# Securing Electronic Health Records on Mobile Devices

**Volume C:**
**How-To Guides**

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

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

**Colin Bowers**
**Kyle Kamke**
Ramparts, LLC
Clarksville, MD

July 2018

**NIST**
**National Institute of Standards and Technology**
**U.S. Department of Commerce**

**NCCoE**
**NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

## DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document 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, equipment, products, or materials are necessarily the best available for the purpose.

## FEEDBACK

As a private-public partnership, we are always seeking feedback on our Practice Guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at hit_nccoe@nist.gov.

All comments are subject to release under the Freedom of Information Act (FOIA).

<div align="center">

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

</div>

## NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov. To learn more about NIST, visit https://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 align more easily with relevant standards and best practices and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

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

## ABSTRACT

Healthcare 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 healthcare providers, mobile devices can introduce vulnerabilities in a healthcare organization's networks. At the 2012 Health and Human Services Mobile Devices Roundtable, participants stressed that many providers are using mobile devices for healthcare delivery before they have implemented safeguards for privacy and security [1].

This NIST Cybersecurity Practice Guide provides a modular, open, end-to-end reference design that can be tailored and implemented by healthcare organizations of varying sizes and information technology (IT) sophistication. Specifically, the guide shows how healthcare providers, by using open-source and commercially available tools and technologies that are consistent with cybersecurity standards, can more securely share patient information among caregivers who are using mobile devices. The scenario considered is that of a hypothetical primary care physician using her mobile device to perform recurring 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 healthcare provider's existing tools and infrastructure.

## KEYWORDS

## ACKNOWLEDGMENTS

| Technology Partner/Collaborator | Build Involvement |
|---|---|
| Cisco | Identity Services Engine (ISE), Adaptive Security Virtual Appliance (ASAv), and RV220W |
| IBM | MaaS360 |
| Intel | Intel® Identity Protection Technology (Intel® IPT) with Public Key Infrastructure (PKI) |
| MedTech Enginuity | OpenEHR software |
| Ramparts | Risk assessment and security testing |
| RSA | Archer Governance, Risk & Compliance (GRC) |
| Symantec | Endpoint Protection |

# Contents

# List of Figures

# List of Tables

# 1    Introduction

The following guides show information technology (IT) professionals and security engineers how the NCCoE implemented this example solution for securing the transfer of electronic health records (EHRs) on mobile devices. We cover all the products in the selected versions 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 into our environment.

These guides assume that you have experience implementing security products in a healthcare 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. 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 done. Refer to National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-1D: Standards and Controls Mapping, Section 4, 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 alternative products. NIST SP 1800-1D, Section 4, Security Characteristics and Controls, Table 2, describes how we arrived at this list of controls.

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

- The NCCoE developed an example solution to this problem by 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 the 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.

## 1.1    Practice Guide Structure

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices.

A NIST Cybersecurity Practice Guide does not describe "the" solution but a possible solution. We seek feedback on this guide's contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to hit_nccoe@nist.gov.

*Note: 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.*

## 1.2 Typographic Conventions

The following table presents typographic conventions used in this volume.

| Typeface/Symbol | Meaning | Example |
|---|---|---|
| *Italics* | filenames and pathnames references to documents that are not hyperlinks, new terms, and placeholders | For detailed definitions of terms, see the *NCCoE Glossary.* |
| **Bold** | names of menus, options, command buttons and fields | Choose **File > Edit**. |
| `Monospace` | command-line input, on-screen computer output, sample code examples, status codes | `mkdir` |
| **`Monospace Bold`** | command-line user input contrasted with computer output | **`service sshd start`** |
| [blue text] | link to other parts of the document, a web URL, or an email address | All publications from NIST's National Cybersecurity Center of Excellence are available at https://www.nccoe.nist.gov. |

# 2 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.

## 2.1 Windows Installation and Hardening

### 2.1.1 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 GB

Disk space       Minimum 150 GB

## 2.1.2     Windows Installation

We assume you purchased the appropriate Microsoft operating system (OS) and that you have both the compact disc and product key.

If you are not familiar with Microsoft's command line or nongraphical management, we recommend that 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

- 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.

## 2.1.3     Windows Post-Installation Tasks

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

## 2.1.4     Windows Security Hardening

### 2.1.4.1     Using Puppet

We employed Windows OS 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 of 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 that Windows updates are on.

### 2.1.4.2    Using Security Technical Implementation Guides (STIGs)

The Department of Defense's (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 to be important, that the STIG 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.

## 2.2    Linux Installation and Hardening

### 2.2.1    Linux Installation

We downloaded the Fedora 20 image from the following links:

- 64 bit — http://archives.fedoraproject.org/pub/archive/fedora/linux/releases/20/Images/x86_64/

- 32 bit — http://archives.fedoraproject.org/pub/archive/fedora/linux/releases/20/Images/i386/

We 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 implementing 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 EHR application should have its own partition or disk.

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

### 2.2.2    Linux Post-Installation Tasks

Install the Puppet agent by following the Puppet Enterprise installation instructions in Section 4.2.

Follow the instructions in Section 4.2, Puppet Enterprise Configuration, to configure the hostname in the *site.pp* file.

Install the backup agent by following the UrBackup instructions in .

## 2.2.3    Linux Security Hardening

Use the Puppet Enterprise configuration tool for all Linux OS 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 of 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, four tasks 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 the systems 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 a set 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 online 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 accurate time-stamped logs.

*warningbanners.pp* – creates warning banners at the console and remote login sessions that warn users that their sessions will 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.

# 3   Basic Network Infrastructure Services

Basic network infrastructure services exist throughout the architecture and consist of all switching and routing protocols related to layer 2 and layer 3 of the Open Systems Interconnection 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 internet protocol (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 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.

**Table 3-1 Qualified Domain Names and IP Addresses Used in This Build**

| 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 | 192.168.200.252 |
| 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 |

| Capability Name | Hostname/FQDN | IP |
|---|---|---|
| HealthIT Organization #1 Mobile Devices | | 10.10.101.0/24 |
| HealthIT Organization #2 Mobile Devices | | 10.10.102.0/24 |

## 3.2 Bind Domain Name System (DNS) and Domain Names Search Engine (DNSE) Installation and Hardening

The 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 split-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 8 GB

- Disk space       Minimum 150 GB

**You will also need the following parts of this guide:**

- Section 2.2, Linux Installation and Hardening

- Section 3.1, Hostnames

- Section 4.2, 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.

Install Bind DNS by using root or sudo by entering the following (procedures are the same for Internal DNS and External DNS):

```
> 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 Internet Service Provider (ISP) by entering:

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

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

```
> vi healthitorg1.org
```

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

```
> vi healthitorg2.org
```

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

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

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

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

Sample DNS files used in this build can be found in the online file repository for this use case at
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1-draft.zip.

## 3.3   Firewalls: IP Tables

A firewall is used to control egress and ingress network traffic among multiple subnets and/or systems.
A firewall will determine what traffic goes in what 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 among other
subnets has a firewall to protect internet traffic from traversing inbound to the internal network.

**Figure 3-1 Integrated Firewalls**
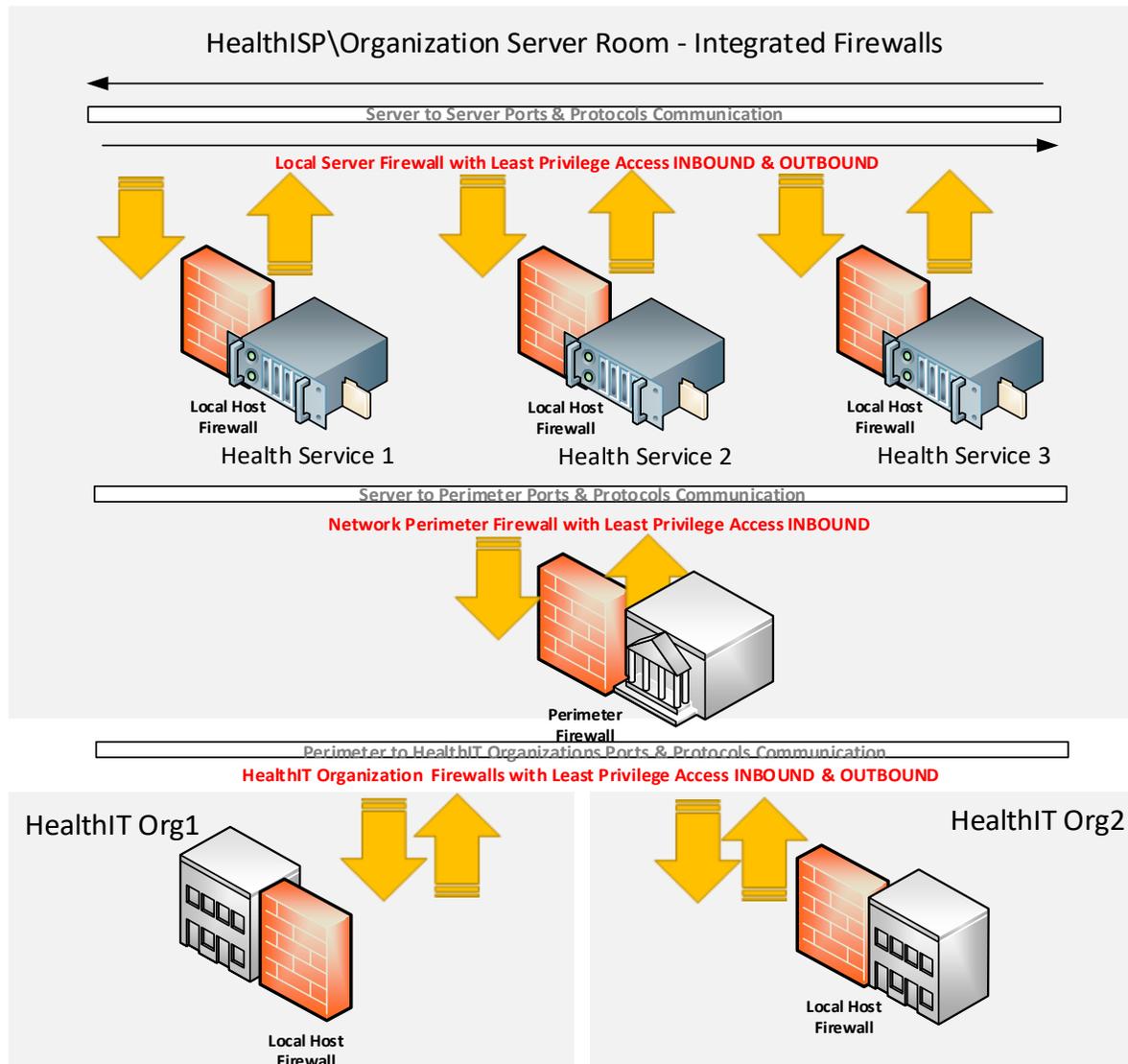


**System requirements**

- Linux OS

- 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 list [HCL] for more)

- If this is a system that protects multiple subnets, then multiple network interface cards (NICs) 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 2.2.2, 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 below has been followed.

## 3.4 Intrusion Detection System (IDS)

An IDS monitors a network for known threats to an organization's 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 transmission control protocol (TCP) transmission analysis.

### 3.4.1 Security Onion

Security Onion is the IDS selected for this build. It was selected based on its record in the open-source community for its support of 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 might not have been asked.

- **Sguil** – used as a database for IDS alerts.

- **ELSA** – allows the user 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://github.com/security-onion-solutions/security-onion/wiki/Hardware.

- Find the ISO (International Standards Organization) image full version at https://github.com/security-onion-solutions/security-onion/wiki/quickISOimage.

- Find the Install Version for Ubuntu Linux at https://github.com/security-onion-solutions/security-onion/wiki/InstallingOnUbuntu.

**You will also need the following parts of this guide:**

- Section 2.2, Linux Installation and Hardening

- Section 3.1, Hostnames

**Security Onion setup**

We followed the documentation provided by Security Onion:

- Introduction
  https://github.com/security-onion-solutions/security-onion/wiki/IntroductionToSecurityOnion

- Production installation steps
  https://github.com/security-onion-solutions/security-onion/wiki/ProductionDeployment

- Booting issues
  https://github.com/security-onion-solutions/security-onion/wiki/TroubleBooting

- Post-installation
  https://code.google.com/p/security-onion/wiki/PostInstallation

# 4 Configuration Management

Understanding, implementing, and maintaining a secure baseline for all systems that process and store protected health information (PHI) is critical to the systems' 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

**Figure 4-1 System Security Baseline and Configuration Management System**
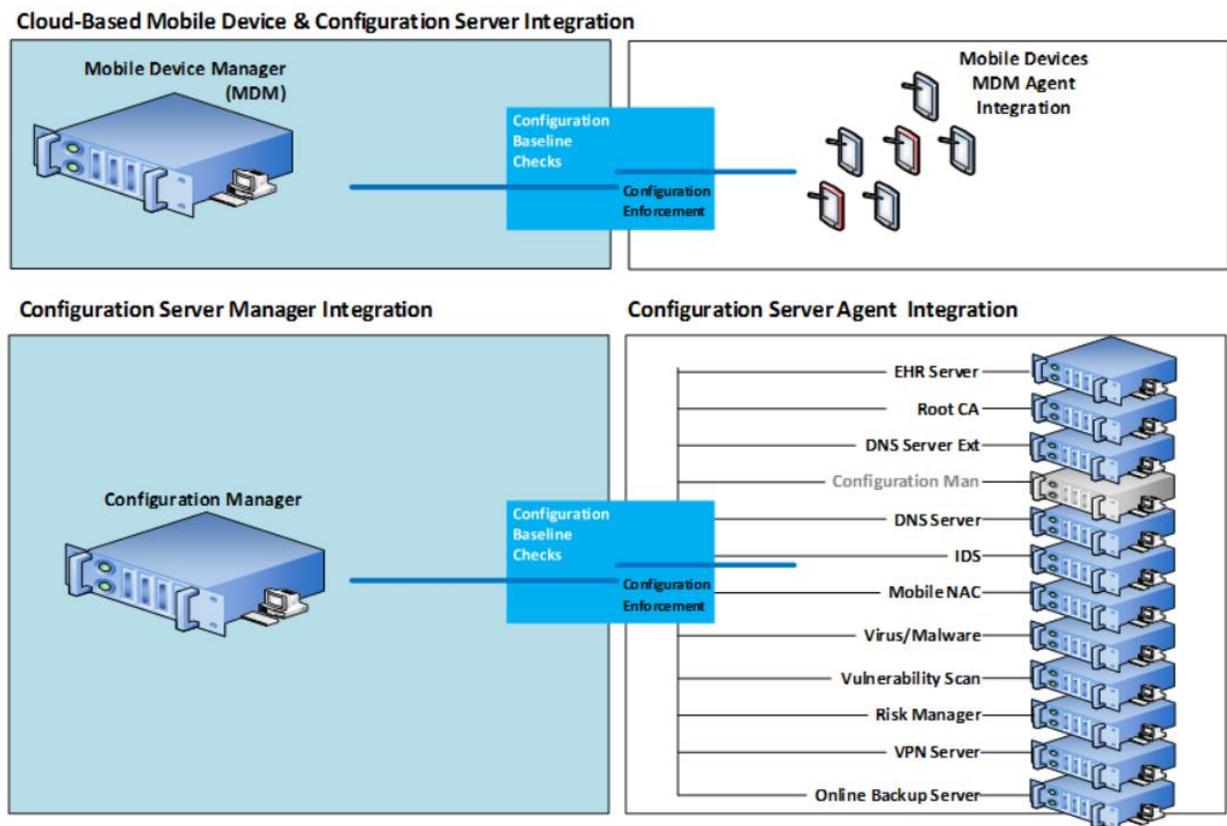
**System requirements**

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

**You will also need the following parts of this guide:**

- Section 2.2, Linux Installation and Hardening
- Section 3.1, Hostnames

## 4.1  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.

### 4.1.1  Pre-installation Tasks

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

### 4.1.2  Installation Instructions

This build used Puppet Enterprise on Fedora 20 Linux. Find install instructions for Puppet Enterprise at Fedora 20.

### 4.1.3  Post-Installation 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 4.2, Puppet Enterprise Configuration. We give specific guidance in Section 4.2.3 regarding changes to the Puppet Enterprise post-installation documentation.

According to the post-installation 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-installations unless you are familiar with the security implications and advanced features.

- Automatic Puppet Master Certificate Processing – this has security implications.
- 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-installation 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 4.2.5, Puppet Enterprise Web-Based Reporting Installation and Configuration; and in Section 4.3, Production Web Server.

## 4.2    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 used Puppet templates to assist with creating Linux-based files to be used in configuration management and secure baseline controls.

### 4.2.1    Puppet.conf

The *puppet.conf* file for the Puppet Master is located in the */etc/puppet* directory. The configuration file for this build can be found at https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1-draft.zip. Once downloaded, the file should be moved to the */etc/puppet/puppet.conf* directory of Puppet Master.

### 4.2.2    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/projects/use_cases/medical_devices.

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 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 manifest imports and calls to predefined classes created in each manifest.

- *accounts.pp* – this file 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 it back based on the entries in this file.

- *crontabconfig.pp* – this file creates tasks that run automatically at set intervals. In this case, four tasks 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 the systems 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 a set time every day.

- *harden.os.single.commands.sh* – this is a series of single commands to ensure that changes to permissions on critical system files and 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 OS 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 Transport Layer Security (TLS) and Online Certificate Status Protocol (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 accurate time-stamped logs.

▪ *warningbanners.pp* – this creates warning banners at the console and remote login sessions that warn users that their sessions will be authorized and monitored. This banner should deter good people from accidentally doing bad things. It will in no way stop a determined attacker under any circumstances.

## 4.2.3   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 re-create 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 in this build can be downloaded from this page: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1-draft.zip.

Once you download the templates, move them to the */var/lib/puppet/templates* directory. The templates directory may need to be created by 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 nonroot 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*

## 4.2.4 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 by 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
```

