

CA Nimsoft® Unified Management Portal

DMZ Guide

7.6



Document Revision History

Document Version	Date	Changes
1.0	June, 2014	Initial version for UMP 7.6. Updated to include an overview graphic and a procedure to set up the Tomcat Connector.

CA Nimsoft Monitor Copyright Notice

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.

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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: How to Set up Access to UMP through a DMZ

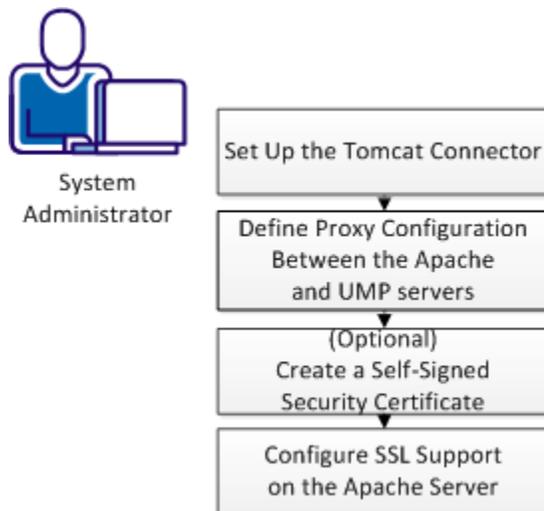
As a system administrator, you enable secure communication through a proxy web server to set up access to UMP through a DMZ.

A DMZ limits your network vulnerability to unauthorized use or attack. External users have direct access only to the proxy web server in the DMZ and not your internal network.

Prerequisites:

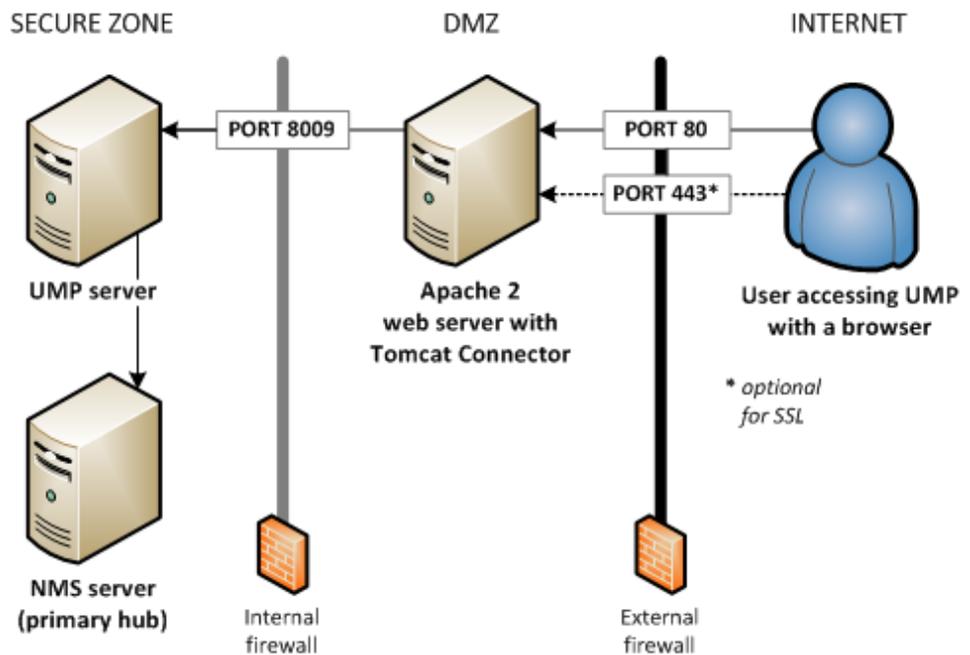
- Install NMS.
- Install UMP and ensure that it is communicating with NMS.
- Download and install Apache and the Tomcat Connector on the server in the DMZ.
- Ensure that you have a JkMount directive appropriate for your configuration.
- Designate a public IP address for the Apache web server (if you want to access UMP from the Internet).

The following flowchart shows how to set up access to UMP through a DMZ.



1. [Set up the Tomcat Connector](#) (see page 7).
2. [Define Proxy Configuration between the Apache and UMP Servers](#) (see page 9).
3. [\(Optional\) Create a Self-Signed Security Certificate](#) (see page 10).
4. [Configure SSL Support on the Apache Server](#) (see page 11).

Graphic Overview of UMP Configured with a DMZ



Set up the Tomcat Connector

Set up the Tomcat Connector to allow communication between the Apache web proxy server and the web application service probe (wasp) in UMP.

Follow these steps:

1. Create the workers.properties file and save it in:

C:\Program Files (x86)\Apache Software Foundation\Apache\conf

2. Specify the UMP server.

For example:

```
# Define 1 real worker using ajp13
worker.list=worker1
# Set properties for worker1 (ajp13)
worker.worker1.type=ajp13
worker.worker1.host=10.10.10.10
worker.worker1.port=8009
```

3. On the Apache server, download the version of mod_jk.so that it matches your version of Apache and save it to:

C:\Program Files (x86)\Apache Software Foundation\Apache\modules

Important! Ensure that you have a JkMount directive appropriate for your configuration.

