VIX/CVIX Certificates

July 30, 2013

Updated August 2013

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Revision** | **Description** | **Author** |
| 7/30/2013 | 1.0 | Initial Version | Julian Werfel |
| 8/15/2013 | 1.1 | Added details for using VIX Certificate Tool | Julian Werfel |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of Contents**

[1 Purpose 4](#_Toc364331733)

[2 Acronyms and Definitions 4](#_Toc364331734)

[3 Overview 4](#_Toc364331735)

[4 Federation Certificates 4](#_Toc364331736)

[4.1 Certificate Authority 4](#_Toc364331737)

[4.2 Generating Certificates 6](#_Toc364331738)

[4.3 Expiring Certificates 6](#_Toc364331739)

[5 VIX SSL Certificates 8](#_Toc364331740)

[6 CVIX SSL Certificates 8](#_Toc364331741)

[6.1 CVIX Expiration Dates 8](#_Toc364331742)

[6.2 Configuring OpenSSL 8](#_Toc364331743)

[6.3 Generating Certificate Signing Request 9](#_Toc364331744)

[6.4 Verifying Certificate 10](#_Toc364331745)

[7 CVIX Accepting Certificates 10](#_Toc364331746)

# Purpose

The purpose of this document is to describe how the VIX and CVIX applications use certificates, how they are generated and when they need to be updated.

# Acronyms and Definitions

|  |  |
| --- | --- |
| AWIV | Advanced Web Image Viewer |
| BHIE | Bidirectional Health Information Exchange |
| CA | Certificate Authority |
| CSR | Certificate Signing Request |
| CVIX | Centralized VistA Imaging Exchange Service |
| CSR | Certificate Signing Request |
| DoD | Department of Defense |
| FQDN | Fully Qualified Domain Name |
| HAIMS | Health Artifact and Image Management Solution |
| SSL | Secure Socket Layer |
| VIX | VistA Imaging Exchange |
| XCA | Cross Community Access |

# Overview

The VIX and CVIX use certificates to ensure secure communications. The VIX/CVIX communicates with each other using certificates to ensure only authorized applications communicate with the VIX and CVIX.

The CVIX also uses certificates to provide an SSL secured connection when communicating with the DoD.

# Federation Certificates

The VIX and the CVIX communicate with each other using an interface developed by the VistA Imaging team called Federation. To ensure only authorized applications request information from a VIX/CVIX the certificate must be provided as part of the request and the responding VIX/CVIX verifies the certificate is valid before returning any data.

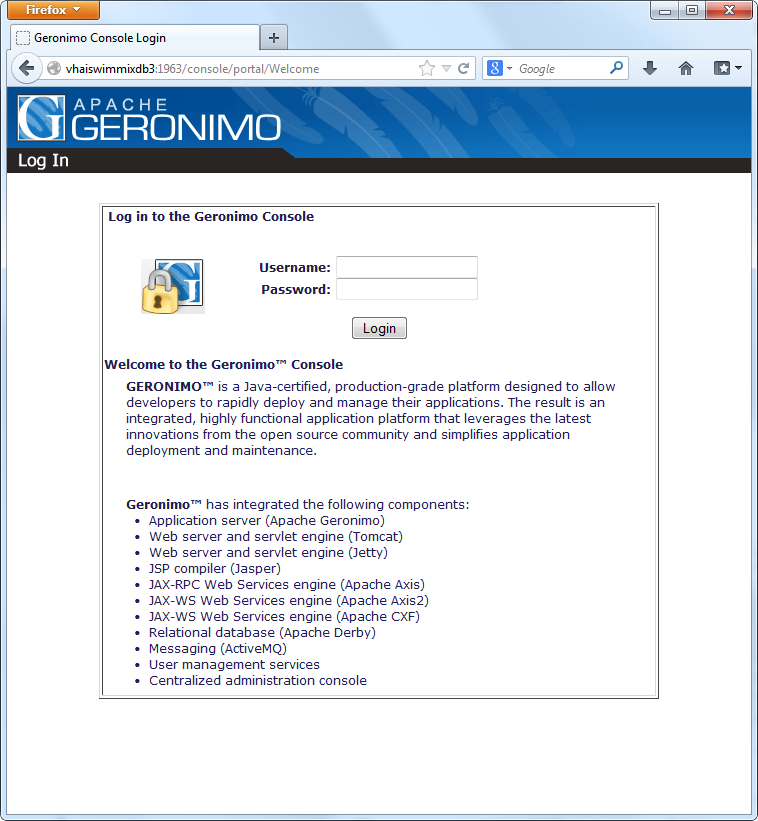
## Certificate Authority

The Federation certificates are generated using a Certificate Authority currently hosted on vhaiswimmixdb3. These certificates can only be generated by this certificate authority or the VIX/CVIX will not validate the certificate.

