CA Nimsoft ® Unified Management Portal ™

HTTPS Implementation Guide

7.5

Document Revision History

Document Version	Date	Changes
1.0	March 2014	Initial version for UMP 7.5.

Legal Notices

This online help system (the "System") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This System may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This System is confidential and proprietary information of CA and protected by the copyright laws of the United States and international treaties. This System may not be disclosed by you or used for any purpose other than as may be permitted in a separate agreement between you and CA governing your use of the CA software to which the System relates (the “CA Software”). Such agreement is not modified in any way by the terms of this notice.

Notwithstanding the foregoing, if you are a licensed user of the CA Software you may make one copy of the System for internal use by you and your employees, provided that all CA copyright notices and legends are affixed to the reproduced copy.

The right to make a copy of the System is limited to the period during which the license for the CA Software remains in full force and effect. Should the license terminate for any reason, it shall be your responsibility to certify in writing to CA that all copies and partial copies of the System have been destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS SYSTEM “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS SYSTEM, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The manufacturer of this System is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Legal information on third-party and public domain software used in the Nimsoft Monitor solution is documented in *Nimsoft Monitor Third-Party Licenses and Terms of Use (*http://docs.nimsoft.com/prodhelp/en_US/Library/Legal.html*).*

Contact CA

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

Send comments or questions about CA Technologies Nimsoft product documentation to nimsoft.techpubs@ca.com.

To provide feedback about general CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction

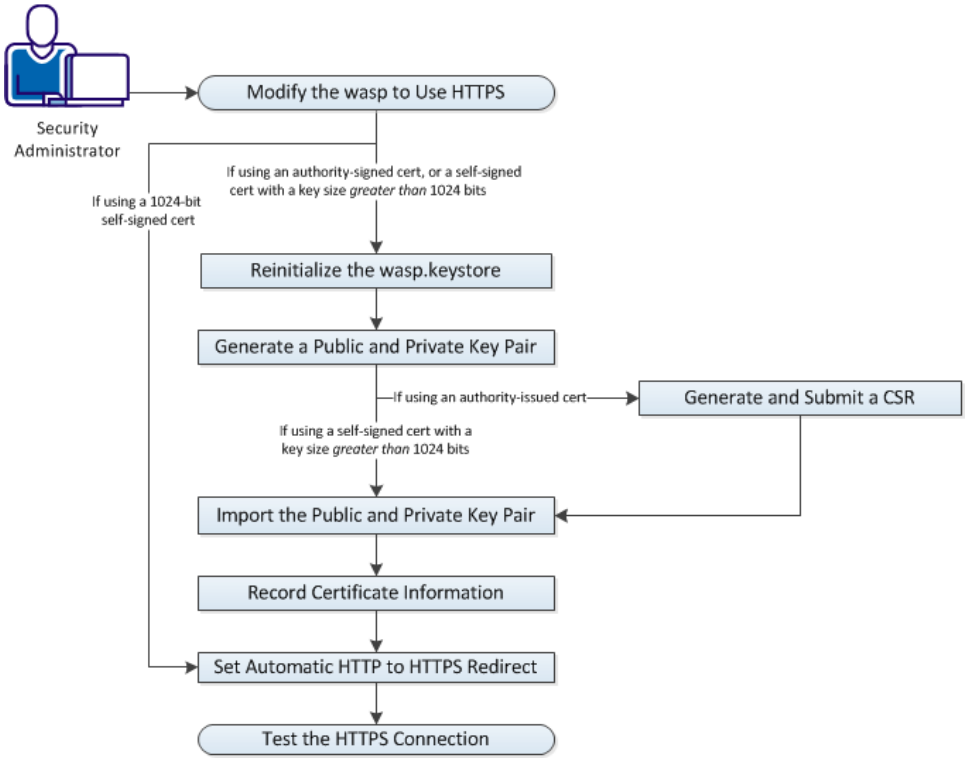
This scenario describes how a security administrator configures the CA Nimsoft Unified Management Portal (UMP) to be accessible via an HTTPS connection.

CA Nimsoft recommends that you consult your network security engineers and compliance specialists regarding your specific security requirements. In general, industry-standard security requirements mandate the use of SSL encryption for client-server communications on an untrusted network. This includes the following situations:

- If users access UMP via a public network, such as the Internet
- If sessions traverse an unsecured part of your network, such as wireless networks in meeting rooms or in public-access areas
- If sessions traverse mobile networks

Note: For high-security environments, it is recommended that you use at least 2048-bit encryption. However, using longer RSA keys significantly affects the speed of encryption and decryption.

The following diagram shows how to configure UMP to use HTTPS:



Prerequisites

Verify the following prerequisites before continuing:

- You are an administrative user with access to Infrastructure Manager.
- Your environment is configured to run keytool commands if you plan to use a certificate other than a 1024-bit self-signed certificate. This means that the $PATH system variable includes a path to java.exe and keytool. See the section keytool Command Not Found (see page 19) for additional information.