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

- ▪ *puppetlabs-apache* – streamlined creation of web services by using Apache
- ▪ *puppetlabs-mysql* – streamlined edits of *mysql* with minimal configuration
- ▪ *puppetlabs-concat* – allows creation of configuration files based on concatenation
- ▪ *puppetlabs-ntp* – allows the user to manage standard time on systems
- ▪ *puppetlabs-registry* – allows edits to the Windows registry for configuration
- ▪ *puppetlabs-stdlib* – the standard library for resources on Puppet

## 4.2.5 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:**

After downloading the puppet-dashboard package, 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.<YourOrganization>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
```

## 4.3    Production Web Server

These instructions are for a nonproduction 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.

# 5    Backup

The backup system is an important part of security, as it assists with ensuring that 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 off-site backups are harder to tamper with or lose in a local disaster to the architecture.

This section will show you how to install an online backup system by using UrBackup.

UrBackup is a remote backup system that will facilitate both full and incremental backups. It is 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 8 GB
- ▪ Disk space         Minimum 150 GB

**You will also need the following parts of this guide:**

- ▪ Section 2.2, Linux Installation and Hardening
- ▪ Section 3.1, Hostnames
- ▪ Section 4.2, Puppet Enterprise Configuration

## 5.1    UrBackup Server Setup

Baring details on http://urbackup.org/download.html, download software and compile the server:

1. Download the *UrBackup server* source tarball and extract it.

2. Install the dependencies. Those are *gcc*, *g++*, *make*, *libcrypto++*, and *libcurl* (as development versions).

3. Compile and install the server via `./configure`, `make`, and `make install`.

4. Run the server with `start_urbackup_server`.

5. Add */usr/sbin/start_urbackup_server* to your */etc/rc.local* to start the *UrBackup server* on server start-up.

After you have installed the UrBackup Server, perform the following steps:

1. Go to the user settings and add an admin account. If you do not do this, everybody who can access the server will be able to see all backups.

     a.   Set up the mail server by entering the appropriate mail server settings.

     b.   If you want the clients to be able to back up via the internet and not only via local network, configure the public server name or IP of the server in the internet settings.

2. If you want to get logs of failed backups go the Logs screen and configure the reports for your email address.

Change any other setting according to your usage scenario.

## 5.2 UrBackup Client Setup

Follow these instructions to build, install, and set up UrBackup on Fedora 20 Linux systems.

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

1. Follow Section 2.2, Linux Installation and Hardening.

2. Install the dependencies UrBackup needs:

     a.   If installing on Fedora 20, there should be a WxWidgets application already installed. If not, download the WxWidgets and install it according to the installation instruction. Please verify that its version is higher than 3.0 by using the command `wx-config--version`.

     b.   On Fedora 20, you will use *yum* as your installer.

3. Input the following commands:

```
> 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 path name 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. Set up 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
   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 of 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 to resolve the above authentication error:

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

a. Log in to the UrBackup Server via the web link http://<yourhost.yourdomain.com>:55414.

b. Go to the Status screen.

c. Under Internet Clients enter the FQDN name of the laptop/personal computer (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.

d. 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.

e. In 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.

f. 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.

g. 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 back end on start-up by using the following for Fedora 20:

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

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

```
[Unit]
Description=Starting back end 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 boot-up:

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

**Or**

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

8. Start the UrBackup client back end on start-up by 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:

   a. Log in to the UrBackup Server web portal.

   b. Use the client dropdown menu and select the client for whom you want to set custom settings for this configuration.

   c. Select the Separate Settings for This Client radio button and begin edits.

   d. 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 -- 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
```

# 6 Certificate Authority

The certificate authority (CA) uses the OpenSSL cryptographic libraries to create and then sign soft certificates for use in identifying mobile devices that would ultimately connect to both the access point (AP) and the OpenEMR server. The CA 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 CA. Using a public key infrastructure (PKI) approach is among the strongest methods to ensure proper identity and access control for PHI.

## 6.1 Fedora PKI Manager

The CA used for this build is based on a Linux PKI Manager used in Fedora, RedHat Enterprise, and other production-class Linux distros.

**System requirements**

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

**You will also need the following parts of this guide:**

- Section 2.2, Linux Installation and Hardening
- Section 3.1, Hostnames
- Section 3.2, Bind Domain Name System (DNS) and Domain Names Search Engine (DNSE) Installation and Hardening
- Section 4.2, Puppet Enterprise Configuration

**Fedora PKI Manager Installation**

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

## 6.2 Post-Installation

Fedora PKI Manager Administrator setup instructions can be found at http://pki.fedoraproject.org/wiki/CA_Admin_Setup.

To manually create user/device certificates, follow the steps in Section 10.1, Mobile Devices, 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 will be a list of pending requests. Write down the request number for use later in the process. 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 your certificate request reference number that was 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 10.1 for details on how to install the certificate.

# 7    Identity and Access Controls

This build utilizes a RADIUS server integrated with our CA and AP, which combine to create the full identity and access control function. A RADIUS server uses the authentication, authorization, and accounting (AAA) protocol to manage network access via those functions. 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 CA as a recipient of a signed root certificate and OCSP communication. The authorization mechanism is integrated with the mobile device manager to check mobile device policy for compliance.

**Figure 7-1 Integrated Web-Based Mobile EHR System Architecture**
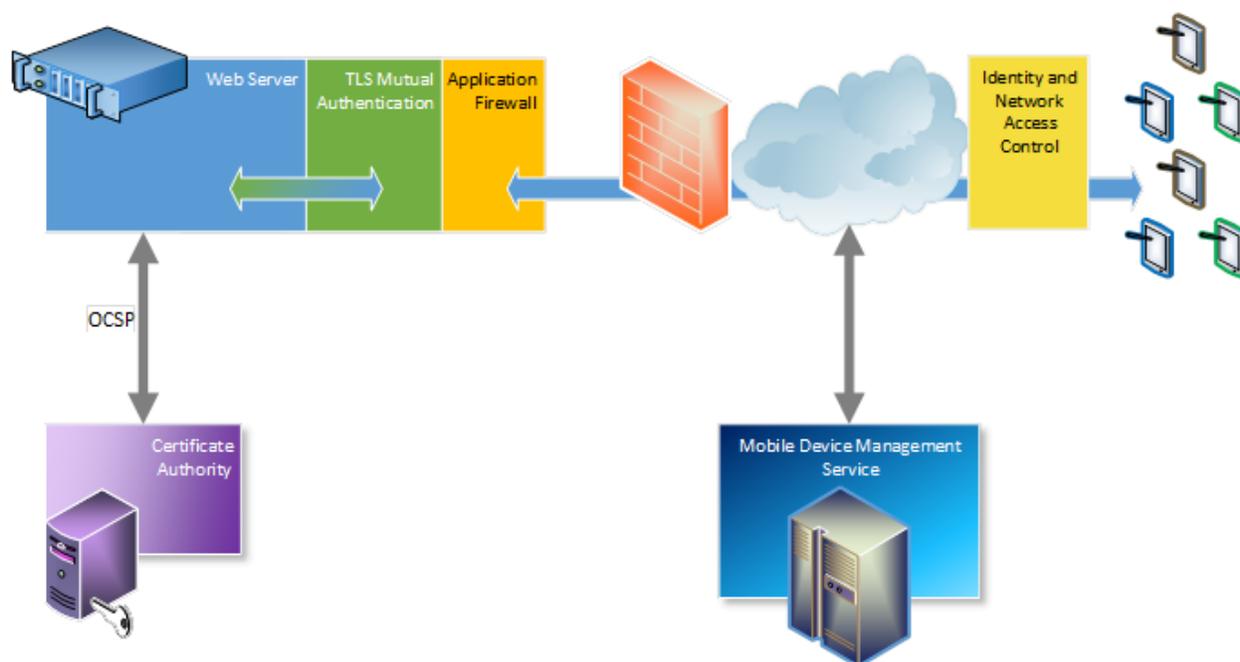


## 7.1    Cisco Identity Services Engine

Benefits of the Cisco Identity Services Engine (ISE):

▪  Identity and access policy management are centralized and unified.

▪  Certificate challenges provide visibility and more assured device identification.

▪  Organizations can use business rules to segment access to sections of the network.

▪  The user experience during the challenge process is made seamless.

**System requirements**

- Virtual Hypervisor (VH) capable of housing virtual machines (VMs)

- VM with central processing unit (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 6.1, Fedora PKI Manager

- Section 10.2.1, 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 VM.

2. Follow the guidance from your VM vendor to boot the DVD or ISO and start the installation
   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 with the CLI and the admin portal access are provided by the Cisco ISE

More detailed procedures for installing the Cisco ISE are available from the installation guide provided by Cisco, available at https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/installation_guide/ise_ig/ise_pref.html.

## 7.2 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.

## 7.3 Configure Cisco ISE to Support EAP-TLS Authentication

### 7.3.1 Set ISE to support RADIUS authentication

The following steps are used to set up a communication connection from Cisco ISE to the network device (AP) 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.

   - 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 Advanced Encryption Standard (AES) Key Wrap algorithm. However, you should be experienced with Cisco ISE and confident that your network device supports this configuration.

### 7.3.2 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 Common Name (CN) field matches the FQDN of the Cisco ISE server.

2.  Export the CSR from the navigation path **Administration > System > Certificates > Certificate Signing Requests,** then select **Export.**

3.  Save and submit the CSR file to a CA. 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 6, Certificate Authority.

5.  Use the ISE Administration interface to bind the acquired CA-signed certificate with its private key by using the path **Administration > System > Certificates > Local Certificates,** then **Add > Bind CA Signed Certificate.**

If you intend to use this certificate for client Extensible Authentication Protocol-Transport Layer Security (EAP-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.

### 7.3.3    Populate Certificate Store with Required CA-Signed Certificates

The CA-signed root certificate and the certificate for Fiberlink MaaS360 MDM server are required by the certificate store. You will need to have the CA root certificate in Privacy Enhanced Mail (PEM) or Distinguished Encoding Rules (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 6, 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.

### 7.3.4    Set Identity Source for Client Certificate Authentication

No internal or external identity source is required for the EAP-TLS certificate-based authentication method because 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.

## 7.3.5    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, Protected Extensible Authentication Protocol, and the 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.

## 7.3.6    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 a Hypertext Transfer Protocol Secure (HTTPS) session from the ISE to the Fiberlink MaaS360 server located in the public internet. The session is established outbound from ISE toward 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.

    a.  From the browser, log on to the MaaS360: https://login.maas360.com*.*

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

**Figure 7-2 Page Info Window**
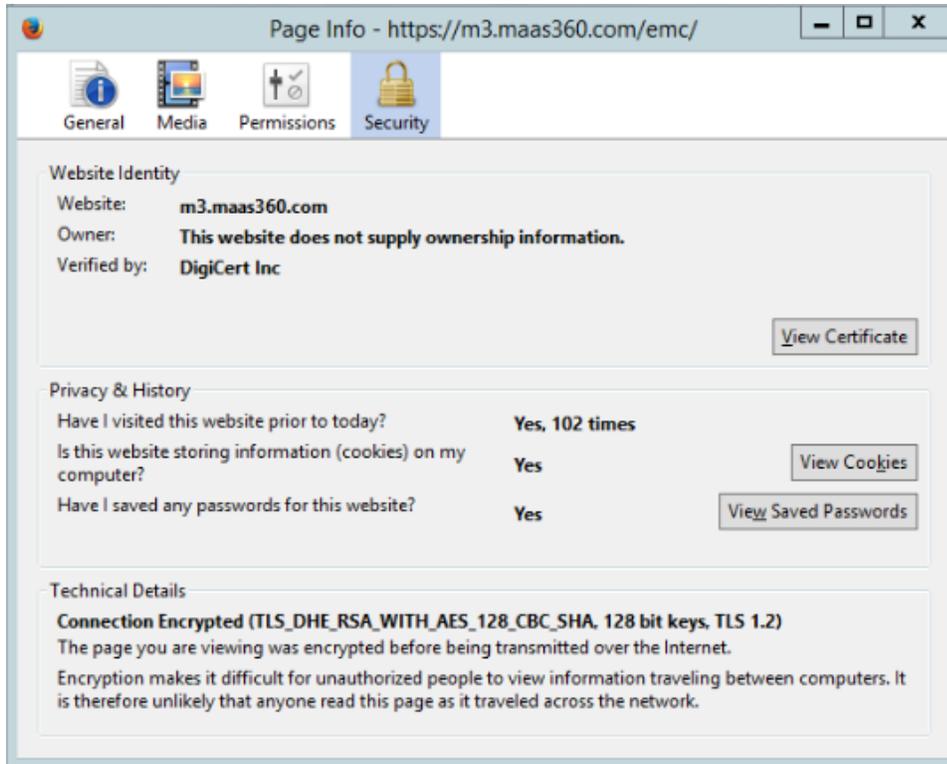


c. Click the **View Certificate** button to view the certificate.

**Figure 7-3 Certificate Viewer – General**
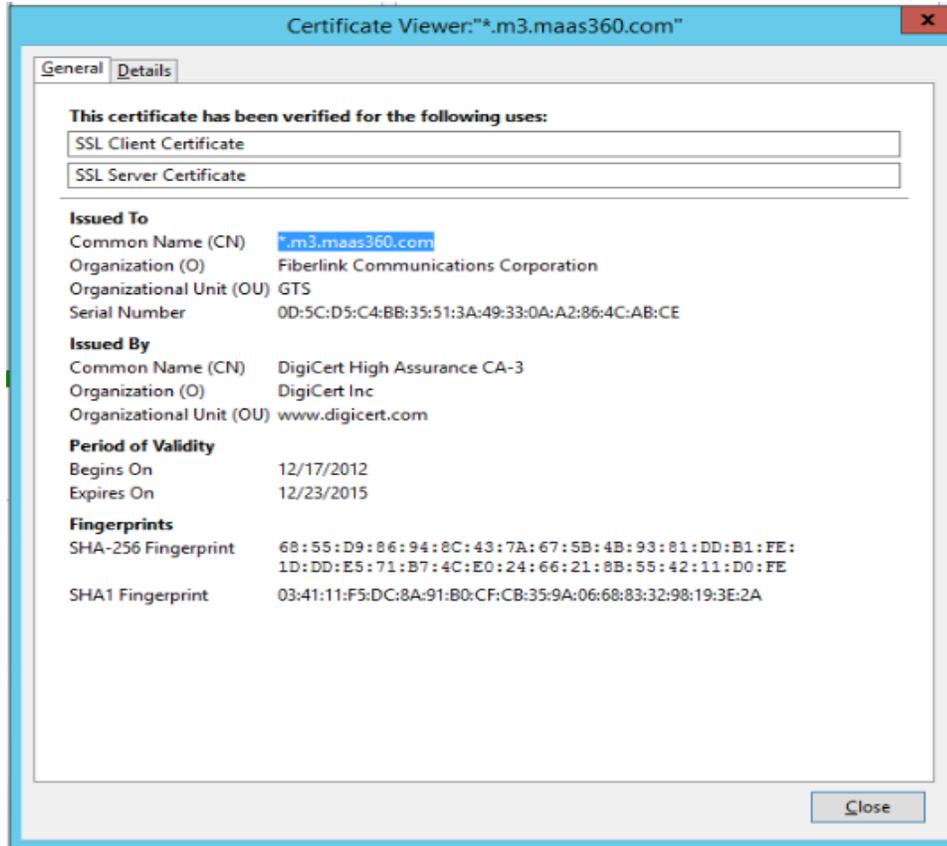


d.  Select the **Details** tab to view the detailed certificate information. From there you should have an **Export** button to export the certificate.

**Figure 7-4 Certificate Viewer – Details**
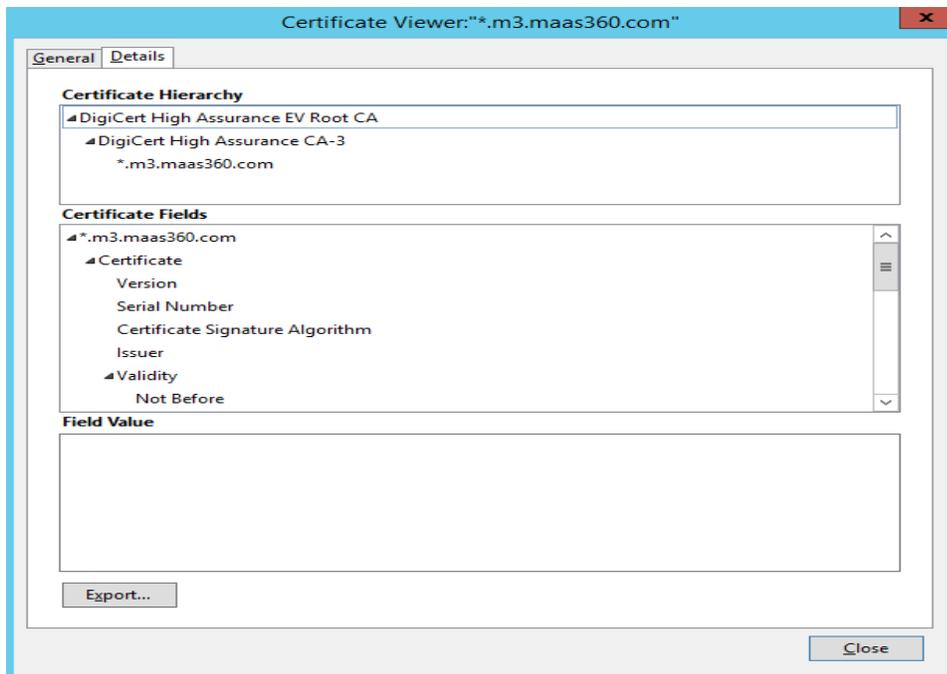
  e. **Save** the certificate to a file.

