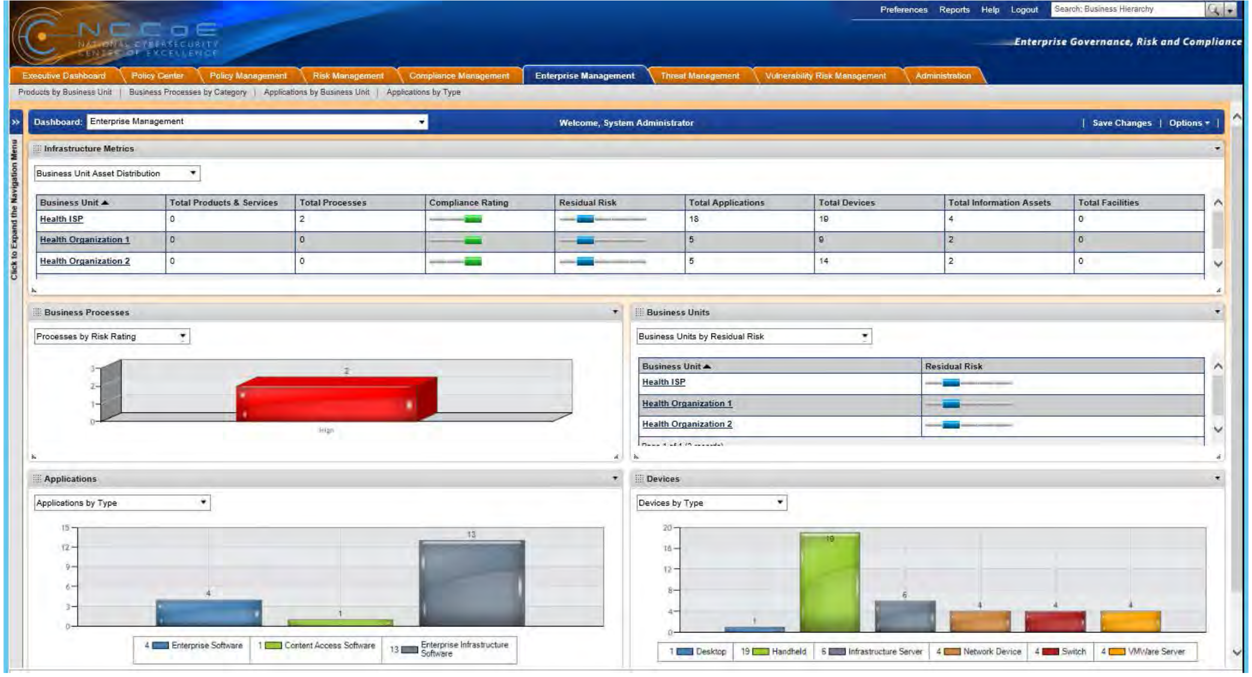
Welcome, System Administrator

Infrastructure Metrics

Business Unit Asset Distribution

Business Unit ▲	Total Products & Services	Total Processes	Compliance Rating	Residual Risk	Total Applications	Total Devices	Total Information Assets	Total Facilities
Health ISP	0	2	🟩	▬	18	19	4	0
Health Organization 1	0	0	🟩	▬	5	9	2	0
Health	0	0	🟩	▬	5	14	2	0

Enterprise Management Dashboard



Preferences | Reports | Help | Logout
Search: Business Hierarchy
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
Enterprise Governance, Risk and Compliance
Executive Dashboard
Policy Center
Policy Management
Risk Management
Compliance Management
Enterprise Management
Threat Management
Vulnerability Risk Management
Administration
Products by Business Unit | Business Processes by Category | Applications by Business Unit | Applications by Type
Click to Expand the Navigation Menu
Save Changes | Options ▾
Business Processes
Processes by Risk Rating ▾
3
2
1
0
2
High
Applications
Applications by Type ▾
15
12
9
6
3
0
4
1
13
4 ▬ Enterprise Software
1 ▬ Content Access Software
13 ▬ Enterprise Infrastructure Software
Devices
Devices by Type ▾
20
16
12
8
4
0
1
19
6
4
4
4
1 ▬ Desktop
19 ▬ Handheld
6 ▬ Infrastructure Server
4 ▬ Network Device
4 ▬ Switch
4 ▬ VMWare Server

