CA Nimsoft® Unified Management Portal

DMZ 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 7

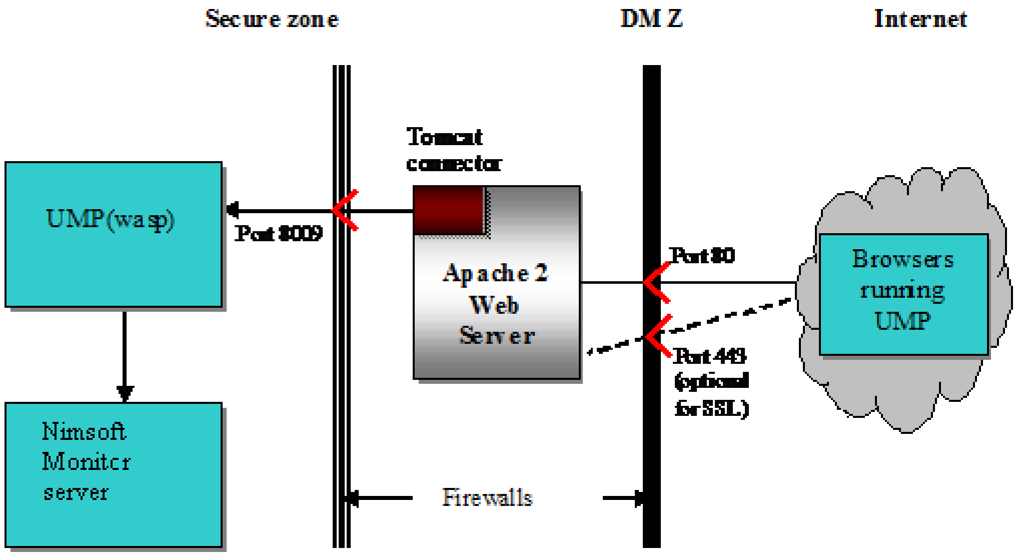
Chapter 2: Setting up a DMZ 9

Chapter 3: Configuring Secure Communications 11

Chapter 1: Introduction

Using a demilitarized zone (DMZ) is the recommended way to set up the Unified Management Portal (UMP) in a firewalled environment. You can install and configure the Apache Web Server as a light-weight proxy server and enable SSL on the Apache server.

The following graphic shows a UMP implementation with a DMZ.



For additional information on using CA Nimsoft products with a DMZ, see the section on installing in a firewalled environment in the *Nimsoft Monitor Server Installation Guide*.

Chapter 2: Setting up a DMZ

This section describes how to set up a DMZ for use with UMP.

Follow these steps:

1. If you have not already installed Apache and the Apache Tomcat connector, download and install them on the server in the DMZ.

   If you have already installed Apache and the Apache Tomcat connector, continue to the next step.

2. Open the Apache configuration file, httpd.conf, for editing.

3. Uncomment the following line:

   ```
   LoadModule proxy_module modules/mod_proxy.so
   ```

4. Uncomment the following line:

   ```
   LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
   ```

5. Locate the following line:

   ```
   #ServerName www.example.com
   ```

6. Remove the pound or hash sign (#) and change the line to the following:

   ```
   ServerName <your_server_name>.<domain>.com
   ```

7. Add the following lines to the end of the httpd.conf file before the line ProxyRequests Off:

   ```
   ProxyPass / ajp://<ump server>:8009/
   ProxyPass /c/portal ajp://<ump server>:8009/c/portal
   ProxyPass /web/guest ajp://<ump server>:8009/web/guest
   ```

   Example

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

8. Open port 8009 on the inside firewall and port 80 on the outside firewall. If you are using SSL, also open port 443 (or an alternative port) on the inside firewall.

   The DMZ is now set up for use with UMP.

Chapter 3: Configuring Secure Communications

To access UMP via HTTPS, you must configure SSL support on the Apache server.

Note: Using secure communication adds overhead to the communication between Apache and UMP.

Follow these steps:

1. Open the httpd.conf file for editing:
   - Uncomment the following line:

     ```
     LoadModule ssl_module modules/mod_ssl.so.
     ```

   - Uncomment the following line:

     ```
     Include conf/extra/httpd-ssl.conf.
     ```

2. Open the file conf/extra/http-ssl.conf:
   - Change the Listen port number as required. If using 443, make sure there are no other applications using it, particularly IIS.
   - Change the SSLSessionCache path to point to the correct location.
   - Change <VirtualHost> to point to the port number specified above.
   - Change the DocumentRoot path to point to the correct location.
   - Change ServerName to the correct value, including port number.
   - Change the ServerAdmin email address as required.
   - Change the ErrorLog path to point to the correct location.
   - Change the TransferLog path to point to the correct location.
   - Change the SSLCertificateFile path to point to the PEM encoded certificate. (If you do not have a certificate, follow the instructions in step 3 to generate a self-signed certificate.)
   - Change the SSLCertificateKeyFile path to point to the private key if it is not already combined with the certificate. (If you do not have a certificate, follow the instructions in step 3 to generate a self-signed certificate.)
   - Change CustomLog to point to the correct location.

3. If you do not have a certificate, use the following steps to generate a self-signed certificate:

   a. Open a Windows Command prompt and change directories to C:\Program Files\Apache\conf.

b. Run the following command to generate a private key:

   ```
   ..\bin\openssl genrsa -des3 -out server.key 1024
   ```

c. Run the following command to generate a CSR (Certificate Signing Request):

   ```
   ..\bin\openssl req -config ..\conf\openssl.cnf
   -new -key server.key -out server.csr
   ```

d. Run the following commands, depending on your OS, to remove the passphrase from the key :

   ```
   Linux/UNIX: cp server.key server.key.org
   ```

   ```
   Windows: copy server.key server.key.org
   ```

   followed by

   ```
   ..\bin\openssl rsa -in server.key.org -out server.key
   ```

e. Run the following command to generate a self-signed certificate:

   ```
   ..\bin\openssl x509 -req -days 365 -in server.csr -signkey
   server.key -out server.crt
   ```

f. Update SSLCertificateFile and SSLCertificateKeyFile in http-ssl.conf file to point to the newly generated certificate and private key files.

4. Restart the Apache web server.

   The Apache server is now configured for SSL support.