4. Import the certificate into the local certificate store in ISE.

  a. From the ISE Administration Portal, use the navigation path **Administration > System > Certificates > Certificate Store** to perform the import action.

  b. Grant ISE Access to the Fiberlink MaaS360 Application Programming Interface (API).

5. Create a Fiberlink MaaS360 administrator account with an API role.

  a. Log on to the MaaS360 with an Administrator Account.

  b. Navigate to **Setup > Administrators** and click **Add Administrator.**

  c. Enter the *new username* and a *corporate email address* and click **Next.**

  d. Enter *Roles* for the newly created administrator and click **Next.**

  e. Verify the setting and press **Save.**

6. Add MDM server to ISE.

  a. Use the MaaS360 MDM admin account created above.

  b. Configure Cisco ISE to integrate with the MaaS360: **Administration > MDM > External MDM Server,** then click **Add.**

  c. Fill out the required information using the account created in Step 5 and the *host name* or *IP address* provided by Fiberlink. A sample result is given below:

**Figure 7-5 Identity Services Engine**



  d. You can use the **Test Connection** button to test the connection between the Cisco ISE and the cloud MaaS360. A successful message will be displayed if the connection succeeds.

### 7.3.7 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.

   a. From the **Cisco Administration Portal,** navigate to **Policy > Authorization.**

   b. 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.

   a. From the **Cisco Administration** Portal, navigate to **Policy > Authorization.**

   b. 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.

   a. From the **Cisco Administration** Portal, navigate to **Policy > Authorization.**

   b. Create a third rule as

      Name:              *Default*

      Condition:         *If no matches*

      Permissions:       *DenyAccess*

# 8 Remote Office Network Configuration

## 8.1 Access Point: Cisco RV220W

This build uses the Cisco business class wireless APs. These business-class APs have additional functions beyond normal home-use APs. As an example, the APs allow enterprise connection security to enable certificate-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 by using the AP connection.

This section will describe how to configure the APs with IPs, media access control (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 10.2.1, MDM Setup

- Section 7.1, Cisco Identity Services Engine

### 8.1.1 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 wide area network (WAN) port of the RV220W.

2. Connect one end of a different Ethernet cable to one of the local area network (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 are 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.

### 8.1.2 Post-Setup Tasks

1. Use a PC to connect to a LAN port of the Cisco RV220W. If Dynamic Host Configuration Protocol (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 by using the default address https://<default IP address> 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 request that the user change the default password.

4. Verify that the IPv4 WAN setting is correct. It 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:

   a. 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:

      i. Download the firmware from https://software.cisco.com/download/ release.html?mdfid=283118607&softwareid=282487380&release=1.0.6.6&relin d=AVAILABLE&rellifecycle=&reltype=latest, and save it to a file.

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

      iii. Browse to the saved download file.

      iv. Press the Start Firmware Upgrade button and follow the instructions from the installer.

### 8.1.3    Cisco RV220 AP Setup for RADIUS Authentication

#### 8.1.3.1    *To configure LAN for IPv4*

1. Navigate to the path from the Configuration Utility Portal: **Networking > LAN (Local Network) > IPv4 LAN (Local Network)** to set up the IPv4 LAN.

2. 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 connected 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)

3. Configure static IP addresses and MAC addresses for known computers:

   a. 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.

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

#### 8.1.3.2    *Cisco RV220 AP Wireless Setup for IPv4 LAN*

1. Navigate to the path from the Configuration Utility Portal: **Wireless > Basic Setting.**

2. Enable one of the four default preset Service Set Identifiers (SSIDs) in the wireless Basic Setting table setting:

      a. Assign an SSID name.

      b. Disable SSID broadcast.

      c. After an SSID has been selected, enable security mode.

      d. Enable the MAC filter.

3. Edit Security Mode:

      a. Select a Wireless SSID to edit the security mode.

      b. Click Security Setting Mode.

      c. Select WPA2 Enterprise for Security and save, then select back.

4. Edit MAC filtering to block devices with MAC addresses that are not registered in the AP.

      a. Select a Wireless SSID to edit the security mode.

      b. Edit MAC Filtering and then select the Enable radio button. Click the radio button for Allow Only the Following MAC Addresses to Connect to the Wireless Network, then enter the MAC addresses in the boxes provided. Select SAVE. When saved, select Back. Follow the form to add the MAC addresses that you want the AP to control.

### 8.1.3.3   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.

1. Navigate to the path from the Configuration Utility Portal: **Security > RADIUS Server** to set up the AP to communicate with the authentication server. Select **Add** (press the button).

2. Fill out details in the RADIUS configuration pages, which normally include:

- Authentication Server IP address – the IP address of the authenticating RADIUS server (e.g., for HealthITOrg1, it is 10.10.101.101)

- Authentication Port – the RADIUS authentication server's port number used to send RADIUS traffic (e.g., 1812)

- Enter a preshared secret that will be used between the AP and the RADIUS authenticator server.

- Time-out – the time-out interval (in seconds) after which the RV220W re-authenticates with the RADIUS server

- Retries – the number of retries for the RV220W to reauthenticate 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 was set to the default setting for this installation. This blocked all inbound traffic except Internet Control Message Protocol 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 communicate with the RADIUS server. In this case, use the firewall network address as the authentication server IP address.

# 9 Virtual Private Network Using Intel Identity Protection Technology with PKI

The Data Center is secured using a firewall as detailed in Section 3.4. One of the techniques for securing access to the Data Center when using mobile devices in unsecured networks is the VPN. This document guides you and your organization through the process of performing enhanced secure VPN access by using the Cisco ASAv and the Intel IPT to provide VPN Services. The use of Intel IPT with PKI as the VPN authentication method offers the opportunity to simplify the authentication procedure by eliminating the password authentication requirement without sacrificing the strength of the security.

**Figure 9-1 Integrated VPN and IPT with PKI**
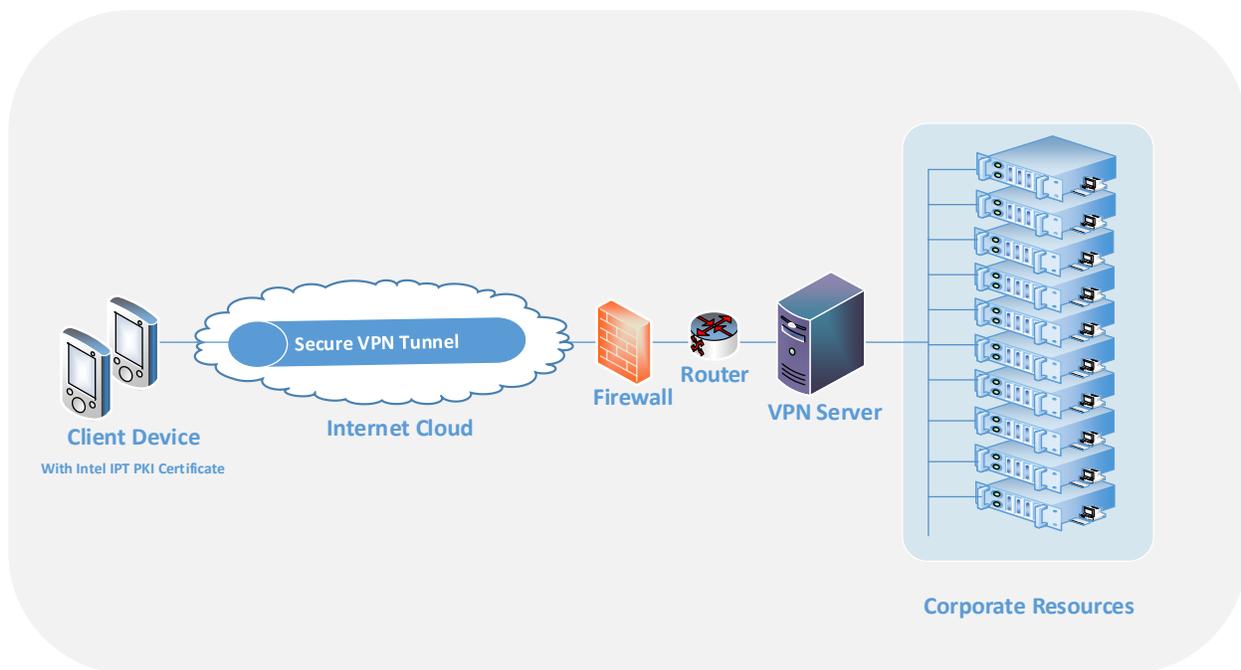


**Server software requirements**

- Microsoft Server 2012 with .NET Framework 3.5 or 4.0
- Enterprise PKI infrastructure using Microsoft Enterprise Certificate Authority
- Intel IPT server component

**Client requirements**

- Fourth-generation Intel Core vPro processor-based platform with one of the following: Intel chip set Q87 or QM87 along with the Management Engine (ME) 9.X firmware
- Microsoft Windows 7 or Windows 8 OS
- Appropriate version of Intel ME component installed

**Infrastructure requirements**

- VH capable of housing VMs

- ▪ VM with CPU: single CPU; 2.0 GHz or faster

- ▪ 2 GB RAM

- ▪ Cisco ASAv to provide VPN services

## 9.1 Microsoft Enterprise CA Server Installation

Install Microsoft Enterprise CA server on the Windows 2012 server with preconfigured IP address (e.g., 192.168.200.211).

1. Install Active Directory

   a. **Start > Administrative Tools > Server Manager**

   b. Click on **Roles > Add Role** to open the Add Roles Wizard.

   c. Click **NEXT** to select the Active Directory Domain Service.

   d. Click **Add** to add the required features if listed.

   e. Follow the Add Roles Wizard to complete adding roles with the default value.

   f. The Active Directory Domain Services Configuration Wizard begins after Add Roles Wizard is finished.

   g. Leave the **Use advanced mode** unchecked and click **NEXT** to proceed with the installation.

   h. The wizard will present some information related to operating system compatibility. Click **NEXT** to continue to choose a deployment configuration.

   i. Select a new domain in a new forest and click **NEXT.**

   j. Fill in a domain name for your organization (e.g., healthit.org).

   k. Continue to follow the wizard to complete the installation by using the default value.

   l. Restart the server to complete the Active Directory and DNS server installation.

2. Install Certificate Authority Server

   a. Click **Administrative Tools > Server Manager** to add new roles.

   b. Click **Add Roles** to open the installation wizard.

   c. Check the **Active Directory Certificate Services** from the role list window; then click **NEXT** to proceed.

   d. A new window with services related to Active Directory Certificate Services is shown. The Certification Authority Web Enrollment option is needed for requesting certificates through the web. Check the **Certification Authority** and the **Certification Authority Web Enrollment** check boxes. Click **NEXT** to continue.

   e. For Setup type, choose **Enterprise** and click **NEXT.**

   f. Choose **Root CA** as the CA type.

g. For Setup Private Key, use **Create a new private key** as the option.

h. Follow the wizard and use the default values to complete the installation for the CA Server. We recommend selecting **SHA256** for hash algorithm for the Cryptography option.

3. Configure CA Web Enrollment role service

To provide a set of web pages that allow interaction with the CA role service by using web browsers, use the following instruction guide for setting up the Certificate Enrollment Web Service on the same computer where enterprise CA is installed.

a. Create a domain user account to act as the service account.

   i. Sign in to the domain controller.

   ii. Open Active Directory Users and Computers by using an account that has permissions to add users to the domain.

   iii. In the console tree, locate the container where you want to create the user account. Right-click the container, click **New,** and then click **User.**

   iv. In the New Object —User text boxes, enter appropriate names for all the fields so that it is clear that you are creating a user account, and then click **NEXT.**

   v. Set a complex password for the account and confirm the password. Configure the password options to correspond to your organization's security policies regarding service accounts.

   vi. Click **NEXT,** and then click **Finished.**

b. Add the service account to the local IIS_IUSERS group.

   i. On the server that is hosting Certificate Enrollment Web Service, open Computer Management (**compmgmt.msc**).

   ii. In the Computer Management console tree, under System Tools, expand **Local User** and **Groups,** and then click **Groups.**

   iii. In the details pane, double-click **IIS_IUSRS.**

   iv. On the General tab, click **Add.**

   v. In the Select Users, Computers, Service Accounts, or Groups text box, type the user sign-in name for the account that you configured to be the service account.

   vi. Click **Check Names,** click **OK** twice, and then close Computer Management.

c. Configure HTTPS on the Default Web Site.

   i. On the server where IIS is installed, click on **Start > Administrator Tools > Internet Information Services (IIS) Manager** to open the IIS Manager.

   ii. From the Server and Sites nodes, select the **Default Web Site.**

   iii. On the Actions pane, click **Bindings,** and then in the **Site Bindings** click **Add.**

iv. In **Add Site Binding,** set Type to HTTPS and use the default port 443.

v. Set Secure Sockets Layer (SSL) certificate to the certificate that you issued to the server. You can confirm you have the correct certificate by clicking **View.** Click **OK.**

vi. Click **OK** to complete the site bindings and click **Close.**

## 9.2 Add the Intel IPT Cryptography Service Provider to Microsoft Enterprise CA Server

The Intel IPT Cryptography Service Provider (CSP) is the key to Microsoft Enterprise CA Server's ability to issue the Intel IPT PKI type of certificate to a client device with the IPT PKI client-side component installed. The following procedure describes how to install the Intel IPT component to the CA server.

1. Download the Intel IPT software

   a. An Intel Premier account is required. Log in to the Intel Premier site at https://www.intel.com/content/www/us/en/design/support/ips/training/access-and-login.html.

   b. Click downloads and select Intel PEAT SDK from the Product pull-down.

   c. Click the proper IPT component to download server-side and client-side installation files. (For example: Intel with PKI CA Components.zip for serverside and Intel IPT with PKI v2.0.0.0638.zip for client site.) The version of these components may change.

2. Add the Intel IPT CSP to the Microsoft Enterprise CA Server

   a. Locate the downloaded IPT with PKI server-side component and double-click it to start the installation.

   b. Follow the instructions and accept the license agreement to finish the installation.

   c. Check to make sure that Intel IPT with PKI Certificate Authority Components is in the list of installed programs.

3. Set Up Intel IPT Authentication Certificate Template

   a. Launch the Microsoft Management Console (**MMC**) on the Microsoft Enterprise CA Server.

   b. In the MMC window, select **File > Add/Remove Snap-in…**

   c. Select **Certificate Template** and click **Add** to add the Certificate Templates to the selected snap-ins window.

   d. Also select **Certificate Authority** to add it to the snap-ins window.

   e. Click **Finish** to complete the addition of the Certificate Authority.

   f. In the console Template Display Name list, select the **user** template and right-click it to show a drop-down list.

   g. Select **Duplicate Template** to open a property window for the new template.

h.  Fill in the proper display name (e.g., IPT PKI User) in the General tab.

i.  Uncheck the **Publish certificate in Active Directory** check box.

j.  In the Cryptographic tab, select the **Intel IPT Cryptographic Provider** as the CSP for this certificate template as shown below.

**Figure 9-2 Properties of New Template**
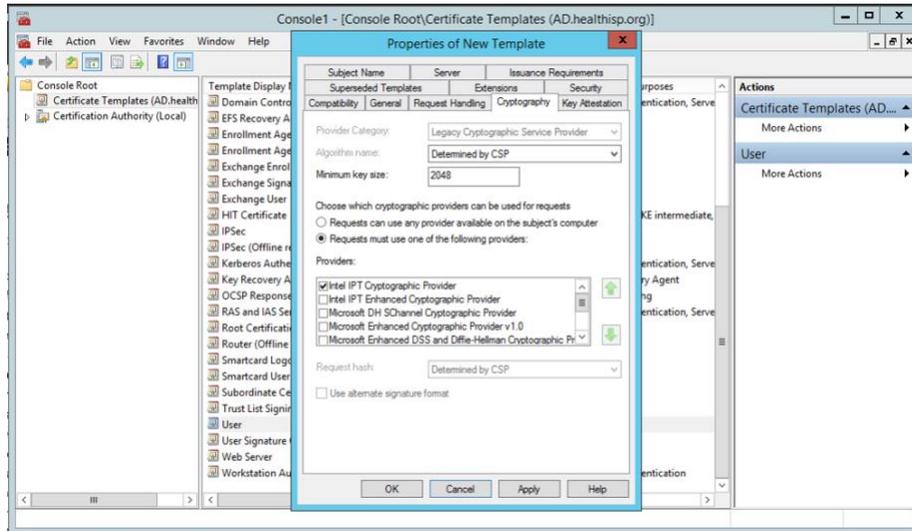


k.  In Request handling, the setting is shown in the figure below.

**Figure 9-3 Properties of New Template – Requesting Handling**
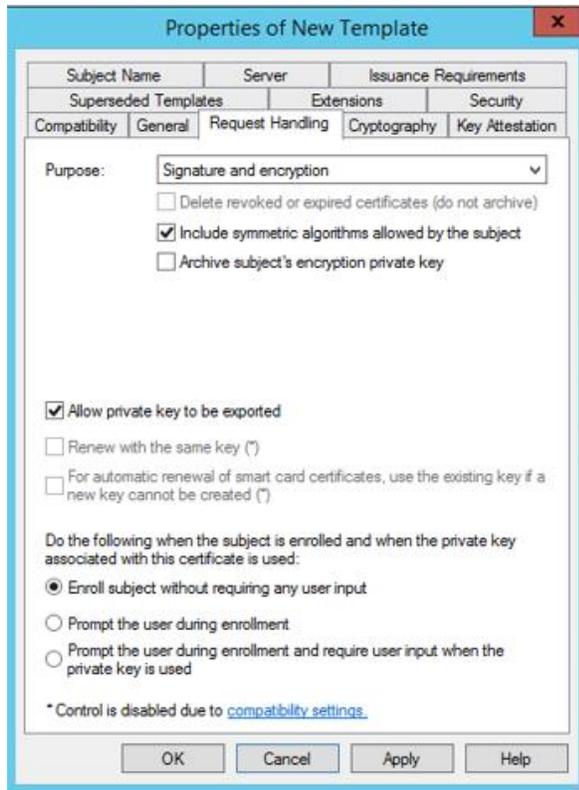
l.  Click **OK** to generate a new template as shown below.