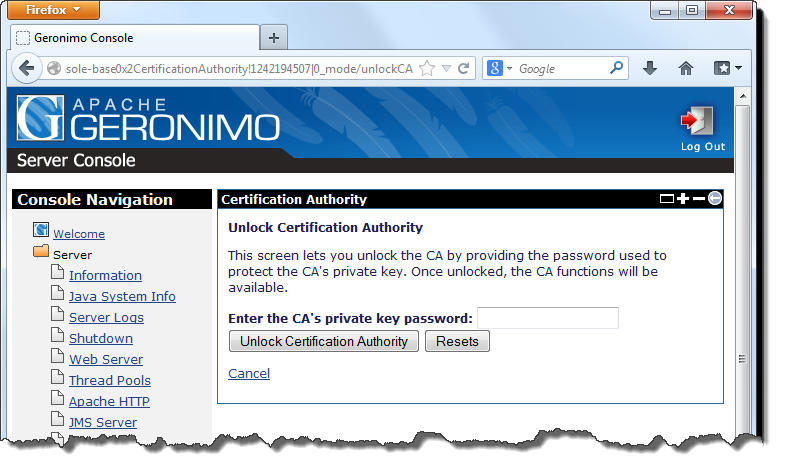
Under normal conditions there is no need to directly access the Certificate Authority. The VIX Certificate Tool (described below) communicates with the CA without the user needing to do anything. On occasion the CA does lock itself which requires the user to go to the CA website and unlock it. If the VIX Certificate Tool has an error communicating with the CA, the most likely reason is because the CA has become locked.

To unlock the CA, follow these steps:

1. Open a web browser to <http://vhaiswimmixdb3:1963/>.
2. On the left side of the page, click the **Console** link.
3. Enter the credentials for the Apache Geronimo login.



1. On the left side of the page click the **Certificate Authority** link.
2. If the CA is locked, a message indicating this will be shown and there will be a link at the bottom that says **Unlock CA**. Click the **Unlock CA** link.
3. Enter the Certificate Authority password and press **Unlock Certificate Authority.**



1. The CA is now unlocked and the VIX Certificate Tool should work. You can also view the issued certificates on this page.

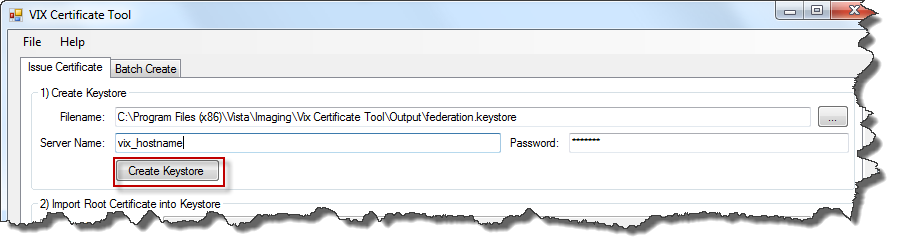
## Generating Certificates

When a VIX or CVIX server is installed the installer will request the VIX certificate. The VistA Imaging development team has a utility (VIX Certificate Tool) that creates the certificate and rolls it up into a ZIP file that the installer expects.

This utility requires that Java be installed the $JAVA\_HOME environment variable be set. If it is not set to the root Java directory the utility will not function properly.

To generate a new certificate for a server, perform the following steps:

1. Launch the VIX Certificate Tool from the Start menu: Start 🡪 All Programs 🡪 VistA Imaging Programs 🡪 VIX Certificate Tool
2. In step 1, enter the hostname of the VIX server and press the **Create Keystore** button.



1. A dialog will appear confirming the keystore was created, press **OK**.
2. Press the **Import Root Certificate** button. A dialog will appear confirming the certificate was imported, press **OK**.
3. Press the **Create CSR** button. A dialog will appear confirming the CSR was generated, press **OK.**
4. Press the **Submit CSR to CA** button.
5. If an error is displayed, it likely means the CA is locked. See instructions above for unlocking the CA. If the CA is working properly you will see a dialog indicating the response was received and the certificate serial number, press **OK**.
6. Press the **Rollup Results** button. A dialog will appear confirming the files were put into a zip file, press OK. A second dialog will appear asking if you want to open the output folder where the ZIP file is contained.
7. The ZIP file generated is what the VIX installer expects (it does not need to be unzipped).

