CA Nimsoft® Unified Management Portal

DMZ Guide

7.0

Document Revision History

Document Version	Date	Changes
1.0	September 2013	Initial version for UMP 7.0.

Legal Notices

Warranty

The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Nimsoft LLC disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Nimsoft LLC shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Nimsoft LLC and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Nimsoft LLC as governed by United States and international copyright laws.

Restricted Rights Legend

If software is for use in the performance of a U.S. Government prime contract or subcontract, Software is delivered and licensed as "Commercial computer software" as defined in DFAR 252.227-7014 (June 1995), or as a "commercial item" as defined in FAR 2.101(a) or as "Restricted computer software" as defined in FAR 52.227-19 (June 1987) or any equivalent agency regulation or contract clause. Use, duplication or disclosure of Software is subject to Nimsoft LLC's standard commercial license terms, and non-DOD Departments and Agencies of the U.S. Government will receive no greater than Restricted Rights as defined in FAR 52.227-19(c)(1-2) (June 1987). U.S. Government users will receive no greater than Limited Rights as defined in FAR 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Trademarks

Nimsoft is a trademark of CA.

Adobe®, Acrobat®, Acrobat Reader®, and Acrobat Exchange® are registered trademarks of Adobe Systems Incorporated.

Intel® and Pentium® are U.S. registered trademarks of Intel Corporation.

Java(TM) is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Netscape(TM) is a U.S. trademark of Netscape Communications Corporation.

Oracle® is a U.S. registered trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of the Open Group.

ITIL® is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries.

All other trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

For information on licensed and public domain software, see the *Nimsoft Monitor Third-Party Licenses and Terms of Use* document at: http://docs.nimsoft.com/prodhelp/en_US/Library/index.htm?toc.htm?1981724.html.

Contact CA Nimsoft

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.

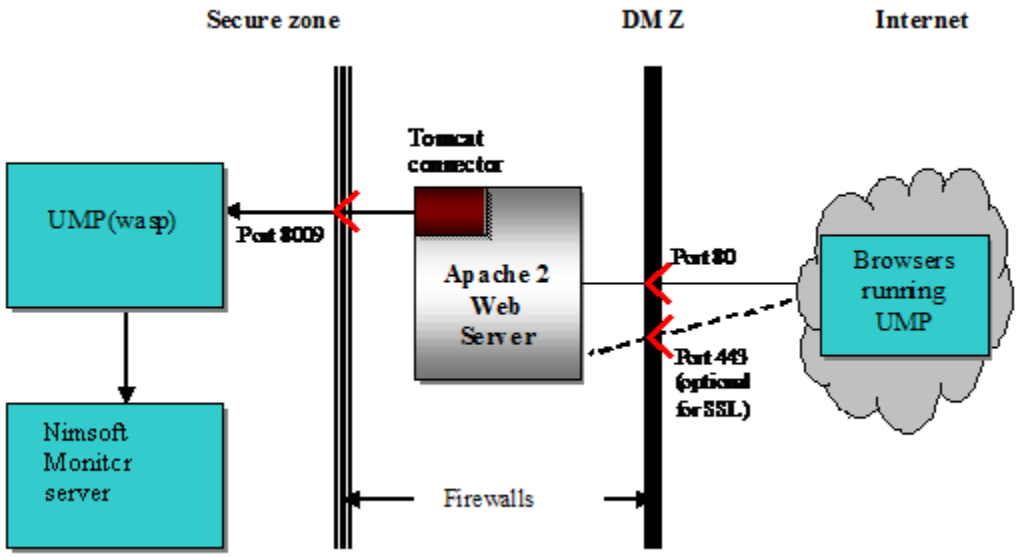
Contents

Chapter 1: Introduction

This section describes how to set up the Unified Management Portal (UMP) to operate in a demilitarized zone (DMZ).

Using a DMZ is the recommended way to set up UMP in a firewalled environment. You can install and configure the Apache 2 web server as a light-weight proxy server and enable SSL on the Apache 2 server.

The following graphic shows a UMP implementation with a DMZ.



For more 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*.

This section contains the following topics:

Prerequisites (see page 8)

Prerequisites

The DMZ installer runs on the following versions of Windows.