The wasp and the ssl_reintialize_keystore Callback

To configure UMP to use HTTPS, you configure the wasp. The wasp (Web Application Service Provider) is an embedded Tomcat web server running as a probe. It is distributed to the system during the UMP installation, and afterward, appears as a probe in Infrastructure Manager.

Regardless of the certificate you wish to implement, the first required step is to modify the wasp.cfg file to enable HTTPS. When this change takes effect, the following occurs:

- The wasp.keystore, an encrypted file that stores certificates, is generated in the directory <*UMP_installation*>/Nimsoft/probes/service/wasp/conf
- A 1024-bit self-signed certificate is automatically generated in the wasp.keystore

You must replace the automatically generated 1024-bit self-signed certificate if you wish to use a different certificate. In addition, you must enter a valid password for the wasp.keystore. However, the wasp.keystore has a *hard-coded, unknown* password. Therefore, the first time you configure the wasp for HTTPS, it is recommended that you execute the *ssl_reinitialize_keystore* callback and set a new password.

The ssl_reinitialize_keystore callback re-creates the wasp.keystore and its password hash. When you run this callback, enter a new password as an argument, and then *securely store the new password for future use*. If you lose or forget this password, the only way to reset it is to reinitialize the wasp.keystore again.

Important! Use caution with the ssl_reinitialize_keystore callback. This callback changes the encryption hash of the wasp.keystore, and will *invalidate any certificates you are currently using*. For this reason, it is strongly recommended that you back up individual key and certificate files, so that if you have to reinitialize the keystore, you can reload the keys and certificates into the new keystore.

In addition, do not use the keytool utility to change the password of the wasp.keystore, as the wasp will not recognize the new password. Currently, the only way to change the password of the wasp.keystore is to use the ssl_reinitialize_keystore callback.

Entity, Intermediate, and Root Certificates

A number of certificate authorities issue intermediate, or *chained* certificates. If your certificate authority issues chained certificates, you will typically receive the following certificate files:

- An *entity* certificate
- One or more *intermediate* certificates
- A root certificate may be included

You must upload the entity certificate and any intermediate certificates your certificate authority provides. You may not need to upload a root certificate. This is because the NMS installation automatically installs a Java Runtime Environment (JRE) that includes the root certificates of many certificate authorities. However, your certificate authority may provide a new root certificate and advise that you upload it.

You can view the root certificates installed automatically with the JRE during the NMS installation.

Follow these steps:

1. Open an administrator command prompt on the server running UMP.
2. Change directories as follows:
   `cd <UMP_installation>/jre/<jre_version>/lib/security`
3. Issue the following command:
   `<UMP_installation>/jre/<jre_version>/bin/keytool keytool -list -keystore cacerts`

   The system prompts you to enter the keystore password. After you enter a valid password, the system displays the default root certificates in the cacerts file.

Chapter 2: Configure UMP to Use HTTPS

This section provides instructions for configuring UMP to use HTTPS.

Note: The steps that you use to implement HTTPS vary depending on the certificate you are using. The diagram in the introduction shows where the work flow varies depending on the certificate you are implementing. In addition, the instructions indicate when you can skip to a later step.

Modify the wasp Configuration to Use HTTPS

Modify the wasp configuration to use HTTPS by specifying an HTTPS port and a maximum number of concurrent HTTPS requests. When you restart the wasp, a 1024-bit self-signed SSL certificate is generated automatically in <UMP_installation>/probes/service/wasp/conf/wasp.keystore.

Follow these steps:

1. Use Remote Desktop to connect to the NMS server.
2. Open Infrastructure Manager.
3. Navigate to the server running UMP, and locate the wasp probe.
4. Press the <Ctrl> key as you right-click the wasp probe, and then select **Raw Configure**.
5. With the **setup** section highlighted, locate the **https_port** key, and click **Edit Key** to specify a port. If necessary, click **New Key** and enter **https_port**.
6. **Note**: The maximum port value you can set is 65535.
7. Edit the **https_max_threads** key to configure the number of concurrent https requests.

   The default value is 500.

   After you click **OK**, the wasp is configured to use an HTTPS connection. The first time the wasp starts with HTTPS enabled, a new keystore, *wasp.keystore*, is generated and stored in <*UMP_installation*>/probes/service/wasp/conf. In addition, a 1024-bit self-signed certificate is generated and stored in the wasp.keystore file.

Important! If you are using the 1024-bit self-signed cert that was generated, restart the wasp probe, and skip to the section Set Automatic HTTP to HTTPS Redirect (see page 15). Otherwise, continue to the next section.