## Expiring Certificates

All certificates have an expiration date. During the initial versions of the VIX deployment the expiration date for the VIX certificate was set as December 31, 2015. After this date, sites with those certificates will not be able to communicate with other VIX/CVIX servers.

After the initial rollout of the VIX and the CVIX the expiration date was set to December 31, 2025.

The following table contains the VIX servers that have certificates expiring in 2015 and MUST be replaced.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Biloxi, MS | 520 | VHABILVIX1.v16.med.va.gov | 45 | Thu Dec 31 00:00:00 EST 2015 |
| Birmingham, AL | 521 | vhabirclu3.v07.med.va.gov | 100 | Thu Dec 31 00:00:00 EST 2015 |
| Central Alabama HCS | 619 | vhacavclu5.v07.med.va.gov | 106 | Thu Dec 31 00:00:00 EST 2015 |
| Dublin, GA | 557 | VHADUBCLU5.v07.med.va.gov | 98 | Thu Dec 31 00:00:00 EST 2015 |
| El Paso, TX | 756 | vhaelpclu2a.v18.med.va.gov | 130 | Thu Dec 31 00:00:00 EST 2015 |
| Fayetteville, AR | 564 | VHAFAVVIX1.V16.MED.VA.GOV | 39 | Thu Dec 31 00:00:00 EST 2015 |
| Fayetteville, NC | 565 | vhafncclu1a.v06.med.va.gov | 71 | Thu Dec 31 00:00:00 EST 2015 |
| Houston, TX | 580 | vhahouclu1a.v16.med.va.gov | 117 | Thu Dec 31 00:00:00 EST 2015 |
| Lebanon, PA | 595 | vhalebvix.v04.med.va.gov | 118 | Thu Dec 31 00:00:00 EST 2015 |
| Little Rock, AR | 598 | VHALITVIX1.V16.MED.VA.GOV | 82 | Thu Dec 31 00:00:00 EST 2015 |
| Loma Linda, CA | 605 | vhalomclu3a.v22.med.va.gov | 114 | Thu Dec 31 00:00:00 EST 2015 |
| Maryland HCS | 512 | vhabalclu2.v05.med.va.gov | 78 | Thu Dec 31 00:00:00 EST 2015 |
| Mountain Home, TN | 621 | VHAMOUCLU4a.v09.med.va.gov | 104 | Thu Dec 31 00:00:00 EST 2015 |
| Muskogee, OK | 623 | VHAMUSVIX1.v16.med.va.gov | 81 | Thu Dec 31 00:00:00 EST 2015 |
| N. Florida/S. Georgia HCS | 573 | vhanflclu7a.v08.med.va.gov | 76 | Thu Dec 31 00:00:00 EST 2015 |
| New Orleans, LA | 629 | VHANOLVIX1.v16.med.va.gov | 89 | Thu Dec 31 00:00:00 EST 2015 |
| North Chicago, IL | 556 | VHANCHVIX.v12.med.va.gov | 41 | Thu Dec 31 00:00:00 EST 2015 |
| Oklahoma City, OK | 635 | VHAOKLVIX1.V16.MED.VA.GOV | 87 | Thu Dec 31 00:00:00 EST 2015 |
| Prescott, AZ | 649 | VHAPREVIX01.v18.med.va.gov | 66 | Thu Dec 31 00:00:00 EST 2015 |
| Spokane, WA | 668 | vhaspoclu4a.v20.med.va.gov | 112 | Thu Dec 31 00:00:00 EST 2015 |
| Washington, DC | 688 | VHAWASVIX1.v05.med.va.gov | 42 | Thu Dec 31 00:00:00 EST 2015 |

To replace the certificate at these sites, a new certificate will have to be generated using the VIX Certificate Tool and then the contents of the resulting zip file should be placed into the VixCertStore directory on the VIX replacing the old files. Then the VIX should be restarted (replacing the federation.keystore and federation.truststore files).

# VIX SSL Certificates

The VIX uses another self-signed certificate for SSL communication on port 443. This allows clients to communicate with the VIX using encryption although the client must accept the unknown certificate root. This certificate expires on March 15, 2025. This certificate is the same for every VIX site.