**Figure 9-4 Console 1**
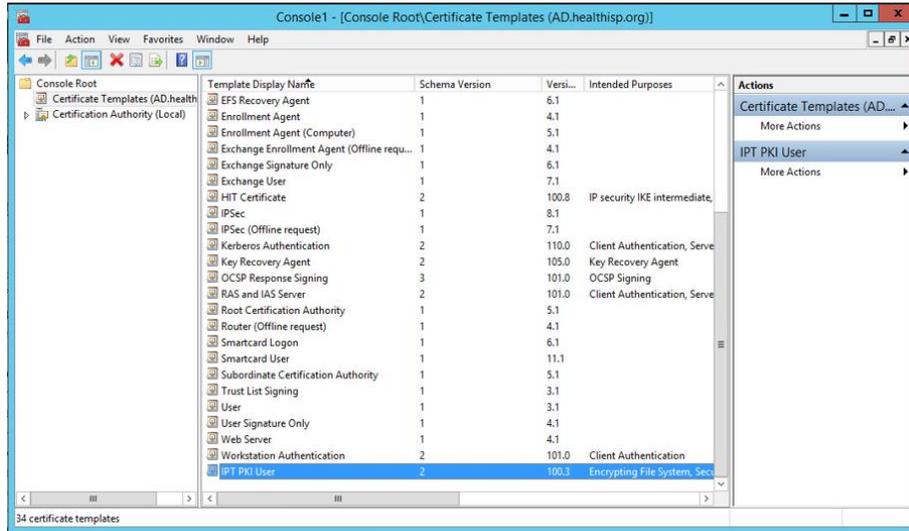


4.  Publish the newly created template.

    a.  In Administrative Tools, click **Certification Authority** to open the certificate console.

    b.  In the console tree, select the **Certificate Templates** container.

    c.  Right-click **Certificate Templates,** and then click **New,** then **Certificate Template to Issue.**

    d.  In the Enable Certificate Templates dialogue box, select the newly created IPT certificate template, and then click **OK.**

    e.  The newly selected certificate template will appear in the details pane.

## 9.3    Set Up Client Device for VPN by Using Intel Identity Protection Technology with PKI

In this build, the Dell Venue 10 with Intel Core i5 processor and 64-bit Windows 8 Pro OS tablet is used as the client device.

1.  Add the Intel Identity Protection Technology with PKI on the client

    a.  Copy the downloaded Intel IPT client component installation package to a client device.

    b.  Double-click the package, and follow the instructions to install the IPT component.

    c.  Check that the Intel IPT with PKI component is installed.

    d.  Restart the client computer.

2.  Install Intel IPT PKI certificate for client

    a.  Install Root CA certificate to the client machine.

        i.  From the Root CA server, click **Start,** type "MMC," and press enter.

ii. Select **File > Add/Remove Snap-In.**

iii. Select Certificate from the available snap-ins and click **Add.**

iv. Select managed certificate for Computer account.

v. When you see Certificate (Local Computer) on the right side, click **OK.**

vi. Select **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates** to see the listed certificate.

vii. Locate the certificate issued by the Certificate Authority server generated from the previous section in the How-To guide.

viii. Right-click the certificate and select **All Tasks > Export.**

ix. Follow the Certificate Export Wizard and select **Do Not Export the Private Key** and DET encoded binary x.509 (*.CER*) for the export file format.

x. Save the export file with the extension *.cer* to a specified location.

xi. Transfer the certificate file from the server machine to the client machine by using copy, email attachment, or other methods.

xii. From the client machine, double-clicking the certificate file will open a certificate window.

xiii. Make sure this is the certificate for the root CA you want to install, and click the **Install Certificate** button.

xiv. Follow the instructions and place the certificates in the Trusted Root Certificate Authorities.

xv. Accept the warning, if there is any, and click **Finish** to complete the Root Certificate installation on the client device.

b. Request and install Intel IPT PKI user certificate for client device.

i. Create a user account for the client in the Active Directory.

ii. Connect the client device to a network that allows access to the CA certificate Web Request web page.

iii. Use Internet Explorer to request a basic certificate by connecting to https://<servername>/certsrv, where <servername> is the host name of the computer running the CA Web Enrollment role service.

iv. Accept the server certificate by clicking **Continue to this website.**

v. Log in to the web page by using the user account created for this client if requested.

vi. From the Microsoft Active Directory Certificate Services Welcome page, select the **Request a Certificate** link.

vii. Click **Advanced Certificate Request** link to submit a request.

      viii.    In the Advanced Certificate Request page, select the **Create and submit a certificate to this CA** link.

      ix.    Accept the web access confirmation. An advanced certificate request page is shown.

      x.    Select the template corresponding to the Intel IPT PKI template created as shown in this guide.

          1)    Fill in the client user information if required.

      xi.    Make sure the CSP is pointed to the Intel IPT Cryptographic Provider.

      xii.    Keep other data fields with the prefilled default values unless you would like to change them according to your needs.

      xiii.    Click **submit** to submit the request.

      xiv.    Then either:

          1)    If you see the Certificate Pending page, the CA administrator will have to approve the request before you can retrieve and install the certificate.

              **Or**

          2)    If you see the Certificate Issued page, click Install to install this certificate. Make sure the certificate is installed successfully.

3. Install Cisco AnyConnect VPN Client for Client Device

    a.    Download AnyConnect VPN package from Cisco's website. The Intel IPT with PKI is expected to work with any 2.5.x or 3.0.x version.

    b.    Double-click the downloaded package, and follow the instructions to install AnyConnect to the client device with Intel IPT component installed.

## 9.4   Cisco ASAv VPN Server Configuration

1. Install ASAv into vCenter

    a.    Acquire the ASAv Open Virtual Appliance (OVA) file from Cisco.com.

    b.    Follow guidance from Cisco and your VM vendor to deploy the OVA.

2. Basic setup for Cisco ASAv VPN Post-Installation Tasks

    a.    Connect to the Cisco ASAv by using Adaptive Security Device Manager (ASDM) via the management interface specified during deployment.

    b.    Use the VPN Connection Setup Wizard. From the menu bar select **Wizards > VPN Wizards > AnyConnect VPN Wizard…,** then click the **Next** button to start the configuration.

    c.    Specify the Connection Profile Name, and check that the outside interface is selected in the VPN Access Interface drop-down. Click **Next** to continue to the next screen.

d.  Make sure that SSL and IPsec are both selected, and the Device Certificate loaded in Section 10.1.1.3 is selected. Click **Next** to continue to the next screen.

e.  For mobile access, no client images are needed. Click **Next** to continue to the next screen.

f.  Specify the AAA servers that will be used to authenticate users accessing the VPN.

g.  Click the **New…** button to create a new AAA Server Group. Fill out the required parameters as indicated in the form:

    i.  Server IP address

    ii.  RADIUS secret key

h.  Click **Next** to continue to the next screen.

i.  Create an Address Pool for AnyConnect clients.

j.  Click the **New…** button.

k.  Fill in the form with the required parameters: Specify the HealthISP's DNS server on the next screen.

l.  Continue through the wizard and select **finish.**

3.  VPN Server Certificate Management Configuration

    For the VPN to function correctly, a root certificate from the CA will need to be installed.

    a.  Connect to the Cisco ASAv by using ASDM via the management interface specified during installation.

    b.  Click Configuration on the toolbar, and select Device Management from the lower left-hand pane.

    c.  In the **Device Management** pane, expand the **Certificate Management** tree element, and select the **CA Certificates** element.

**Figure 9-5 Device Management**
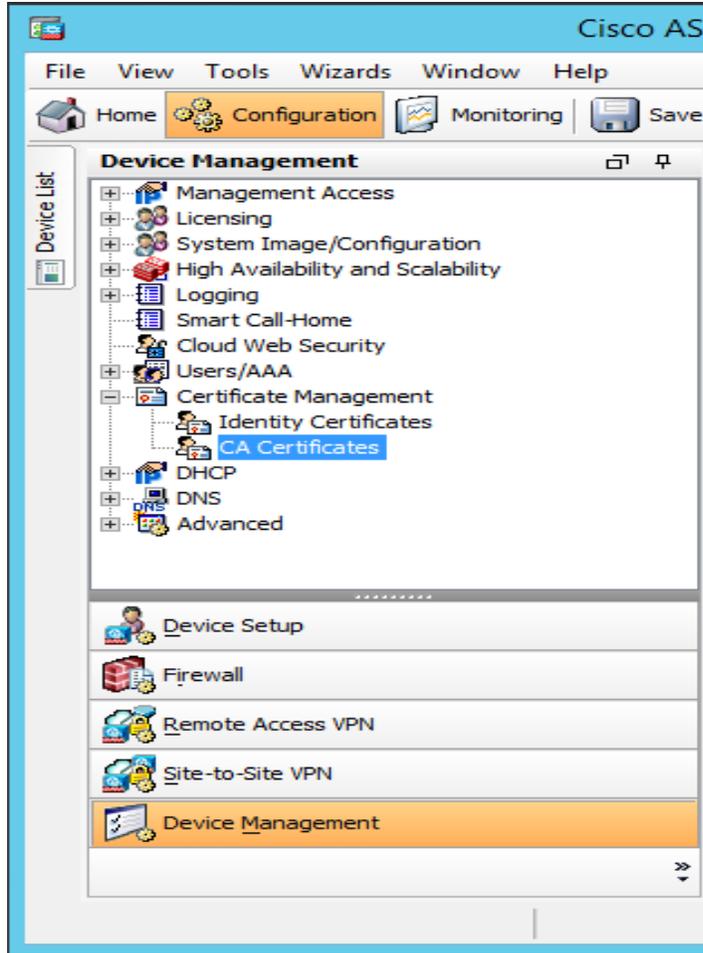


d. Click on the **Add** button to install the certificate. The Install Certificate dialogue box will appear, allowing you to install the CA's signing certificate.

**Figure 9-6 Install Certificate**
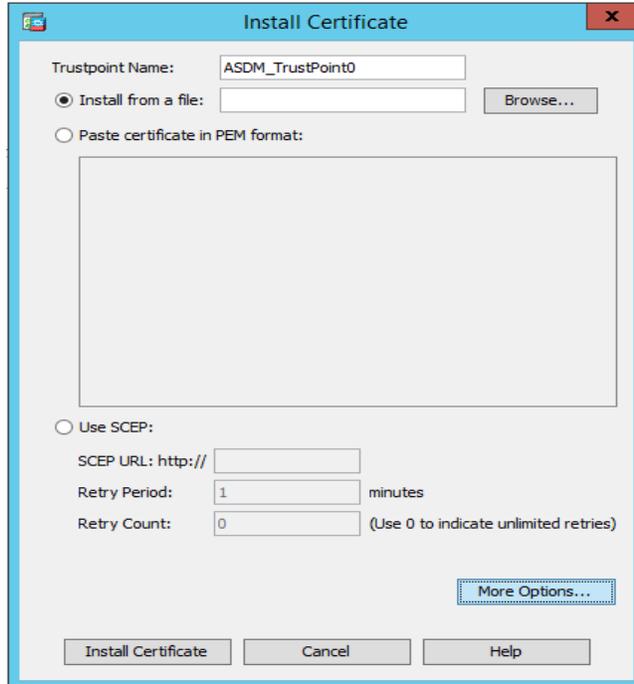


e. To secure connections with the VPN server itself, a signed certificate and private key should be installed.

    i. Generate a private/public key-pair and certificate for the VPN server. Note: If the key is larger than 2,048 bits, it will not be usable to secure the VPN connections. In this case, you should generate a second key-pair and certificate for the VPN connections, using a 2,048-bit key length.

    ii. Use the CA's signing certificate to sign the VPN server's certificate and package by using both the signed certificate and private key in a PKCS12 format file.

**Figure 9-7 Add Identity Certificate**
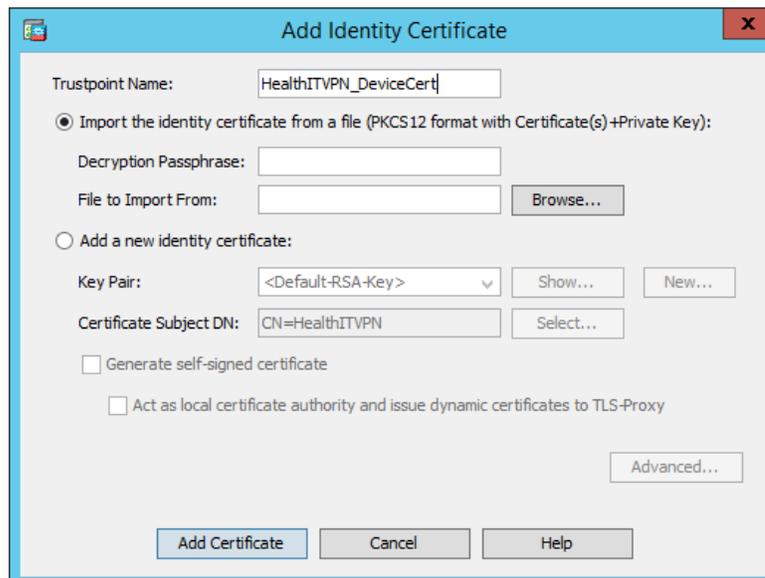
4. Configure ASAv for No-Password VPN Authentication by using Intel IPT with PKI

   a. Connect to the Cisco ASAv using ASDM via the management interface specified during installation.

   b. From the appliance's home page, select the **Configuration** tab.

   c. From the Device setup, click the **Remote Access VPN** from the left column near the bottom to access the VPN setting.

   d. Under the **Network (Client) Access** group in the left column, click the **AnyConnect Profile** to show the current VPN access configuration for the Cisco VPN AnyConnect client software.

   e. Click **Edit** to edit the profile to change the Authentication Method to **Certificate,** and click **OK.**

   f. Click **Apply** on the AnyConnect Connection Profiles page.

   g. Click **Save** to save the changes.

## 9.5 Test and Confirmation

1. From the client device, launch the Cisco AnyConnect Secure VPN Client software.

2. Enter the VPN address or preconfigured VPN host name (e.g., HealthITVPN [IPsec] IPv4).

3. It may display a security warning—Untrusted Server Certificate—if a self-signed CA root certificate is used. Click Connect Anyway to accept the warning, as shown in the following screenshot.

**Figure 9-8 Untrusted Server Certificate**
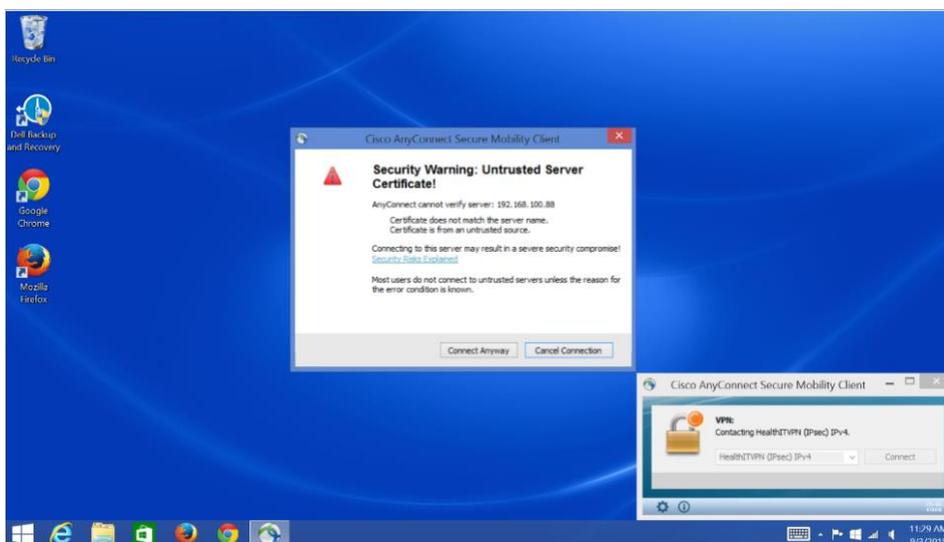


4. If there are many VPN profiles available, select the one configured for no-password Intel IPT with PKI (e.g., Certificate). Then click connect.

**Figure 9-9 VPN Profile**
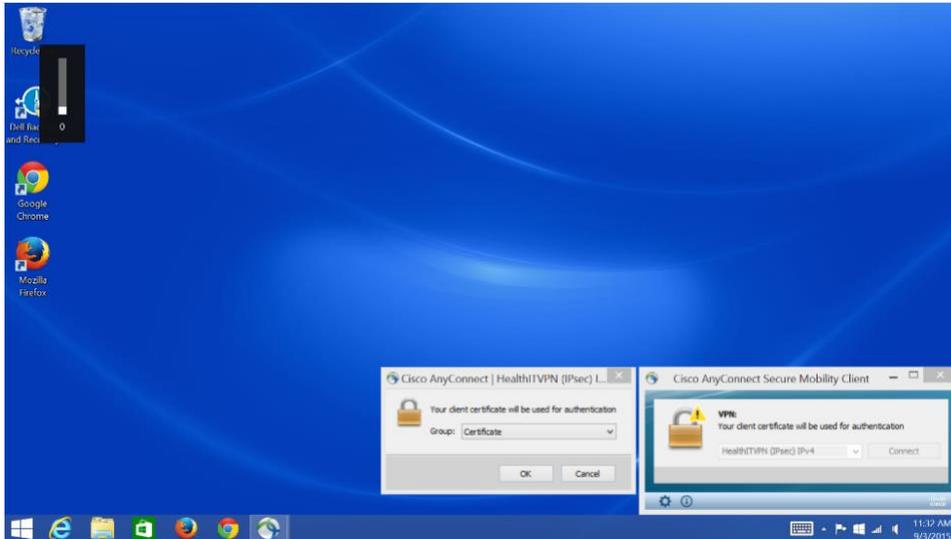


5. The AnyConnect software should not request a password and should show connected after the successful authentication process that used the Intel IPT with PKI certificate.