Dashboard: Enterprise Management

Welcome, System Administrator

Infrastructure Metrics

Business Unit Asset Distribution

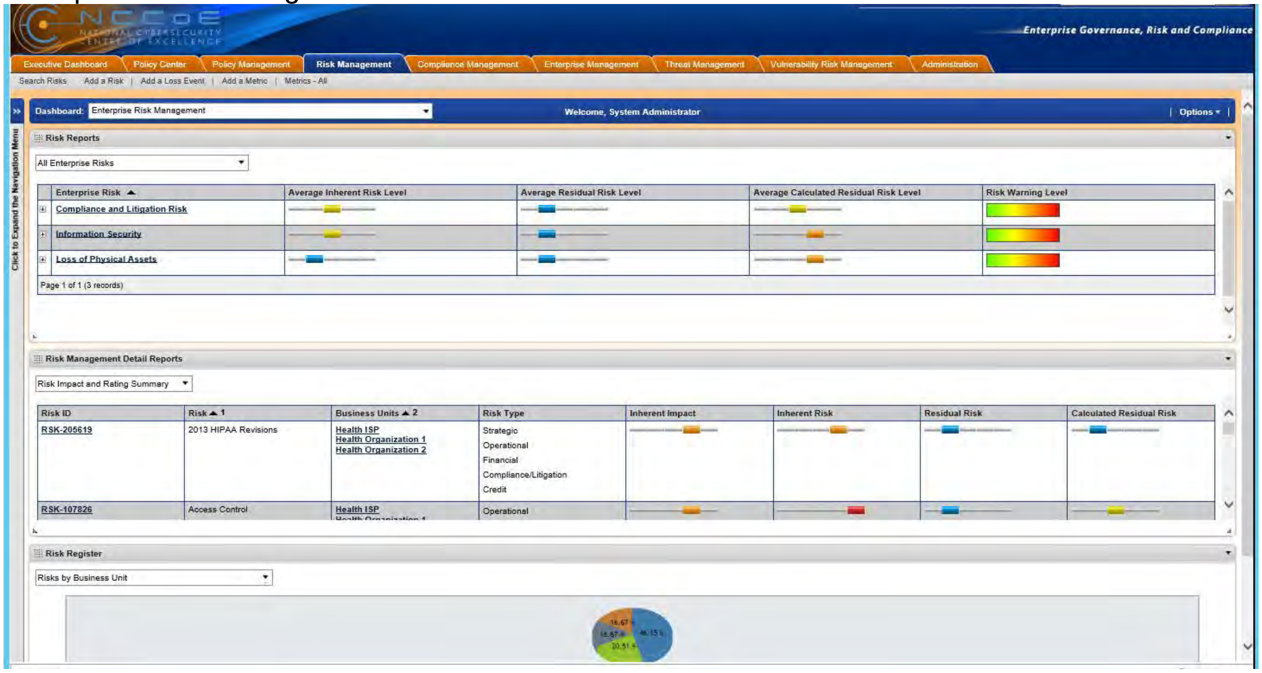
Business Unit ▲	Total Products & Services	Total Processes	Compliance Rating	Residual Risk	Total Applications	Total Devices	Total Information Assets	Total Facilities
Health ISP	0	2	🟩	▬	18	19	4	0
Health Organization 1	0	0	🟩	▬	5	9	2	0
Health Organization 2	0	0	🟩	▬	5	14	2	0

Business Units

Business Units by Residual Risk

Business Unit ▲	Residual Risk
Health ISP	▬
Health Organization 1	▬
Health Organization 2	▬

Enterprise Risk Management Dashboard



Dashboard: Enterprise Risk Management

Welcome, System Administrator

Risk Reports

All Enterprise Risks

Enterprise Risk ▲	Average Inherent Risk Level	Average Residual Risk Level	Average Calculated Residual Risk Level	Risk Warning Level
⊞ Compliance and Litigation Risk	🟨	🟦	🟨	
⊞ Information Security	🟨	🟦	🟧	
⊞ Loss of Physical Assets	🟦	🟦	🟧	