# CVIX SSL Certificates

The CVIX uses certificates issues by the VA certificate authority. All VA hardware has the VA certificate authority root certificate installed which allows these certificates to work properly. The CVIX uses this certificate for all communication done on port 443 which includes the AWIV Web Application and the XCA interface with the DoD.

The certificate generated should be for the name of the server requestors request data from the CVIX on. In the case of the CVIX this name should be *vhacvixclu2.r04.med.va.gov* because that is the cluster name. We have generated certificates for internal test systems and we created a parallel cluster for field testing of Patch 124 which each used their own certificates but the production cluster name is *vhacvixclu2.r04.med.va.gov*.

All nodes of a CVIX cluster use the same certificate (so it only needs to be generated once for each cluster and then copied to each node).

## CVIX Expiration Dates

Certificates issued by the VA are only good for one year so they must be renewed and updated before they expire.

|  |  |  |
| --- | --- | --- |
| **Hostname** | **Description** | **Expiration Date** |
| vhacvixclu2.r04.med.va.gov | Production CVIX | 9/4/2014 |
| vhaiswimmixvix2.vha.med.va.gov | Internal testing CVIX | 1/28/2014 |
| vhacrbimmcvix3.vaco.va.gov | GOLD Test Environment CVIX | 1/22/2014 |

## Configuring OpenSSL

The CVIX uses a FIPS compliant OpenSSL certificates which are signed by the VA. This process configures OpenSSL and only needs to be done once on a workstation.

1. Copy *$/VistA\_Imaging/Configuration/FIPSCertificateAuthority/Certificate Authority* to your workstation
2. Add openssl.exe to $PATH environment variable (*\Certificate Authority\openssl-fips-1.2.2\out32dll\openssl.exe*)
3. Copy *\Certificate Authority\openssl-fips-1.2.2\apps\openssl.cnf* to *C:\usr\local\ssl\fips-1.0* (create directory structure if needed)
4. Copy *$/VistA\_Imaging/Configuration/FIPSCertificateAuthority/XCACertificateAuthority* to the root drive (*c:\XCACertificateAuthority*)

## Generating Certificate Signing Request

1. Run all commands as administrator (run as Administrator in Windows 7)
2. From *C:\XCACertificateAuthority* run:

openssl genrsa -des3 -out key.pem 2048

It will ask for a password, use anything (it will be removed in the next step). A new key.pem file with 2048 bits will be created

1. Run the following command to remove the password:

openssl rsa -in key.pem -out keyout.pem

Enter the password set in step 2

1. Generate the certificate signing request:

openssl req -new -key keyout.pem -out req.pem

Enter the information requested:

Country Name (2 letter code) [AU]:US

State or Province Name (full name) [Some-State]:Maryland

Locality Name (eg, city) []:Silver Spring

Organization Name (eg, company) [Internet Widgits Pty Ltd]:United States Veterans Administration

Organizational Unit Name (eg, section) []:VistA Imaging

Common Name (eg, YOUR name) []: <FQDN of server>

Email Address []: <your email>

Don’t add any extras when asked

1. Submit the contents of the generated req.pem to <https://vaww.portal.va.gov/sites/PKI/Lists/SSLTLS%20Requests/AllItems.aspx>
   1. Click on the New button
   2. For the domain name, use the FQDN of the server
   3. For the Certificate Signing Request (CSR) copy the contents of the req.pem file into the text box
   4. Use Internal Website for Certificate Scope
   5. Use a VA employee as VA Employee Sponsor
   6. Fill in the Program Office and your email address and press OK.
   7. You will get an email when the certificate has been generated (the certificate response will be in the email)
2. The response from the VA is the certificate to be used. Add as a first line to the response:

-----BEGIN CERTIFICATE-----

Add as a last line to response:

-----END CERTIFICATE-----

Save the response as CVIX\_XCA\_Certificate.pem

1. keyout.pem is the private key and should be renamed to CVIX\_XCA\_PrivateKey.pem when placing on the CVIX.
2. The CVIX installer expects these two files to be in a ZIP file but they are placed on the CVIX in the C:\VixCertStore directory on each node. If installing a new CVIX then use the ZIP file. If simply updating the certificate on an existing CVIX replace the existing *CVIX\_XCA\_PrivateKey.pem* and *CVIX\_XCA\_Certificate.pem* files on the CVIX and restart the service.
3. Also place a copy of the ZIP file and all other generated files into the *$/VistA\_Imaging/Configuration/FIPSCertificateAuthority/XCACertificateAuthority/Cert Requests* directory.