6. The AnyConnect VPN window will show Connected to HealthITVPN (IPsec) IPv4 as depicted in the following screenshot.

**Figure 9-10 AnyConnect VPN Window**
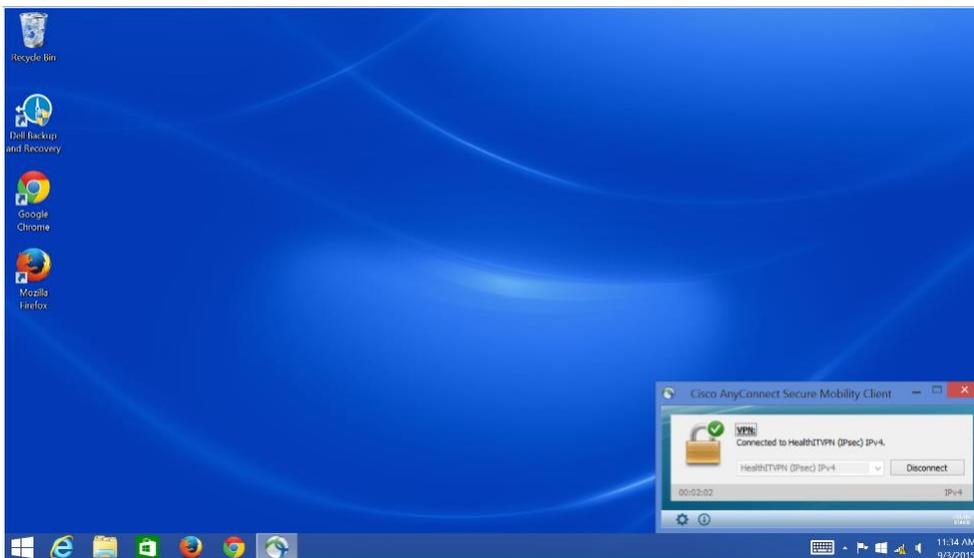


Now you can access the protected resources behind the firewall according to the access policy assigned for the client.

# 10 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. Authorized healthcare professionals and patients use mobile devices to add, change, read, or remove PHI.

**Figure 10-1 Integrated Host-Based Security System**
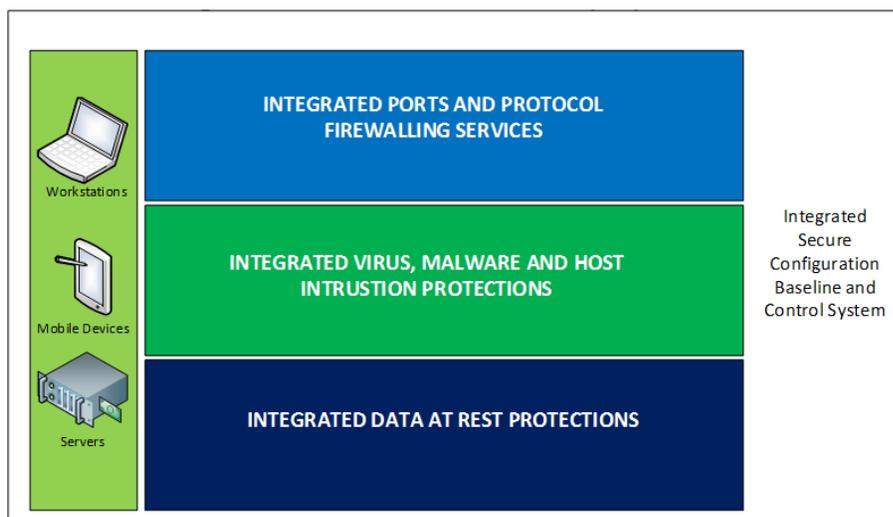


This section will show you how to build and configure hosts and mobile devices securely.

## 10.1 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 PHI from anywhere. These devices must be secured so that they protect both 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 connect and securely protect PHI. This section will also show you how to set up 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 device: 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 8.1, Access Point: Cisco RV220W
- Section 6.1, Fedora PKI Manager
- Section 10.2.1, MDM Setup
- Section 7.1, Cisco Identity Services Engine

### 10.1.1 Android Mobile Device Setup

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

### 10.1.1.1 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/6088915?hl=en). Follow these steps to perform the factory reset:

    a. On your mobile device, open the Settings menu.

    b. Under Personal, tap on Backup & Reset.

    c. Under Personal data, tap on Factory Data Reset.

    d. After you press 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.

    e. Start 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 in the MDM. To set the passcode, follow these steps, as described in https://support.google.com/nexus/answer/2819522?hl=en:

    a. On your mobile device, open the Settings menu.

    b. Under Personal, touch Security.

    c. Under Screen Security, navigate to Screen Lock.

    d. Select the Password option.

    e. Follow the instructions on the screen to complete the passcode setup, 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 be encrypted before enrolling it in MDM. Perform encryption using these steps, as described in https://support.google.com/nexus/answer/2844831?vid=1-635809672234145775-862949942:

    a. Plug in the device to a power cable and allow the battery to charge. Keep the power cable connected during the encryption process.

    b. On your mobile device, open the Settings menu.

    c. Under Personal, touch Security.

    d. Scroll to the Encrypt Tablet option.

    e. Press the Encrypt Tablet button.

    f. The device will reboot several times during the encryption process.

    g. 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 by using these steps:

   a. On your mobile device, open the Settings menu.

   b. Go to Wireless & Networks.

   c. If Wi-Fi is unchecked, tap the empty box.

   d. Since the SSID is not broadcast, use Add New Action to open a new Wi-Fi connection form.

   e. Type in all the details, including the SSID name; the security protocol, e.g., WPA2; and the correct password to join the Wi-Fi network.

**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:

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

   **Figure 10-2 MaaS360 Device Enrollment Request**

b. Click the Device Enrollment URL to start the enrollment process, following these steps:

    i. Download and install the MaaS360 MDM for Android application to the device.

    ii. Click to open the MaaS360 MDM for Android application.
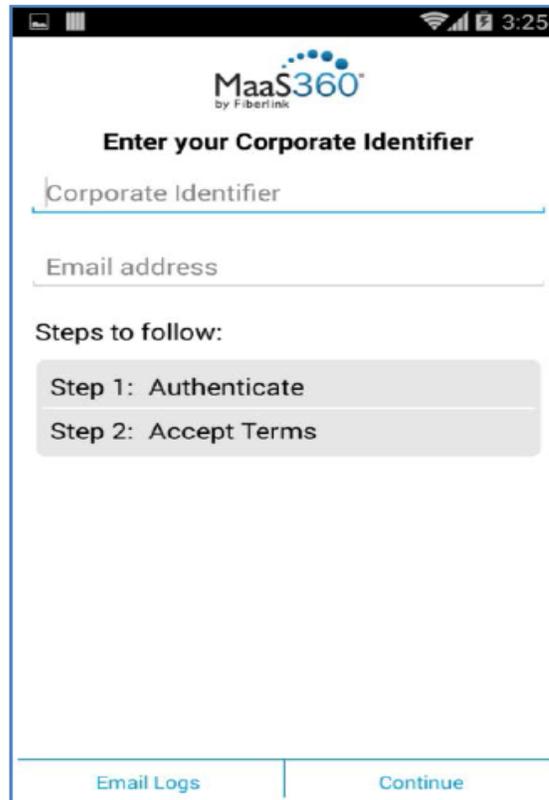


c. Fill in the Corporate Identifier and Email address as shown in the device enrollment request email.

d. Press Continue to open the agreement page, and select the check box and press to continue.

e. Press Activate to enroll the device in MDM.

f. Install all the required apps.

g. Apply policy and rule – Make sure the correct version of policy and rule is applied to the device.

h. Verify compliance – Verify that the device is compliant with all the security requirements. If not, from the Uncompliant list, click the uncompliant item to correct the problem.

### 10.1.1.2 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 8.1, Access Point: Cisco RV220W, for adding a device MAC address for MAC filtering service.

### 10.1.1.3   Install CA Trusted Certificates

Import certificates on Android devices – Most Android devices will import certificates from an internal or external Secure Digital (SD) card. Android OS has Credential Storage under Settings/Security. Some old Android versions cannot recognize certain certificate formats, so additional steps are required to convert the certificate to the format that the device recognizes. For some newer versions of Android devices, directly importing and installing the certificate by using supported 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.

1. From your device, launch a browser.

2. Type the URL *https://<PKI hostname>:<PKI secure EE port>* into the browser to list the CA Certificate Profiles:

**Figure 10-3 Certificate System – Enrollment**
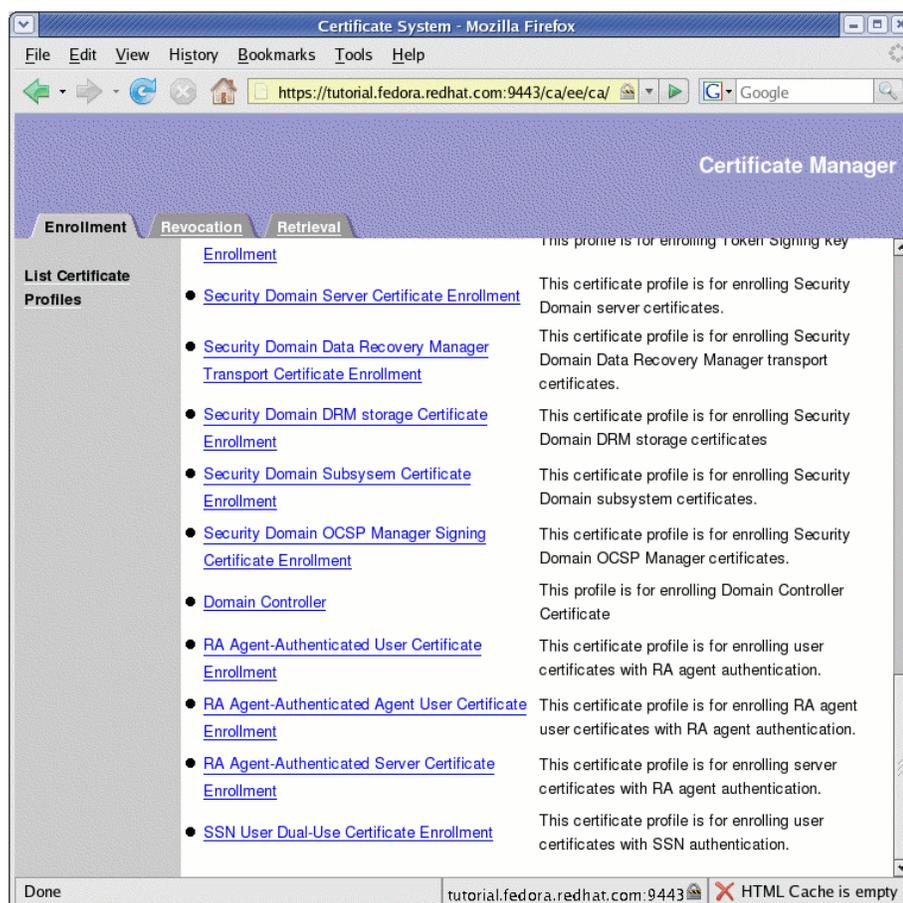


3. Select an Enrollment link and fill in the device identity in the Common Name field as shown on the page below:

**Figure 10-4 Certificate System – Certificate Profile**
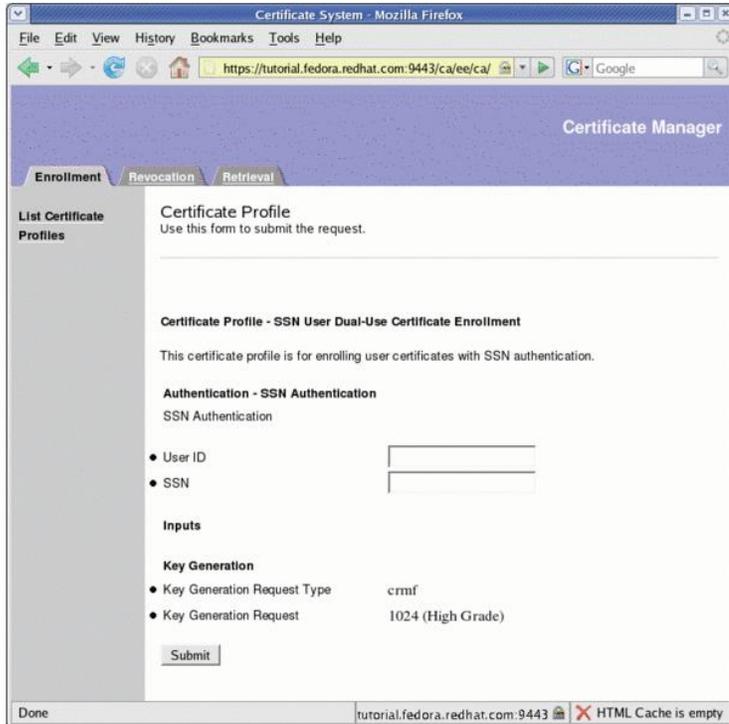
4. Press Submit to request the device certificate.

5. If successful, you will receive a request number. Record this number for later use.

6. The CA Authority Administrator will use the Certificate system to approve or disapprove the request. (Refer to Section 7 for details.)

7. Once approved, use the same interface as shown to select the Retrieval tab.

8. Enter the request number to retrieve the certificate. If you succeed, the certificate will be displayed on the screen with the Import button for importing the certificate to the device.

9. If you succeed, 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 to an external SD card and install the certificate from there.

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

1. Go to **Settings** on your Android device.

2. Select **Security.**

3. 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, it is possible 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 by 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 the 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. The CA admin will verify the request and approve the certificate.

11. Retrieve the approved certificate by 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.

### *10.1.1.4   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 set up 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 Root CA`

   - **User certificate:** `Name of your device certificate`

3. Click **Save.** You should be connected to the network by using EAP-TLS authentication.

4. In this build, we used a protected website, <https://www.examplehealthisp.com>, to verify whether or not the EAP-TLS authentication was successful.

## 10.1.2   Apple Mobile Devices Setup

It is assumed that the MaaS360 has been configured and that 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 and the password for the device.

### *10.1.2.1   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](https://support.apple.com/en-us/HT203977)). Follow these steps to perform the factory reset:

   a. On your Apple device, open the **Settings** menu.

   b. Under **General,** tap **Reset.**

   c. Under **Reset,** tap **Erase All Content and Settings.**

   d. You will have to confirm your selection to set your device to the factory default.

   e. After you confirm your choice, the device will begin the reset process.

   f. Restart your device and follow the onscreen instructions to set up the device for a new owner.

2. Passcode protection and device encryption – Passcode protection is required for iOS devices to be encrypted and to enroll in the MDM. Setting a passcode in the iOS device will also enable encryption on the device. To set the passcode, follow these steps:

     a. On your mobile device, open the **Settings** menu.

     b. Under **Settings,** go to **Passcode Lock** and press **Turn Passcode On.**

     c. Under **Screen Security,** navigate to **Screen Lock.**

     d. When you turn on the passcode, you also enable encryption on your iOS device.

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 server to request and import device certificates. This Wi-Fi is protected by using the WPA2 security protocol. This Wi-Fi SSID is not broadcast. Configure the device to connect to Wi-Fi by using these steps:

     a. On your mobile device, open the **Settings** menu.

     b. Tap **Wi-Fi.**

     c. When **Wi-Fi** is on, the device will automatically search for available **Wi-Fi** networks.

     d. Join the hidden **Wi-Fi** network with no broadcast SSID: Under the **Choose a Network** section, tap **Other.**

     e. In **Name,** put the exact **Wi-Fi** network SSID you want to connect to.

     f. Tap **Security** and choose the type of network encryption used. (For the NCCoE build, WPA2 was used.)

     g. Return to the primary connection screen.

     h. Enter the Wi-Fi SSID password and tap **Join** to connect to the hidden wireless network.

**MDM enrollment** – We assume that your organization has already purchased a license to MaaS360 and that you have created a user account with privileges to enroll devices. We also assume that the device enrollment request has been completed and that the enrollment notification has been received via email.

1. For enrollment application

     a. Enroll your iOS device by 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.

**Figure 10-5 MaaS360 Device Enrollment Request**



b.  Clicking the **Device Enrollment URL** will start the enrollment process.

c.  The enrollment steps are to Authenticate, Accept Terms, Download & Install Profile, and Install MaaS360 for iOS App to the device.

d.  Click Continue to proceed, and follow the instructions to provide necessary authentication information from the enrollment email, such as passcode and Corporation Identifier.

e.  Accept terms. You must agree to the Fiberlink end user agreement to enroll your device.

f.  The device will start to install the MDM Profile. Press Continue. The profile will enable the MaaS360 administrator to manage the device by using MaaS360. Click Install to install the profile, and accept any prompts for profile installation to continue with the enrollment.

g.  After the profile is installed, you will be prompted to install the required MaaS360 application from the **Apple App Store.**

h.  Return to the home screen and locate the **MaaS360** application. Tap the **MaaS360** icon to install the Fiberlink MDM for iOS application.

i.  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.

j.  Your device is now enrolled in MaaS360.

k.   Apply policy and rule – From the home screen, locate the **MaaS360** icon. Tap 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.

l.   Verify compliance – Verify that the device is compliant with all the security requirements. If not, from the Uncompliant list, click the uncompliant item to correct the problem.