Reinitialize the wasp.keystore

Important! Only perform the following steps if you are not using a 1024-bit self-signed certificate, and *at least one of the following statements is true*:

- You do not know the password of the wasp.keystore.
- This is the *first time* you are configuring UMP to use HTTPS.

If neither of the above statements is true, review the section The wasp and the ssl_reintialize_keystore Callback (see page 9) before continuing.

Follow these steps:

1. Open Infrastructure Manager.
2. Navigate to the server running UMP.
3. Click on the wasp probe to highlight it.
4. Press <Ctrl>+<P> to open the probe utility.
5. In the drop-down menu under **Probe commandset**, select **ssl_reinitialize_keystore**.
6. Enter a new password as an argument.

   Note: Use a password that is at least six characters long. The wasp probe utility will not prevent you from using a shorter password, but you will be unable to make changes to the wasp.keystore as described later.
7. Click the green play button to run the callback.

   The **Command** status bar displays the text **OK**.
8. Securely record the password you set for future use.

Generate a Public and Private Key Pair

Follow these steps:

1. Open an administrator command prompt on the server running UMP.

   Note: Run the following keytool commands in the same directory as the wasp.keystore file, typically <*UMP_installation*>/probes/service/wasp/conf.

   The keytool utility is located in the directory where the JRE resides, typically <*UMP_installation*>/jre/<*jre_version*>/bin/keytool.
2. Verify that you have a valid password for the wasp.keystore:
   `<UMP_installation>/jre/<jre_version>/bin/keytool -list -keystore wasp.keystore`
3. Delete the automatically generated private key:
   `<UMP_installation>/jre/<jre_version>/bin/keytool -delete -alias wasp -keystore wasp.keystore`

4. Verify the key was deleted:
   `<UMP_installation>/jre/<jre_version>/bin/keytool -list -keystore wasp.keystore`
5. Generate the public and private key pair with the key size you require:
   `<UMP_installation>/jre/<jre_version>/bin/keytool -genkeypair -alias wasp -keyalg RSA -keysize <key_size> -keystore wasp.keystore –validity <days_cert_is_valid>`
6. When prompted for your first and last name, enter the FQDN.
7. When prompted, provide entries for the following fields:
   - Organizational unit
   - Organization
   - City or Locality
   - State or Province
   - Two-letter country code

   You are prompted to confirm that the information you entered is correct.

Important! If you are using a self-signed certificate with a key size greater than 1024 bits, skip to the section Import the Public and Private Key Pair (see page 14). If you are using an authority-issued certificate, continue to the next section, Generate and Submit a CSR (see page 13).

Generate and Submit a CSR

Follow these steps:

1. Generate a Certificate Signing Request (CSR):
   `<UMP_installation>/jre/<jre_version>/bin/keytool -certreq -alias wasp -validity <days_cert_is_valid> -keystore wasp.keystore -file <your_domain>.csr`

   Note: For a wildcard certificate, enter ***.<your_domain>.csr** as the last argument in this command.
2. Create a backup copy of the wasp.keystore.

   Note: This is not a required step, but it is strongly recommended. In the event you encounter a problem later in this procedure, a backup copy of the wasp.keystore will save you from having to repeat previous steps.
3. Submit the CSR to the certificate authority:
   a. Paste the CSR into the web form of the certificate authority.
   b. Remove any characters before **----BEGIN CERTIFICATE REQUEST** and after **END CERTIFICATE REQUEST----.**

Import the Public and Private Key Pair

Note: All keystore entries must use a unique alias. You must use the alias *wasp* for the signed, or entity certificate. If your certificate authority provides multiple intermediate certificates, each intermediate certificate must also use a unique alias.

Follow these steps:

1. Open an administrator command prompt on the server running UMP.

   Note: Run the following keytool commands in the same directory as the wasp.keystore file, typically <*UMP_installation*>/probes/service/wasp/conf.

   The keytool utility is located in the directory where the JRE resides, typically <*UMP_installation*>/jre/<*jre_version*>/bin/keytool.

2. If your certificate authority provided a root certificate, import the root certificate:
   `<UMP_installation>/jre/<jre_version>/bin/keytool -import -trustcacerts -alias <root_certificate> -file <root_certificate>.cer -keystore wasp.keystore`

3. Import the intermediate certificate:
   `<UMP_installation>/jre/<jre_version>/bin/keytool -import -trustcacerts -alias <first_intermediate_certificate> -file <first_intermediate_certificate>.cer -keystore wasp.keystore`

4. Repeat the previous step as needed for additional intermediate certificates.

5. Import the signed certificate. This is the entity certificate if you received a chained certificate:
   `<UMP_installation>/jre/<jre_version>/bin/keytool –import –trustcacerts –alias wasp –file <your_domain>.crt –keystore wasp.keystore`

6. Choose **yes** at the prompt **Existing entry alias wasp exists, overwrite?**

7. Issue the following command to verify that the wasp.keystore was updated:
   `<Nimsoft_installation>/jre/<jre_version>/bin/keytool -list -keystore wasp.keystore`

8. Restart the wasp probe.

Record Certificate Information

Follow these steps:

1. Securely record the new password you set for the wasp.keystore.

2. Ensure that you record the validity period you set for the certificate.

3. Back up the certificate files to a secure location.

Set Automatic HTTP to HTTPS Redirect

Follow these steps:

1. Locate the following directory:

   <*Nimsoft_installation*>/Nimsoft/probes/service/wasp/webapps/ROOT/WEB-INF/classes.