4. Add the Tomcat Connector configuration to the Apache configuration file, httpd.conf:

For example:

```
# Load mod_jk module
# Update this path to match your modules location
LoadModule jk_module modules/mod_jk.so
# Where to find workers.properties
# Update this path to match your conf directory location (put
workers.properties next to httpd.conf)
JkWorkersFile conf/workers.properties
# Where to put jk shared memory
# Update this path to match your local state directory or logs directory
JkShmFile logs/mod_jk.shm
# Where to put jk logs
# Update this path to match your logs directory location (put mod_jk.log next
to access_log)
JkLogFile logs/mod_jk.log
# Set the jk log level [debug/error/info]
JkLogLevel debug
# Select the timestamp log format
JkLogStampFormat "[%a %b %d %H:%M:%S %Y] "
# Send everything for context / to worker named worker1 (ajp13)
JkMount / worker1
```

The Tomcat Connector is set up for communication.

Define Proxy Configuration between the Apache and UMP Servers

Configure proxy communication between the Apache proxy web server and UMP server so that external browsers can access UMP through the DMZ.

Follow these steps:

1. Edit the Apache configuration file, `httpd.conf`, as follows:

- Uncomment the following lines:
`LoadModule proxy_module modules/mod_proxy.so`
`LoadModule proxy_ajp_module modules/mod_proxy_ajp.so`
- Locate: `#ServerName www.example.com`; uncomment and change it to:
`ServerName <Apache_server_name>.<domain>.com:80`
- Add the following lines to the end of the `httpd.conf` file:
`ProxyRequests On`
`<Proxy *>`
`Order deny,allow`
`Allow from all`
`</Proxy>`
`ProxyPass / ajp://<ump_server_name_orIP>:8009/`
`ProxyPass /c/portal ajp://<ump_server_name_orIP>:8009/c/portal`
`ProxyPass /web/guest ajp://<ump_server_name_orIP>:8009/web/guest`
`ProxyRequests Off`

For example:

```
ProxyRequests On
<Proxy *>
Order deny,allow
Allow from all
</Proxy>
ProxyPass / ajp://10.10.10.10:8009/
ProxyPass /c/portal ajp://10.10.10.10:8009/c/portal
ProxyPass /web/guest ajp://10.10.10.10:8009/web/guest
ProxyRequests Off
```

2. On the *inside* firewall, open Port 8009.

3. On the *outside* firewall, open:

- Port 80
- OR Port 443 if you are using SSL

Note: (Optional) To allow internet access to a hub in the DMZ, you must assign a public IP address.

4. Restart the Apache server.

5. To test whether the Apache web server proxies you to the UMP login page, access the URL of the proxy server in your web browser.

You defined proxy configuration between the Apache and UMP servers.

(Optional) Create a Self-Signed Certificate

You must have a security certificate to configure a secure connection between the proxy web server and web browsers. A certificate from a certificate authority ensures site visitors that any transferred data is more secure. If you do not transfer sensitive data and you are less concerned about security, create a self-signed certificate.

Note: Visitors see a warning that a trusted certificate authority did not issue the certificate but they can proceed to the website.

Follow these steps:

1. Open a command prompt on the web server.
2. Change directories:
C:\Program Files\Apache\conf
3. Generate a private key:
`..\bin\openssl genrsa -des3 -out server.key 1024`
4. Generate a CSR (Certificate Signing Request):
`..\bin\openssl req -config ..\conf\openssl.cnf
-new -key server.key -out server.csr`
5. Remove the passphrase from the key:
`copy server.key server.key.org
..\bin\openssl rsa -in server.key.org -out server.key`
6. Generate a self-signed certificate:
`..\bin\openssl x509 -req -days 365 -in server.csr -signkey server.key -out
server.crt`
7. Edit httpd-ssl.conf to update paths to:
SSLCertificateFile and SSLCertificateKeyFile

You created a self-signed certificate.

Configure SSL Support on the Apache Server

Configure SSL support on the Apache server to establish an encrypted link between the web proxy server and external browsers.

Follow these steps:

1. In the Apache configuration file, `httpd.conf`, uncomment the following lines:
`LoadModule ssl_module modules/mod_ssl.so`
`Include conf/extra/httpd-ssl.conf`

2. In the Apache configuration file `conf/extra/httpd-ssl.conf`, edit the following parameters:

Listen port

Identifies the port number that is opened on the inside firewall for SSL as required.

Note: You can use the `netstat` command to make sure that no other applications are using the port that you specify. If you use port 443 on an Internet Information Services (IIS) web server, this may be an issue.

VirtualHost

Identifies the port number that is opened on the inside firewall for SSL. (Default value is 443.)

ServerName

Defines the name for the Apache server, including port number (for example: `10.10.10.10:443`).

ServerAdmin

Defines the email address for the administrator.

SSLCertificateFile

Identifies the path to the PEM encoded certificate.

SSLCertificateKeyFile

Identifies the path to the private key if it is not already combined with the certificate.

3. In the Apache configuration file `conf/extra/httpd-ssl.conf`, accept the default or specify the desired path for the following parameters:

- **DocumentRoot**
- **SSLSessionCache**
- **ErrorLog**
- **TransferLog**
- **CustomLog**

-
- Restart the Apache web server.

You configured SSL support on the Apache server.

Chapter 1: How to Set up Access to UMP through a DMZ **5**

Graphic Overview of UMP Configured with a DMZ.....	6
Set up the Tomcat Connector	7
Define Proxy Configuration between the Apache and UMP Servers	9
(Optional) Create a Self-Signed Certificate	10
Configure SSL Support on the Apache Server	11