Page 1 of 1 (3 records)

Risk Management Detail Reports

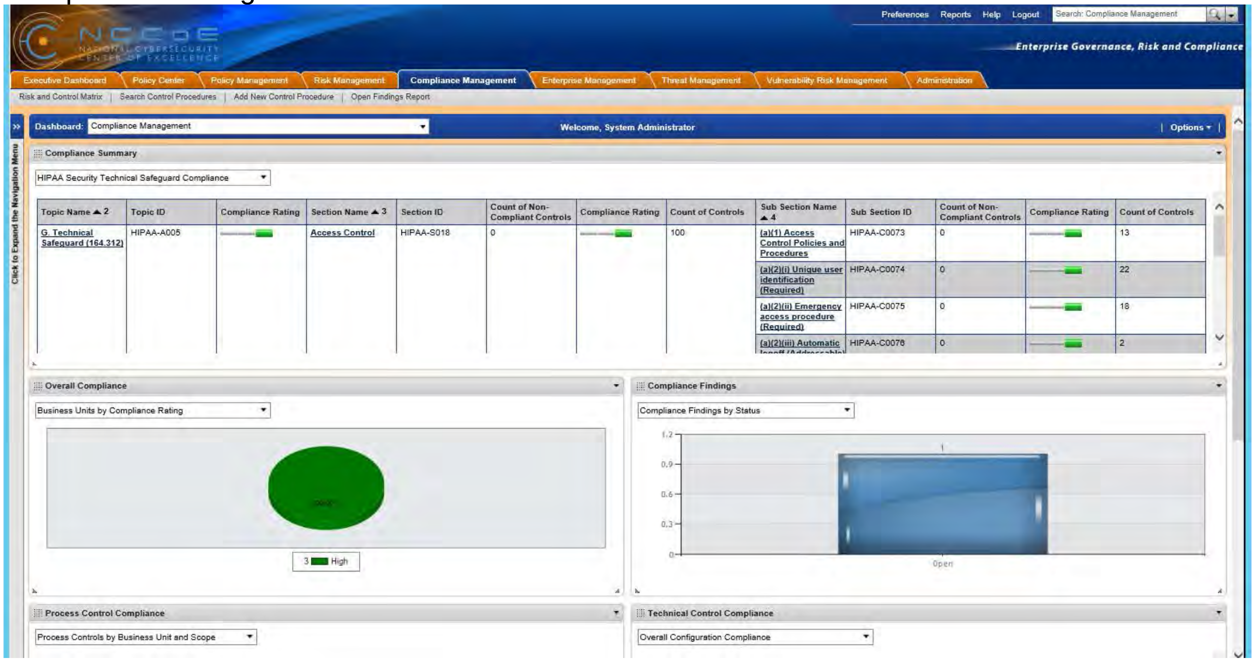
Risk Impact and Rating Summary

Risk ID	Risk ▲ 1	Business Units ▲ 2	Risk Type	Inherent Impact	Inherent Risk	Residual Risk	Calculated Residual Risk
RSK-205619	2013 HIPAA Revisions	Health ISP Health Organization 1 Health Organization 2	Strategic Operational Financial Compliance/Litigation Credit	🟧	🟧	🟦	🟦
RSK-107826	Access Control	Health ISP Health Organization 1	Operational	🟧	🟥	🟦	🟨

Risk Register

Risks by Business Unit

Compliance Management Dashboard



Dashboard: Compliance Management

Welcome, System Administrator

Compliance Summary

HIPAA Security Technical Safeguard Compliance

Topic Name ▲ 2	Topic ID	Compliance Rating	Section Name ▲ 3	Section ID	Count of Non-Compliant Controls	Compliance Rating	Count of Controls	Sub Section Name ▲ 4	Sub Section ID	Count of Non-Compliant Controls	Compliance Rating	Count of Controls
G. Technical Safeguard (164.312)	HIPAA-A005	🟩	Access Control	HIPAA-S018	0	🟩	100	(a)(1) Access Control Policies and Procedures	HIPAA-C0073	0	🟩	13
								(a)(2)(i) Unique user identification (Required)	HIPAA-C0074	0	🟩	22
								(a)(2)(ii) Emergency access procedure (Required)	HIPAA-C0075	0	🟩	18
								(a)(2)(iii) Automatic	HIPAA-C0076	0	🟩	2

Overall Compliance

Business Units by Compliance Rating

Compliance Findings

Compliance Findings by Status

Process Control Compliance

Process Controls by Business Unit and Scope

Technical Control Compliance

Overall Configuration Compliance

11 Operating Systems

We used two types of operating systems, Windows-based and Unix-based. These choices were driven by the commercial products used in this example solution. Typically, open-source products run on open-source Unix-based operating systems.