Production environments:

- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

Small production environments and test environments:

- Microsoft Windows XP
- Microsoft Windows Vista

Chapter 2: Setting Up the DMZ

This section tells you how to set up a DMZ to use with UMP. If you do not already have the Apache 2 web server and Apache Tomcat connector installed, you will install them using the SDP DMZ Wizard.

If you do already have the Apache 2 web server and Apache Tomcat connector installed, you will configure them for use with UMP by editing configuration files.

This section contains the following topics:

New Apache 2 Installations

This section tells you how to install Apache 2 with the Apache Tomcat connector to allow access to UMP from the Internet.

If you already have the Apache 2 web server with the Apache Tomcat connector installed, skip to Existing Apache 2 Installations (see page 11).

Installing Apache 2 and the Apache Tomcat connector consists of these high-level steps:

1. Run the SDP DMZ wizard on the server in the DMZ.

   This wizard installs the Apache 2 web server and the Tomcat connector. It also opens port 80 and port 8009 (or the ports specified in the SDP DMZ Wizard) on the server.

2. Edit the httpd.conf file.

3. 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 following sections tell you in detail how to do these steps.

Installing Apache 2

Run the SDP DMZ wizard on the server in the DMZ. This wizard installs the Apache 2 web server and the Tomcat connector.

1. Download the SDP DMZ installation file from the CA Nimsoft support site:

   http://support.nimsoft.com/downloads/SDP-V02/SDP-V0261/GA/GA1/Installation/Nimsoft-SDP-DMZ-V0261.exe

   If the link does not work, go to the CA Nimsoft support site Downloads page and under Nimsoft Service Delivery Portal 2.6.1 GA Build 1210 click on Nimsoft SDP DMZ installation.

2. Execute the Nimsoft-SDP-DMZ-V0261.exe file.

3. In the License Agreement dialog, read the text and click Yes.

4. In the Choose Destination Location dialog, click Browse to choose another directory if wanted, then click Next.

5. In the Proxy Server Configuration dialog, enter:

   - The IP address and port of the UMP server. The default is port 8009.
   - The IP address and port number of the Unified Reports Server (if you want to use Unified Reports).

     Note: For UMP, Unified Reports must be installed on the same host as UMP, so the host and port for SDP Server and SDP Unified Reports Server must be the same.

   - The port to be opened for the DMZ Server (from outside the firewall into the web server in the DMZ). The default is port 80.

     If you need to change the port number for the Tomcat server, see the section Existing_Apache_2 Installations (see page 11).

6. Click Install.

   The installer copies files.

7. When the installer finishes, click Finish to exit the installation wizard.

8. Open the Apache2/conf/httpd.conf file for editing and find the following line:

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

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

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

10. 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
    ```

The lines look similar to this:

```
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
```

11. 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 to use with UMP.

Existing Apache 2 Installations

This section tells you how to configure an existing Apache 2 web server with the Apache Tomcat connector to allow access to UMP from the Internet.

Configuring the Apache Web Server with mod_proxy_ajp

1. Open the Apache configuration file, httpd.conf, for editing.
2. Uncomment the following line:

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

3. Uncomment the following line:

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

4. Add the following lines at the end of the 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
   ```

   The lines look similar to this:

   ```
   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
   ```

5. Restart the Apache 2 web server.

For more information about Apache servers, see:

http://httpd.apache.org/docs/2.2/mod/mod_proxy.html

http://httpd.apache.org/docs/2.2/mod/mod_proxy_ajp.html

Configuring the Apache Web Server for Secure Communication

If you want to run UMP with SSL (Secure Sockets Layer) and HTTPS (Hypertext Transfer Protocol Secure), you must configure the Apache 2 web server with SSL support. Information on how to configure the Apache 2 web server with SSL can be found on the following web site:

http://httpd.apache.org/docs/2.2/ssl/

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

To configure the Apache 2 web server to use secure communication:

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. Create 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 as it is the default SSL port for 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, do the following steps to generate a self-signed certificate:
   a. Open a Windows Command window and change directories to C:\Program Files\Apache2\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.

Important!: If you are using a self-signed certificate and Mozilla Firefox as a browser, due to the implementation of the Adobe FlashPlayer plugin you must set the wasp configuration variable webapps/sdp/use_html_upload=1 in order to be able to upload images and dashboards. Refer to the wasp probe documentation for information about wasp configuration variables.