2. Open the file portal-ext.properties in a text editor.
3. At the bottom of the portal-ext.properties file, add the line web.server.protocol=https.
4. Save the portal-ext.properties file and restart the wasp probe.

   UMP is now configured to redirect an HTTP login attempt to HTTPS.

Test the HTTPS Connection

Follow these steps:

1. Open a supported web browser.
2. Enter https:// followed by the URL of the UMP server.

The UMP login page appears if the wasp configuration was successfully modified to use HTTPS. If the UMP login page does not appear, verify that you entered the URL of the UMP server correctly.

Note: You can click the lock icon to the left of the URL in the browser address window to view information about the connection.

Appendix A: Troubleshooting SSL Certificates

This appendix provides information to help you troubleshoot issues implementing SSL with UMP.

This section contains the following topics:

Alias <wasp> Already Exists

Symptom:

I see the exception:

```
java.lang.Exception: Key pair not generated, alias <wasp> already exists
```

Solution:

All keystore entries must have a unique alias. When you configure the wasp.cfg to enable SSL, 1024-bit self-signed certificate using the alias wasp is automatically generated in the wasp.keystore. To use a different certificate, you must delete this keystore entry first.

Issue the following keytool command in the same directory as the wasp.keystore:
<UMP_installation>`/jre/`*<jre_version>*`/bin/keytool -delete -alias wasp -keystore wasp.keystore`

Alias Name wasp Does Not Identify a Key Entry

Symptom:

I see the exception:

```
java.io.IOException: Alias name wasp does not identify a key entry
```

Solution:

This exception may occur if you generated a CSR using Microsoft Internet Information Services (IIS). If you use IIS, the certificate and keys that you obtain from a certificate authority may not be in a format that the wasp.keystore can import. In this case, you must convert the certificate files to the PKCS#12, or PFX format before importing them.

Note: The following requires O*penSSL,* a library that provides cryptographic functionality. You can obtain binary distributions at http://www.openssl.org/related/binaries.html.

Issue the following openssl command to convert the certificate to the PFX format:
`openssl pkcs12 -export -out <pfx_file>.pfx -inkey <private_key>.key -in <cert_file>.crt -certfile CACert.crt`

See the website https://www.sslshopper.com for additional help with converting certificate files.

Given Final Block Exception

Symptom:

I see the exception:

```
javax.crypto.BadPaddingException: Given final block not properly padded
```

Solution:

Note: The following requires O*penSSL,* a library that provides cryptographic functionality. You can obtain binary distributions at http://www.openssl.org/related/binaries.html.

Issue the following OpenSSL commands to overwrite the existing wasp alias in the keystore:

```
openssl pkcs12 -in <my_pfx_file>.pfx -out <my_pem_file>.pem
openssl pkcs12 -export -in <my_pem_file> -out <my_keystore>.p12 -name wasp
```

keytool Command Not Found

Symptom:

When I issue a keytool command, a message tells me the command was not found.

Solution:

Verify that paths are set for java.exe and keytool in the $PATH system variable:

1. Open an administrator command prompt on the server running UMP.
2. Issue the following command in the same directory as the wasp.keystore, typically <*UMP_installation*>/probes/service/wasp/conf:
   `java -version`
3. If the system returns errors instead of java version information, add paths for java.exe and keytool to the $PATH system variable.

Signer Cert Does Not Match Issuer Name

Symptom:

I see the exception:

```
java.security.cert.CertificateException: Subject name of signer cert
does not match issuer name of supplied cert chain
```

Solution:

This or a similar exception may occur if your certificate authority issued a *chained* certificate, but the intermediate certificate(s) was not uploaded. You must upload the entity certificate *and* any intermediate certificates your certificate authority provides.

Issue the following keytool command in the same directory as the wasp.keystore, typically <*UMP_installation*>/probes/service/wasp/conf:

```
<UMP_installation>/jre/<jre_version>/bin/keytool -import -keystore
wasp.keystore -trustcacerts -file <intermediate_cert>.CER
```

Note: All keystore entries must use a unique alias. You must use the alias *wasp* for the signed, or entity certificate. If your certificate authority provides multiple intermediate certificates, each intermediate certificate must also use a unique alias.

See the section Entity, Intermediate, and Root Certificates (see page 10) for additional information.