11.1 Windows Installation and Hardening

11.1.1 Windows System Requirements

This build requires purchase and installation of the Windows 2012 Server and Windows 7 and 8.1 for workstations. You will also need the following:

Processor	Minimum 1.4 GHz 64-bit processor
RAM	Minimum 8 G
Disk space	Minimum 150 GB

11.1.2 Windows Installation

We assume you purchased the appropriate Microsoft OS and that you have both the CD and product key.

If you are not familiar with Microsoft's command line or non-graphical management, we recommend you first select the Desktop Experience option to make the installation process easier.

> Microsoft recommends Server Core as the most secure installation of Windows 2012.[2] In this build, however, we recommend a known interface—Desktop Experience—to help those unfamiliar with Server Core to navigate. We feel our defense in depth strategy addresses some of the risks. As you become more familiar with Server Core, you should opt for that.

Boot the system with the installation disk and follow the onscreen instructions to enable:

- Desktop Experience Installation (Windows 2012 Server only) for Windows 2012, versions 7 and 8.1

[2] According to Microsoft, “The Server Core Installation option reduces the space required on disk, the potential attack surface, and especially the servicing requirements, so [Microsoft] recommends that you choose the Server Core installation unless you have a particular need for the additional user interface elements and graphical management tools that are included in the ‘Server with a GUI’ option. An intermediate state is possible where you start with a Server with a GUI installation and then remove Server Graphical Shell, resulting in a server that comprises the ‘Minimal Server Interface,’ Microsoft Management Console (MMC), Server Manager, and a subset of Control Panel.” https://technet.microsoft.com/en-us/library/hh831786.aspx

- Local firewall – all unneeded ports and protocols blocked inbound and outbound
- Windows update – on and in a regularly scheduled state
- Bitlocker – full disk encryption enabled
- IPV6 – off, unless absolutely needed for your environment
- Roles and features – install only the roles and features needed to provide the production feature needed to serve your organization; remove all others if possible

See Section 3.1, Hostnames for hostnames to use.

> If you opt to change your organization's hostnames, you should make note of any changes for comparison and make necessary changes to the implementation of other products described here.

11.1.3 Windows Post-Installation Tasks

- Install the Puppet agent by following the Puppet Enterprise instructions in Section 5.
- Install the backup agent by following the URBackup instructions in Section 4.

11.1.4 Windows Security Hardening

11.1.4.1 Using Puppet

We employed Windows operating system hardening tasks that use the Puppet Enterprise Configuration Tool. At the least, each Windows system should be configured to receive base and custom sets of configuration enforcement instructions from Puppet. Puppet uses configuration files called manifests to house configuration enforcement instructions. The list of base Windows configuration manifests is below, along with a short explanation on why each was implemented on the Windows systems in this build.

Puppet Manifests

accounts.pp - allows control over users who can log in and their passwords. If an attacker changes any information, puppet will change settings back based on the entries in this file.

> We configured this feature, but did not use it, for Windows. In this case, organizations that wish to implement it can view this file as a demonstration.

site.pp – the build described in this practice guide uses the *site.pp* file as a main launch point for all of the various classes in the manifests file. In this case, there is one class in the *site.pp* file itself that configures Windows systems to enable firewalls, deny reboots with logged in users, and ensure Windows updates are on.

11.1.4.2 Using Security Technical Implementation Guides (STIGs)

The Department of Defense (DoD) Defense Information Systems Agency created and manages a series of technical security best practice guides that assist DoD services and agencies with hardening their systems. Many of the STIG documents are based on the NIST 800 series guidance and controls recommended for systems security. Organizations implementing Windows systems similar to the architecture described in this document should use these guides as ancillary references on how to secure their systems. Because the DoD considers protection from nation-state threats regarding unauthorized access to personally identifiable information, government secrets, and health information important, that may not be practical or functional in a private sector health organization.