## Verifying Certificate

The certificate can be checked by going to https://<FQDN of CVIX cluster> (ie <https://vhacvixclu2.r04.med.va.gov/>). The SSL lock icon should appear without an error (if on a VA computer)

# CVIX Accepting Certificates

When the CVIX requests data from other services (such as BHIE and HAIMS) using SSL it must accept their certificate. This information is stored in the federation.truststore file that gets placed in the c:\vixcertstore directory on the CVIX during the installation. All CVIX nodes have already been configured to communicate with BHIE and HAIMS so no modification should be needed. However if they change their certificate trust chain a new certificate might be necessary.

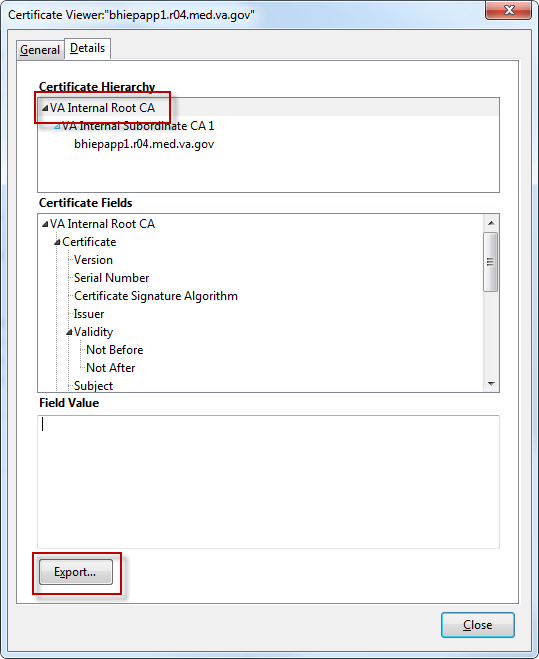
**Note**: The federation.truststore file is the same on each CVIX node. Once this process has been done once, the file can be copied to the other nodes and then restart the CVIX on that node.

**Note**: The federation.keystore file is unique to each server and should not be modified!

keytool.exe must be part of the $PATH (located in the Java\jre\bin directory).

The following steps describe what needs to be done to update the federation.truststore file for a new BHIE certificate.

1. Open in a web browser to BHIE (<https://bhiepapp1.r04.med.va.gov>)
2. Enter credentials for BHIE
3. View the certificate (the steps below are using Mozilla FireFox).
   1. Click on the safe icon next to the URL and click More Information.
   2. Click View Certificate
   3. Click on the VA Internal Root CA and click Export



* 1. Save it as a X509 Certificate (bhie\_root.crt)

1. Open a Command Prompt as an administrator
2. Navigate to c:\vixcertstore
3. Run the following command to list the existing certificates

C:\VixCertStore>keytool -list -keystore federation.truststore

1. Enter the truststore password

Keystore type: JKS

Keystore provider: SUN

Your keystore contains 5 entries

ncat, Jul 28, 2011, trustedCertEntry,

Certificate fingerprint (MD5): 58:08:E8:39:3A:A0:29:08:90:8A:B7:FD:5F:8E:A5:CD

root, Nov 25, 2008, trustedCertEntry,

Certificate fingerprint (MD5): E3:35:ED:5D:87:1E:89:A9:22:4B:1C:4C:20:36:DA:57

bhie\_web, Jun 24, 2011, trustedCertEntry,

Certificate fingerprint (MD5): 88:78:88:B9:E7:15:D0:09:C9:B9:53:CF:12:11:2E:F0

bhie, Jun 16, 2011, trustedCertEntry,

Certificate fingerprint (MD5): A8:9A:12:6A:86:79:E6:38:F9:2D:6B:58:58:A6:5A:B7

haims, Jan 4, 2012, trustedCertEntry,

Certificate fingerprint (MD5): E0:8E:00:0A:38:2B:02:1D:7D:AE:39:15:C7:D5:10:F5

The certificate highlighted above is the one to be replaced (root VA cert used by BHIE)

1. Run the following command to delete the existing cert:

C:\VixCertStore>keytool -delete -alias bhie -keystore federation.truststore

1. Run the following command to import the new cert:

C:\VixCertStore>keytool -importcert -alias bhie -file bhie\_root.crt -keystore federation.truststore

1. When asked to trust this certificate, type yes and press enter