### 10.1.2.2   Register Device in AP for MAC Address Filtering

Add the 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 8.1, Access Point: Cisco RV220W for adding a device MAC address for MAC filtering service.

### 10.1.2.3   Install CA Trusted Certificates

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

**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, it is possible 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 by 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 the process is successful, a request number will be displayed for future retrieval of the approved certificate.

10. The CA administrator will verify the request and approve the certificate.

11. Retrieve the approved certificate by 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 blob 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 iOS device by secure email.

16. Install the certificate as shown in Option 2.

### 10.1.2.4   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 set up 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 now be connected to the network by using EAP-TLS authentication.

## 10.2   MaaS360

The MDM selected for this build is based on the MaaS360 product. Maas360 is a cloud-based solution that is responsible for managing policies 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 browser installed
- Windows Phone Company Hub certificate

**You will also need the following parts of this guide:**

- Section 8.1, Access Point: Cisco RV220W
- Section 6.1, Fedora PKI Manager
- Section 7.1, Cisco Identity Services Engine

## 10.2.1   MDM Setup

### 10.2.1.1   Enable Mobile Device Management Service

We assume 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/). We also assume that the required Windows Phone Company Hub and the Apple Push Notification Service (APNS) certificates have been acquired. For detailed information on how to acquire these required certificates, please refer to https://www.ibm.com/support/knowledgecenter/en/SS8H2S/com.ibm.mc.doc/pag_source/tasks/pag_getstart_renew_apns_cert.htm for Apple MDM certificate and the document https://www.ibm.com/support/knowledgecenter/en/SS8H2S/com.ibm.mc.doc/winphone_enrollment_source/tasks/winphone_enrollment_mdm_enroll.htm for MaaS360 Windows Phone 8 Company Hub Certificate.

1. Add the Apple MDM Certificate for managing Apple devices.

    a. Log on to **MaaS360** dashboard by using https://login.maas360.com.

    b. Navigate to **Setup > Services,** click **Mobile Device Management.**

    c. Click **Apple MDM Certificate** and use the browser to load the certificate file.

2. Add Windows Phone Company Hub certificate for managing Windows Phones.

    a. Log on to **MaaS360** dashboard using https://login.maas360.com.

    b. Navigate to **Setup > Services,** click **Mobile Device Management.**

    c. Expand the Windows Phone Company Hub certificate by pressing the "+" symbol.

    d. Use the browser to load and install the certificate to the MDM.

### 10.2.1.2   Enable Security Policies for Mobile Devices

1. Create a new policy for a type of device.

a. Log on to the **MaaS360** dashboard by using https://login.maas360.com.

b. Navigate to **Security > Polices,** click **Add Policy.**

c. Add a Name (e.g., Lab_Only_ISO).

d. Add Description.

e. Select a Type from the drop-down list (e.g., iOS MDM).

f. Use the **Start From** drop-down list to copy an existing policy for this new policy.

g. Click Continue to create a new policy for the type of device.

2. Edit and refine the created policies.

a. Log on to **MaaS360** dashboard by using https://login.maas360.com.

b. Navigate to **Security > Policies.**

c. From the **Policy list,** click **View** to view a selected policy.

d. Review each item in the policy to make sure it is set per your security policy and business requirements.

e. If the policy settings do not meet your security requirements, click the Edit button to enter the edit mode.

f. Change the values to your desired values.

g. Click **Save** to save the changes, or click **Save and Publish** to save and publish the new policy.

h. Enter the password and press **Continue.**

i. 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.

### 10.2.1.3   Enable Security Compliance Rule for Mobile Devices

1. Create a new rule set.

a. Log on to **MaaS360** dashboard by using https://login.maas360.com.

b. Navigate to **Security > Compliance Rules** and click **Add Rule Set.**

c. Add a Name (e.g., HIT-RULE).

d. Copy an existing rule set for the new rule from the Copy From drop-down list.

e. Click Continue to create a new rule.

2. Edit and refine the newly created rule.

a. Log on to the **MaaS360** dashboard by using https://login.maas360.com/.

b. Navigate to **Security > Compliance Rules.**

c. Click Edit for the selected rule you want to review and edit.

d. From the **Basic Settings,** under **Select Applicable Platforms,** check the check box next to an OS's name to Enable the Real-Time Compliance for OSs.

e. In the Event Notification Recipients, fill in the emails you want to be notified in case of noncompliance.

f. Use the navigation tree to view and set other rules per your security and operational requirements.

g. Click Save to save the newly set rules.

### 10.2.1.4 Add Applications to Be Distributed to Mobile Devices

1. Add App to App Catalog.

a. Log on to the **MaaS360** dashboard by using https://login.maas360.com/.

b. Navigate to **APPS > Catalog and** click **Add** to select **Apps** from different app stores.

c. In the pop-up page, type a keyword for the application in the search box to list the available applications.

d. Select the application you want and click Add button to add the application to the category.

2. Add Application to Bundles for Distribution.

a. Log on to the **MaaS360** dashboard by using https://login.maas360.com/.

b. Navigate to **APPS > Bundles** and click **Add App Bundle** to open the **App Bundle** window.

c. In the pop-up 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 applications.

d. Click Add button to add the App Bundle.

e. From the **App Bundle list,** click **Distribute** button to set the distribution Target.

### 10.2.1.5 Add Device Group to Manage Mobile Devices

1. Add Device Group.

a. Log on to the **MaaS360** dashboard by using https://login.maas360.com/.

b. Navigate to **USERS > Groups and** click **Add Device Group** to create a new Group.

c. Enter search criteria and select Search.

d. Select **Create Device Group.**

e. Enter a group name and description.

      f.    From the **Device Group Details** window, specify the group Type.

      g.    Click **Save** to save the setting.

2. Configure Group.

      a.    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.

      b.    Detailed settings for group properties can be referenced in the MDM manual: http://compliance.fiberlink.com/download/MaaS360_MDM_User_Guide.pdf.

3. Device Enrollment

      a.    iOS MDM Enrollment is described in Section 10.1.2.

      b.    Android MDM Enrollment is described in Section 10.1.1.

## 10.3  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 remote 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.

### 10.3.1  Symantec Endpoint Protection Suite

The Symantec Endpoint Protection server provides the following options:

- Local Host 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 manages only 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 8 GB
- Disk space        Minimum 150 GB

**You will also need the following parts of this guide:**

- Section 2.1, 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.

# 11 Governance, Risk, and Compliance

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.

## 11.1 RSA Archer GRC

### 11.1.1 System Requirements

This build requires the user to install a single-host RSA Archer GRC platform node on a VMware VM 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 instructions for other options.

### 11.1.2 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 ran under a single server. Below are the pre-installation tasks that we performed prior to the RSA Archer installation:

- Operating System: Windows Server 2012R2 Enterprise
  - Refer to Section 2.1, 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 that database owners have sufficient privileges and correct user mappings.

**Table 11-1 Configuration Settings**

| 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 |

| Setting | Value |
|---|---|
| Locale set | English (United States) |
| Database server time zone | EST |
| Platform language | English |
| Create both the instance and configuration databases within a single SQL Server instance. For migration, create only the configuration database | Database names:<br> *grc-content*<br> *grc-config* |
| User Account set to Database Owner role | *grc-content-user*<br>*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 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.

First install IIS and then install the *.NET* Framework.

Table 11-2 summarizes the required IIS components and *.NET* Framework features followed by the screenshots.

**Table 11-2 IIS Components and .NET Features**

| Required Option | Value |
|---|---|
| IIS | |
| Common HTTP Features | Default Document<br>Directory Browsing<br>HTTP Errors<br>Static Content |
| Health and Diagnostics | HTTP Logging |
| Application Development | .NET Extensibility 4.5<br>ASP .NET 4.5<br>ISAPI Extensions<br>ISAPI Filters |
| Security | Request Filtering |

| Required Option | Value |
|---|---|
| Management Tools | IIS Management Console |
| **.NET Framework** | |
| .NET Framework 4.5 Features | .NET Framework 4.5<br>ASP.NET 4.5 |
| WCF Services | HTTP Activation<br>TCP Port Sharing |

**Figure 11-1 Web Server (IIS) Components Selection Screenshot**
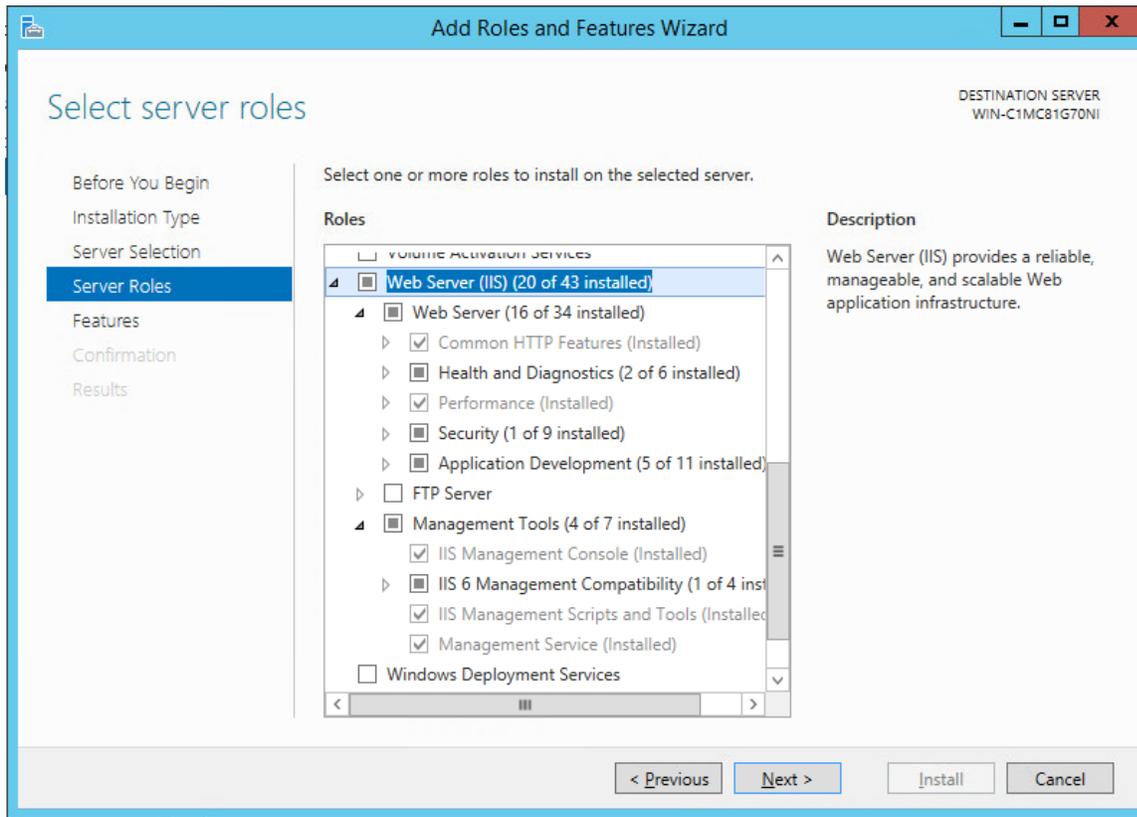
**Figure 11-2 .NET Framework 4.5 Features Selection**
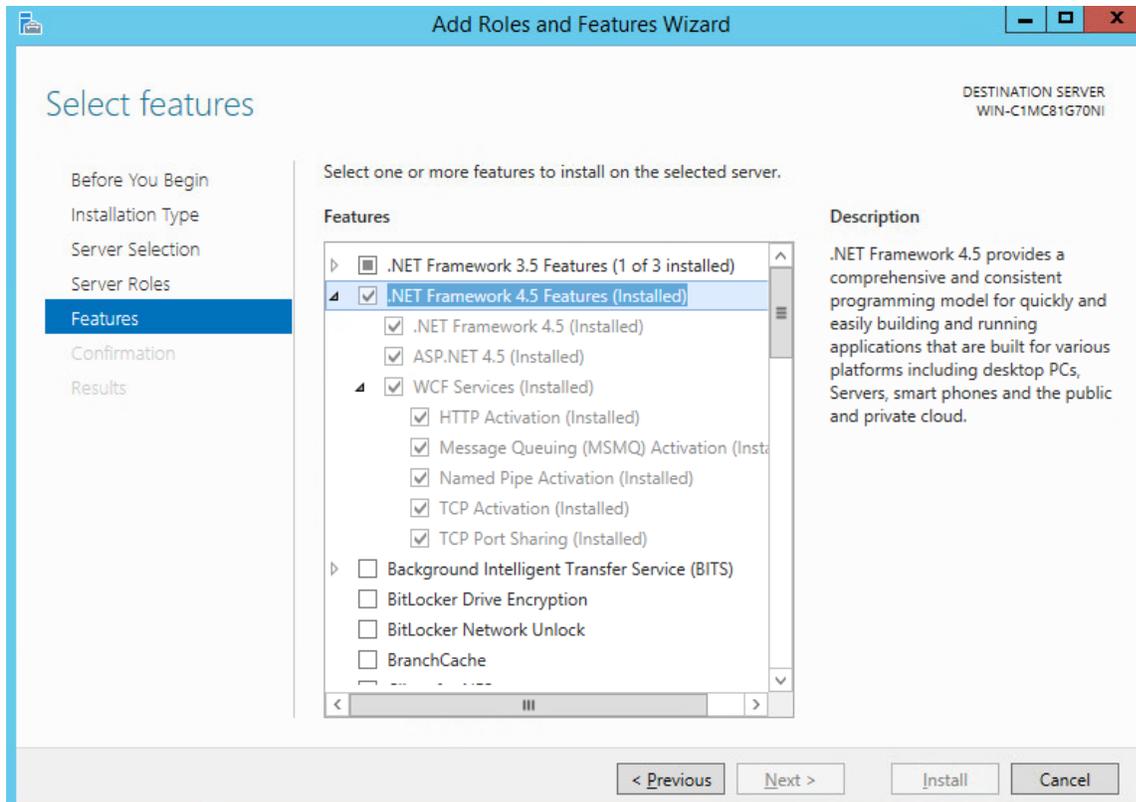
**Microsoft Office 2013 Filter Pack**

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.

## 11.1.3   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.

   a. Open installation folder, right-click on *ArcherInstall.exe.*

   b. Select **Run as Administrator.**

   c. Click **OK** to Run the Installer.

d. Follow the prompts from the installer for each step, set the value, and click Next.

e. Select all components **(Web Application, Services, Instance Database)** for installation, then click **Next**.

f. Specify the X.509 Certification by selecting it from the checklist (create new cert or use existing cert). We created a new cert.

g. 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)

h. 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.

i. Set the Configuration of the Service Credentials.

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

j. 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\.*

k. Set the Log File Path to *C:\ArcherFiles\Logging.*

l. Perform the installation by clicking **Install,** wait for the installer to complete installing all components, then click **Finish.** The **RSA Archer Control Panel** opens.

## 11.1.4   Post-Installation

### 11.1.4.1   *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.

   a. Start the RSA Archer Queuing Service by doing the following steps:

      i. Go to **Start.**

      ii. Open **Server Manager.**

      iii. Locate **RSA Archer Queuing** in the list under the SERVICES section.

      iv. Right-click **RSA Archer Queuing** and click **Start.**

   b. Add a new instance by doing the following steps:

      i. Open the **RSA Archer Control** Panel.

      ii. In **Instance Management,** double-click **Add New Instance.**

      iii. Enter EHR1 as the Instance Name, then click **Go.**

      iv. Complete the properties as needed.

   c. Configure the Database Connection Properties by doing the following steps:

      i. Open the **RSA Archer Control** Panel.

      ii. In the **Database** tab, go to the **Connection Properties** section.

      iii. In **Instance Management,** double-click the EHR1 instance.

      iv. In the **Database** tab, set up the following:

         1) SQL Server: (local)

         2) Login name: *xxxxxx*

         3) Password: *xxxxxx*

         4) Database: *grc-config*

4. Click on the **Test Connection** link to make sure the **Success** message appears.

5. Configure the General Properties by doing the following steps:

   a. Open **RSA Archer Control** Panel.

   b. Go to **Instance Management.**

   c. Under All Instances, click on EHR1.

    d. In the **General** tab, set up the following:

        i. File Repository section – Path *C:\ArcherFiles\Indexes*

        ii. Search Index section – Content Indexing: Check on Index design language only; Path: *C:\ArcherFiles\Indexes\EHR1*

6. Configure the Web Properties by doing the following steps:

    a. Open the **RSA Archer Control** Panel.

    b. Go to **Instance Management.**

    c. Under **All Instances,** click on EHR1.

    d. In the **Web** tab, set up the following:

        i. Base URL: http://localhost/RSAArcher/

        ii. Authentication URL: *default.aspx*

7. Change SysAdmin and Service Account passwords by doing the following steps:

    a. Open the **RSA Archer Control** Panel.

    b. Go to **Instance Management.**

    c. Under **All Instances,** click on EHR1.

    d. Select the **Accounts** tab.

    e. Change the password on the page by using a strong password.

    f. Complete the Default GRC Platform Instance Creation by clicking **Save** on the toolbar.