The STIG process, specific operating system guidance, and automated assessment files can be downloaded at *http://iase.disa.mil/stigs/os/Pages/index.aspx*.

11.2 Linux Installation and Hardening

11.2.1 Linux Installation

Download the Fedora 20 image from the following links:

- 64 bit - *http://archive.fedoraproject.org/pub/fedora/linux/releases/20/Images/x86_64/*
- 32 bit - *http://archive.fedoraproject.org/pub/fedora/linux/releases/20/Images/i386/*

Download the Fedora 20 installation guides:

- PDF: *http://docs.fedoraproject.org/en-US/Fedora/20/pdf/Installation_Guide/Fedora-20-Installation_Guide-en-US.pdf*
- HTML: *http://docs.fedoraproject.org/en-US/Fedora/20/html/Installation_Guide/*

See Section 3.1, Hostnames for hostnames to use.

> If you opt to change your organization’s hostnames, you should make note of any changes for comparison and make necessary changes to the implementation of other products described here.

Use full disk file encryption on all Linux systems as described in the Fedora 20 installation guides.

Use separate disk partitions or hard disks to create the *root, var, usr* and *etc* partitions as described in the Fedora 20 installation guides. The electronic health record application should have its own partition or disk.

Use a 100G disk, at least, to allow for system and other logs.

11.2.2 Linux Post-Installation Tasks

Install the Puppet agent by following the Puppet Enterprise installation instructions in Section 5.

Ensure that all the base system files recommended in Section 11.2, Linux Installation and Hardening are configured in Puppet Master for this host.

Follow the instructions in Section 5.2, Puppet Enterprise Configuration to configure the hostname in the *site.pp* file.

Install the backup agent by following the URBackup instructions in Section 4.1.

11.2.3 Linux Security Hardening

Use the Puppet Enterprise configuration tool for all Linux operating system hardening tasks. Configure each Linux system to receive base and custom sets of configuration enforcement instructions from Puppet. Puppet uses configuration files called manifests to house configuration enforcement instructions. The base Linux configuration manifests list is below, along with a short explanation on why they were implemented on all Linux systems used in this build.

Puppet Manifests

accounts.pp – allows control over users who can log in and also controls the password. If an attacker changes any information in the password file, Puppet will change settings back based on the entries in this file

crontabconfig.pp – creates tasks that run automatically at set intervals. In this case, there are four tasks that are executed to secure Linux:

1. logoutall.sh – runs every few seconds and kills all other user tasks with exception of root, effectively removing normal users from all the Linux systems while they are in production mode
2. puppetagent.config.base.sh – periodically runs the Puppet agent to update any changes to the configuration of the local system based on a remote Puppet Master configuration change
3. yum.config.base.sh – forces the local system to update itself during set a time every day
4. harden.os.single.commands.sh – a series of single commands to ensure changes to permissions on critical system files that disable root console or other one-line commands

firewallrules.pp – creates and enforces individual *IPtables* rules on each local Linux host in accordance with the least access needed in or out of the system

grub2fedora20.pp – this build implemented versions of Fedora 20 with the Grub2 bootloader. The bootloader assists with starting the Linux operating system and allowing the operator to make special configurations prior to the system boot process. This access can be dangerous because it will allow an attacker to boot the system into single user mode or make other changes prior to the boot process. The changes made with this Puppet manifest file create a Grub2 password challenge

packages.pp – ensures that less secure applications are removed and only the applications needed to run the service are installed on the local system

passwdfile.pp – cleans password file of standard users that come with the Fedora 20 Linux distro. It also cleans the group file

securettyfile.pp – creates a new security file in the local system that prevents root from logging into a console session

ssh.pp – hardens the encrypted remote management service for Linux *time.pp* – forces the local system to use a time server for accurate time; creates accurately time-stamped logs

warningbanners.pp – creates warning banners at the console and remote login sessions that warn users that their sessions should be authorized and monitored. This banner should deter good people from accidentally doing bad things. It will not stop a determined attacker under any circumstances