8. Register the Instance by doing the following steps:

    a. Open the **RSA Archer Control** Panel.

    b. Go to **Instance Management.**

    c. Under **All Instances,** right-click on EHR1.

    d. Select Update Licensing, enter the following information, then click on Active:

        i. Serial Number (obtained from RSA)

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

        iii. Activation Method (select Automated)

9. Activate the Archer Instance by doing the following steps:

    a. Start the **RSA Archer Services.**

    b. On **Server Manager,** go to **Local Services or All Services.**

     c.    Locate the following services, right-click on each service, and click **Start.**

          i.    RSA Archer Configuration

          ii.    RSA Archer Job Engine

          iii.    RSA Archer LDAP Synchronization

     d.    Restart the RSA Archer Queuing Service.

          i.    Open **Server Manager.**

          ii.    Go to **Local Services** or All Services.

          iii.    Locate the RSA Archer Queuing.

          iv.    Right-click on **RSA Archer Queuing** and click **Restart.**

     e.    Rebuild the Archer Search Index.

          i.    Open **RSA Archer Control** Panel.

          ii.    Go to **Instance Management.**

          iii.    Under **All Instances,** right-click on EHR1, then click on **Rebuild Search Index.**

10. Configure and activate the Web Role (IIS).

     a.    Set up Application Pools as shown in the screenshot.

          i.    Open **Server Manager.**

          ii.    Navigate to **Tools > IIS Manager > Application Pools** (in the left side bar).

          iii.    Right-click to add applications (.NET, Archer GRC, etc.), example screenshot below.

**Figure 11-3 Internet Information Services (IIS) Manager**
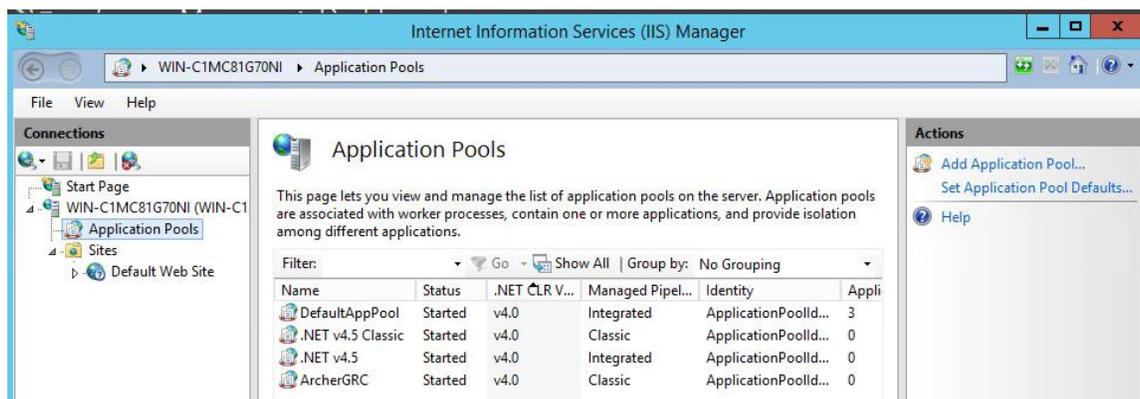


     b.    Restart IIS.

11. Verify that RSA Archer GRC is accessible by opening a browser and inserting the Base and Authentication URL from the web tab of the RSA Archer Control Panel. The RSA Archer GRC Login screen appears as shown below.

**Figure 11-4 RSA Archer GRC User Login**



12. Log in to EHR1 Instance.

**Figure 11-5 Welcome to the Archer Policy Center**

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

## 11.1.5 Content Setup for Establishing GRC Process

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 11-3 Content Sources for GRC Tool**

| Source | Description |
|---|---|
| NIST Framework for Improving Critical Infrastructure Cybersecurity | • 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, and control standards and selecting the relevant control procedures |
| NIST SP 800-66 rev1 | • Used the Security Rule Goals and Objectives in Section 2.1.1 for defining the Corporate Objectives<br><br>• 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) |
| Department of Health and Human Services (HHS) — Office of the National Coordinator for Health Information Technology (ONC) Security Risk Assessment (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

**Figure 11-6 High-Level Structure and Process Steps for NCCoE HIT Mobile Device Use Case GRC Program**
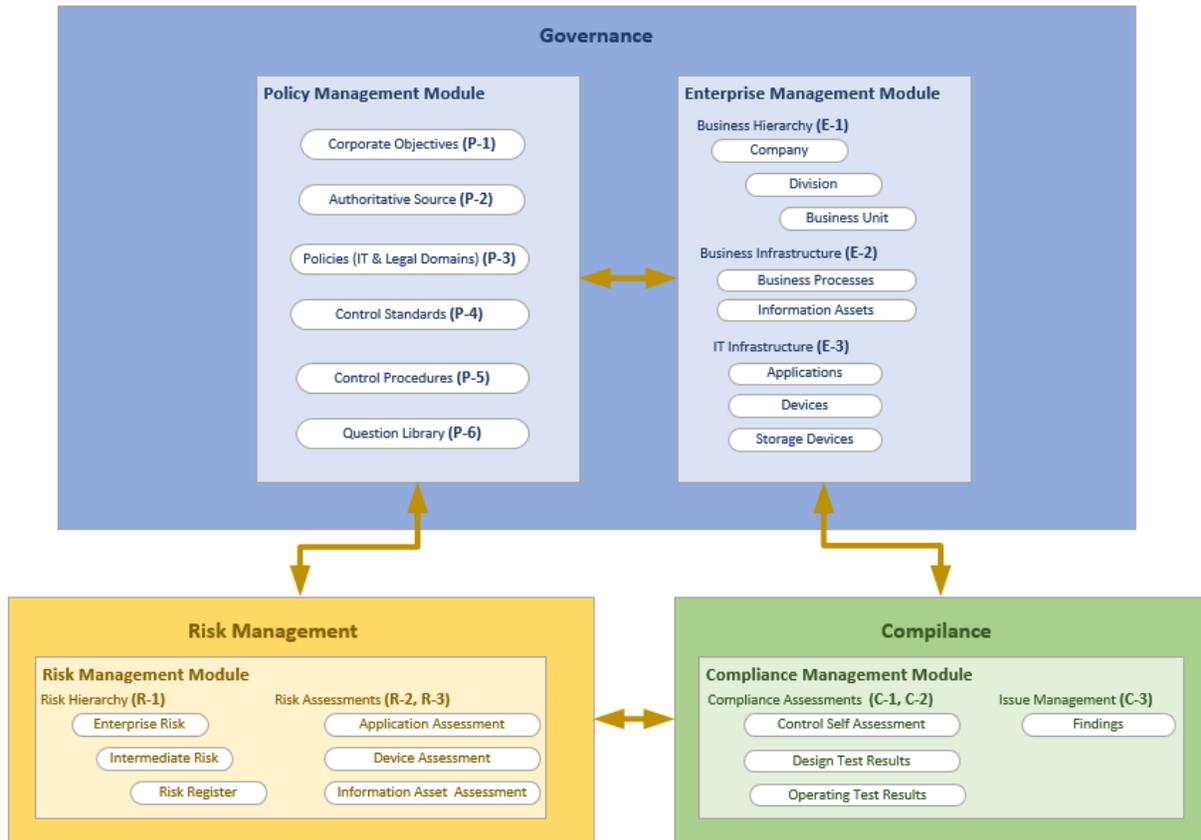


Table 11-4 summarizes the tasks that are conducted for this use case via GRG program. For most of the tasks, the sequential order is not necessary. The task step is used as the content correlator within this guide. The techniques and relevant content sources are outlined as references. The column "RM Tool Required?" indicates that the organization, 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 11-4 High-Level Process Steps for GRC Program**

| 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, and reporting and compliance. The objectives can be related to the defined policies and risks. Through those associations, Archer supports an organization to track policies and monitor related risks and key performance indicators.<br><br>For demonstration purposes, this use case selected a single objective from SP 800-66.<br>**Primary Source:** NIST SP 800-66 | *Archer Module:* Policy Management<br>*Archer App:* Corporate Objectives<br>*Actions:* Use the Archer user interface (UI) to create/update the Corporate Objectives and associate the objective to necessary existing policies, organizations, and risks.<br><br>*To create a Corporate Objective:* **Policy Management (tab) > Corporate Objectives (side menu) > New Record >> Complete desired fields > Save**<br><br>*To update a Corporate Objective:*<br>**Policy Management (tab) > Corporate Objectives (side menu) > Record >> Select the desired record >> Edit >> Update desired fields > Save** | No |
| P-2 | Select/Define Authoritative Source | To scope down the set of relevant controls, NCCoE takes advantage of Archer's content library for | *Archer Module:* Policy Management<br>*Archer App:* Authoritative Sources | Yes |

| Task Step # | Task | Description & Primary Source | Techniques / Steps in Using Archer | RM Tool Required? |
|---|---|---|---|---|
| P-3 | Select/Define related policies | HIPAA Security as the authoritative source, but remaps it to the set of control standards that are specifically created for HIPAA Security (P-4 and P-5).<br>**Primary Source:** HIPAA/Archer content library, NCCoE | *Actions:* Created new report for Authoritative Sources for the target subset of the authoritative source<br><br>*To create the new report:*<br>**Policy Management (tab) > Authoritative Source (side menu) > Reports > New > Fields to Display > Select desired reporting fields > Enter filters (for HIPAA security technical safeguards) > Enter sort option > Enter display option > Save report**<br><br>*To access the new report:*<br>**Policy Management (tab) > Authoritative Source (side menu) > Records (side menu) > Reports (icon) > HIPAA Security Technical Safeguard Compliance (Select Report pop-up)** | |
| P-4 | Create relevant Control Standards | NIST SP 800-66 is used as guidance for NCCoE to create a set of Control Standards that are directly mapped to the HIPAA | *Archer Module:* Policy Management<br>*Archer App:* Control Standards | No |

| Task Step # | Task | Description & Primary Source | Techniques / Steps in Using Archer | RM Tool Required? |
|---|---|---|---|---|
| P-5 | Select SP 800-53 control procedures | 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 800-66, and NIST SP 800-53r4 | *Actions:* Use the Archer UI to create/update the control standards that correspond to relevant source<br><br>*To create new control standard:*<br>**Policy Management (tab) > Control Standards (side menu) > New Record > [enter data] > Save**<br>*Archer App:* Control Procedures<br>*Actions:* Use the Archer UI to import pre-defined data from spreadsheet<br><br>*To import control procedures:*<br>**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 | |

| Task Step # | Task | Description & Primary Source | Techniques / Steps in Using Archer | RM Tool Required? |
|---|---|---|---|---|
| P-6 | Create questionnaires by importing questions | The SRA Tool from the HHS ONC is adopted for populating the questionnaires. **Primary Source:** HHS ONC SRA tool | *Archer Module:* Policy Management<br>*Archer App:* Question Library<br>*Actions:* Use the Archer UI to import pre-defined data from spreadsheet<br><br>*To import questionnaires:*<br>**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 to present the organizations that are defined in lab environment. **Primary Source:** NCCoE HIT EHR Mobile Device Use Case | *Archer Module:* Enterprise Management<br>*Archer App:* Business Hierarchy<br>*Actions:* Use the Archer UI to create/update the Business Hierarchy and associate it to necessary existing policies, objectives, risks, etc.<br><br>*To create new company/division/business unit:*<br>**Enterprise Management (tab) > Business Hierarchy (side menu) > Company/Division/Business Unit > New Record** | No |

| Task Step # | Task | Description & Primary Source | Techniques / Steps in Using Archer | RM Tool Required? |
|---|---|---|---|---|
| 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.<br>**Primary Source:** NCCoE HIT EHR Mobile Device Use Case | *Archer Module:* Enterprise Management<br>*Archer App:* Business Infrastructure<br>*Actions:* Use the Archer UI to create/update the Business Processes and Information Assets and associate them to necessary existing policies, organizations, objectives, risks, etc.<br><br>*To create new business processes/information assets:*<br>**Enterprise Management (tab) > Business Infrastructure (side menu) > Business Processes/Information Assets > New Record** | No |

| Task Step # | Task | Description & Primary Source | Techniques / Steps in Using Archer | RM Tool Required? |
|---|---|---|---|---|
| E-3 | Define/Import IT Infrastructure | With the pseudo organization and lab environment setting, this use case defines Applications and Devices in this group.<br>**Primary Source:** NCCoE HIT EHR Mobile Device Use Case (inventory list, device scanning list, etc.) | *Archer Module:* Enterprise Management<br>*Archer App:* IT Infrastructure<br>*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, etc.<br><br>*To import applications/devices:*<br>**Enterprise Management (tab) > IT Infrastructure (side menu) > Applications/Devices > Data Import >** Follow the Data Import Wizard to Select data file, select format option, perform data mapping, and import data | No |

| Task Step # | Task | Description & Primary Source | Techniques / Steps in Using Archer | RM Tool Required? |
|---|---|---|---|---|
| R-1 | Identify and rate risks and define Risk Hierarchy | Three-level Risk Hierarchy enables an organization to roll up its 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 Risk Assessment Methodology section in Volume E of this guide for details on the risk identification procedures. **Primary Source:** Identified risks from the risk assessment sections | *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, etc. *To create a new risk hierarchy/risk register:* **Risk Management (tab) > Risk Hierarchy/Risk Register (side menu) > New Record** | No |

| Task Step # | Task | Description & Primary Source | Techniques / Steps in Using Archer | RM Tool Required? |
|---|---|---|---|---|
| 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 from 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<br>*Archer App:* Risk Assessments<br>*Actions:* Use the Archer UI to modify existing assessment app; use the Archer UI to conduct assessments<br><br>*To modify existing assessment apps:*<br>**Risk Management (tab) > Administration (side menu) > Application Builder > 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**<br><br>*To conduct risk assessment:*<br>**Risk Management (tab) > Risk Assessments (side menu) > Application Assessment/Device Assessment/Information Asset Assessment (side submenu) > select record > conduct assessment > Save** | Yes |

| Task Step # | Task | Description & Primary Source | Techniques / Steps in Using Archer | RM Tool Required? |
|---|---|---|---|---|
| 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.<br>**Primary Source:** NCCoE | *Archer Module:* all used modules<br>*Archer App:* any application that has risk management tab to be associated or reports that are on the dashboard<br>*Actions:* various – see sample screenshots in Figure 11-16 | Yes |
| C-1 | Compliance Assessment | Various assessments can be used for checking the compliance with HIPAA, control standards, and control procedures.<br>**Primary Source:** HIPAA, HHS ONC SRA tool, Archer Content Library | *Archer Module:* Compliance Management<br>*Archer App:* Compliance Assessments<br>*Actions:* Use the Archer UI to conduct assessments<br><br>*To conduct compliance assessment:*<br>**Compliance Management (tab) > Compliance Assessments (side menu) > Select type of assessment (side submenu) > select record > conduct assessment > Save** | Yes |
| C-2 | Compliance Assessment result/impact analysis and decision-making | Create new customized reports by using existing reports and charts to view the assessment results, and conduct the impact analysis at different levels and different modules.<br>**Primary Source:** NCCoE | *Archer Module:* all used modules<br>*Archer App:* any app that has compliance management tab to be associated or reports that are on the dashboard<br>*Actions:* various – see sample screenshots in section 11.1.5.1 | Yes |

| Task Step # | Task | Description & Primary Source | Techniques / Steps in Using Archer | RM Tool Required? |
|---|---|---|---|---|
| C-3 | Issue Management | The Issue Management module is embedded in other modules, such as Risk Management and Compliance Management. 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 <br> *Archer App:* Findings <br> *Actions:* various – see sample screenshots in section 11.1.5.1 <br><br> *To access "Finding reports":* <br> **Risk/Compliance Management (tab) > Issue Management (side menu) > Findings (side submenu) > Report icon > select report from drop-down list >** view report (drill down for other actions) | Yes |
| Final | Integrate with external data sources and customize reports and dashboards | Utilize the Data Feed feature to set up the dashboards | | Yes |

### 11.1.5.1   Sample Screenshots of Content Setup for Establishing GRC Process

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

**Figure 11-7 P-1: Define Corporate Objectives**



**Figure 11-8 P-2: and P-3: Select/Define Authoritative Source (HIPAA Security) and Related Policies**



**Figure 11-9 P-4: and P-5: Create Relevant Control Standards and Select SP 800-53 Control Procedures (Focus on HIPAA Security, Technical Safeguards)**

**Figure 11-10 P-6: Create Questionnaires by Importing Questions from HHS ONC SRA Tool**



**Figure 11-11 E-1: Define/Import Business Hierarchy**

**Figure 11-12 E-2: Define/Import Business Infrastructure**



**Figure 11-13 E-3: Define/Import IT Infrastructure**

**Figure 11-14 R-1: Identity and Rating Risks and Define Risk Hierarchy**

**Figure 11-15 Risk Register**



**Figure 11-16 R-2: and R-3: Perform Risk Assessment, Result/Impact Analysis, and Decision-Making for Applications, Devices, and Information Asset**
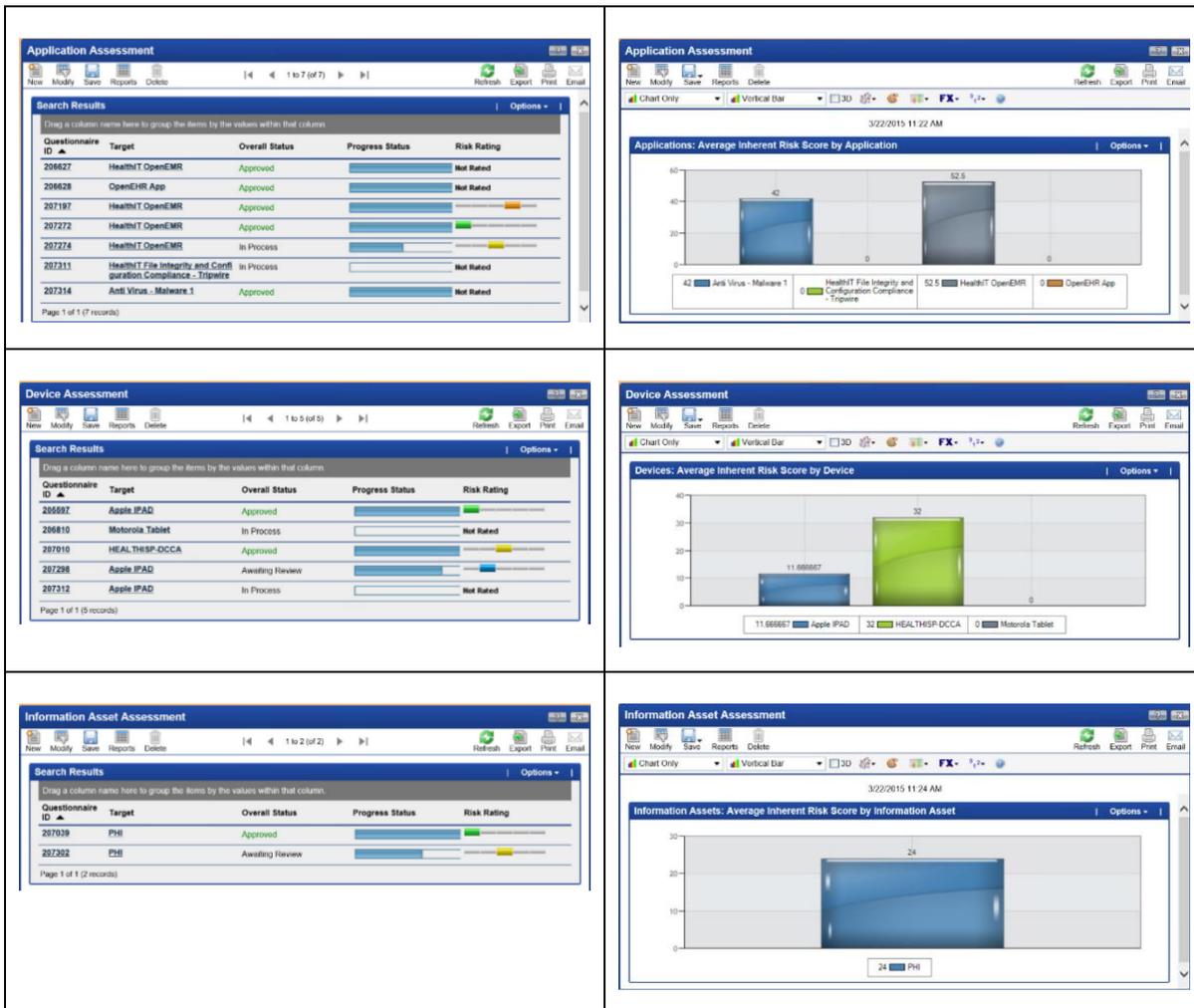
**Figure 11-17 C-1: and C-2: Perform Compliance Assessment, Result/Impact Analysis, and Decision-Making**
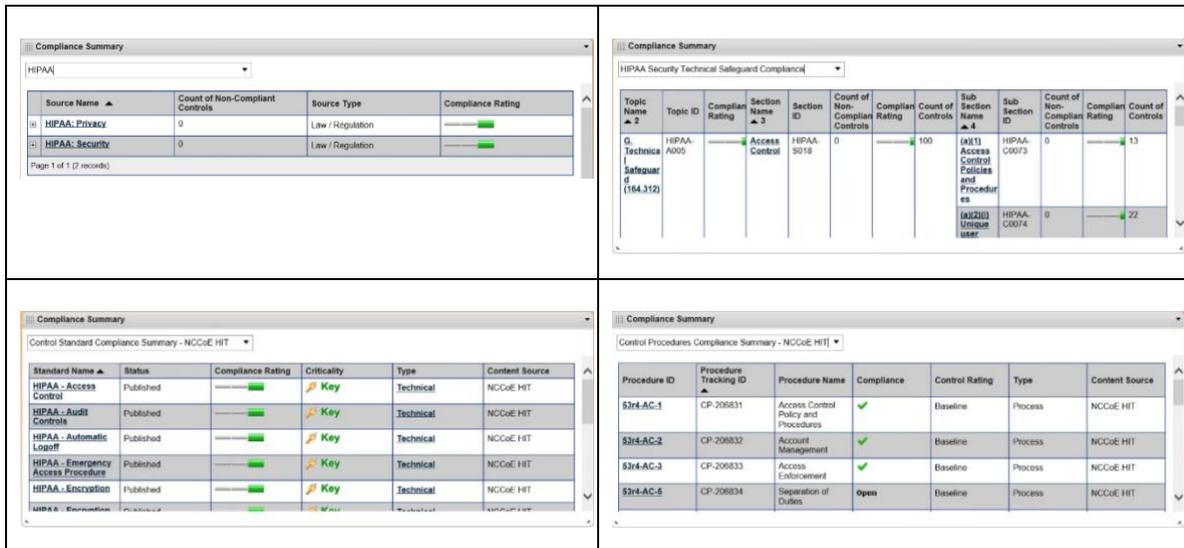


**Figure 11-18 C-3: Manage Issues (Findings)**
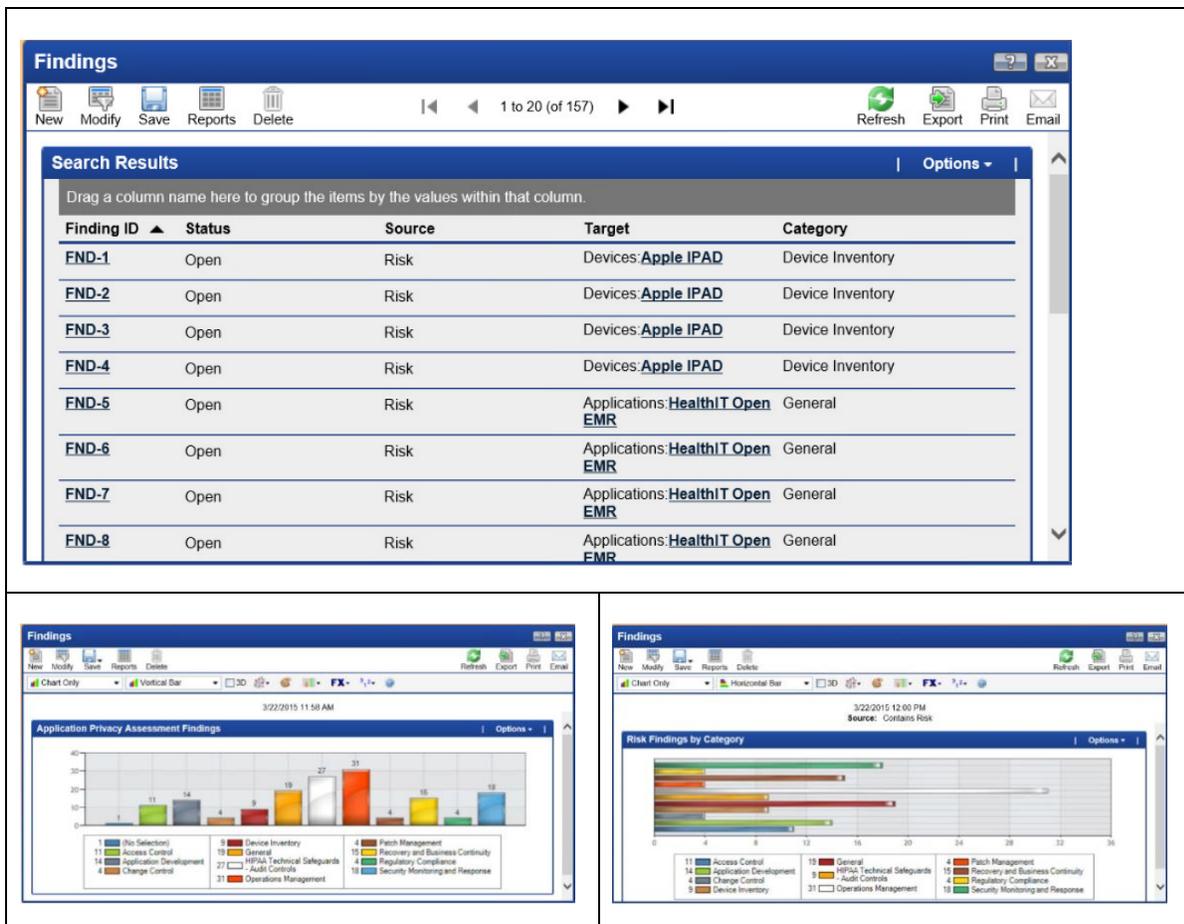
**Figure 11-19 Executive Dashboard**
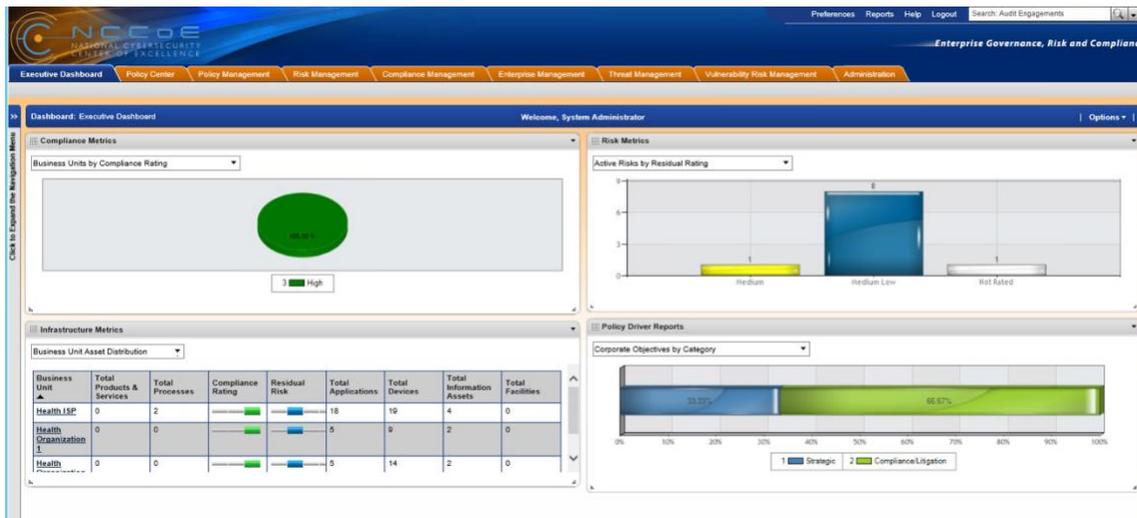


**Figure 11-20 Enterprise Management Dashboard**
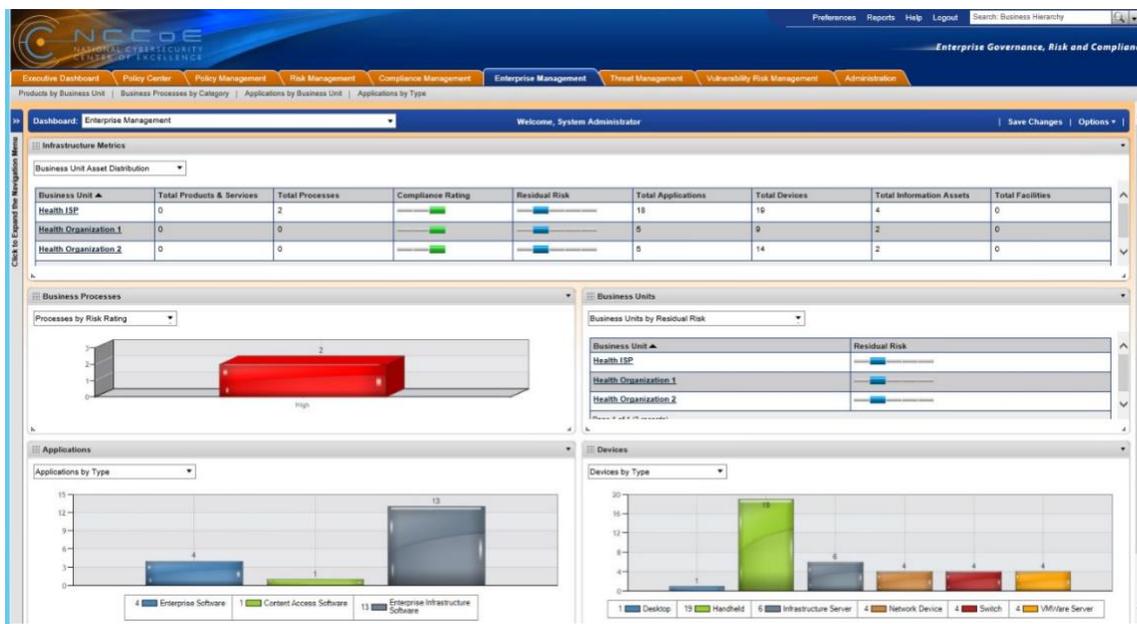
**Figure 11-21 Enterprise Risk Management Dashboard**
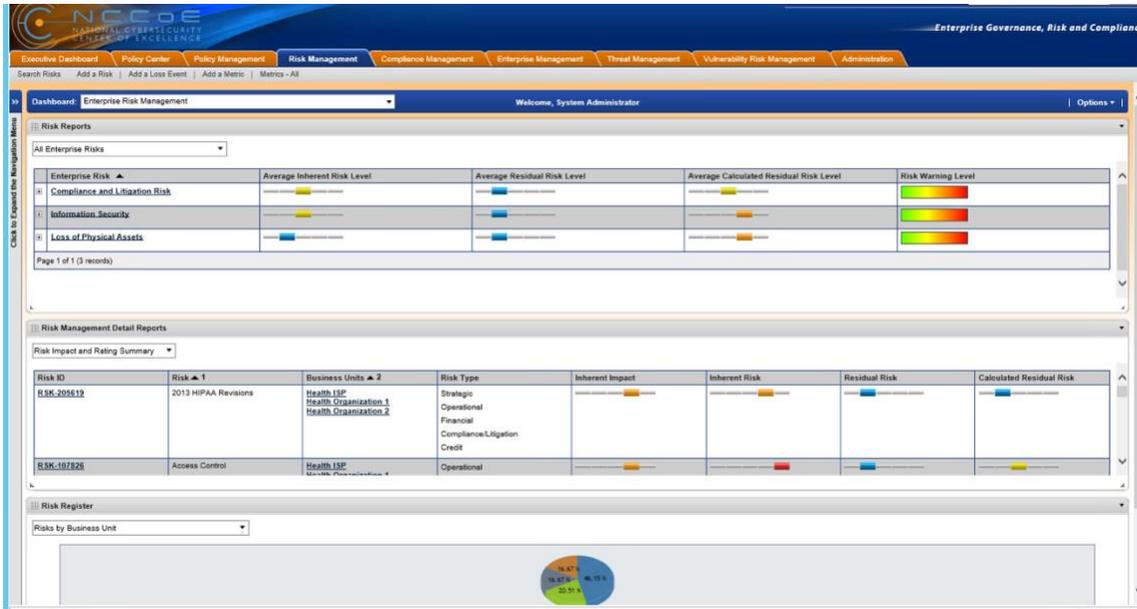


**Figure 11-22 Compliance Management Dashboard**
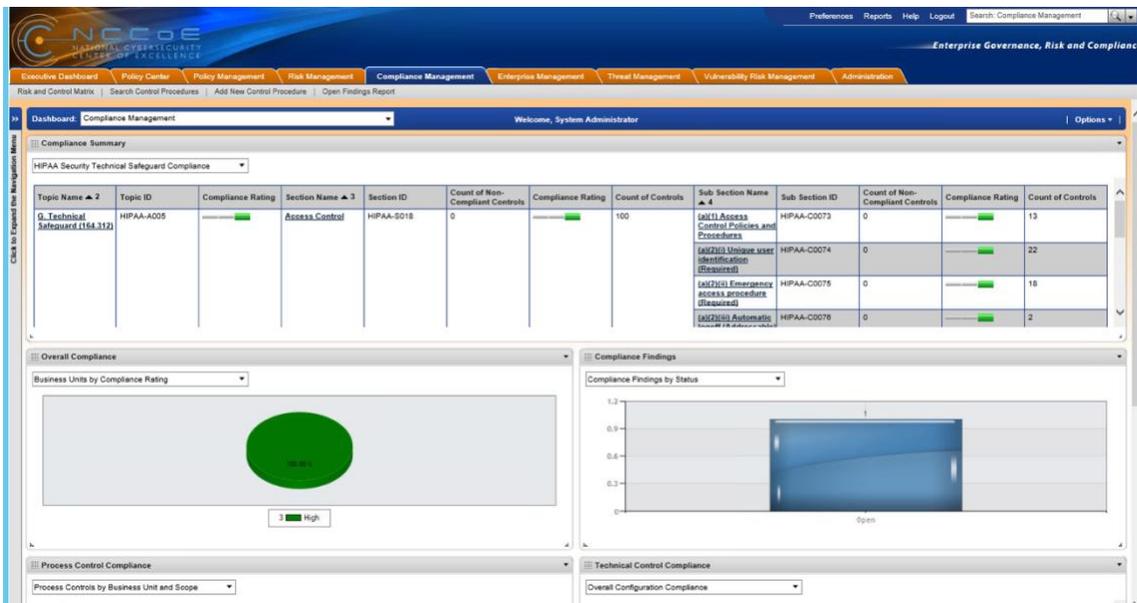
# Appendix A   References

[1]   K. Marchesini, *Mobile Devices Roundtable: Safeguarding Health Information: Real World Usages and Real World Privacy & Security Practices*, March 16, 2012, The Office of the National Coordinator for Health Information Technology, Department of Health & Human Services, https://www.healthit.gov/sites/default/files/onc_ocpo_mobile_device_roundtable_slides_3_16_12.pdf [accessed April 30, 2018].

[2]   *Windows Server Installation Options*, Microsoft TechNet, August 31, 2016, [website], https://technet.microsoft.com/en-us/library/hh831786.aspx [accessed April 30, 2018].