Admin Console

User Documentation

7.0

technologies

Legal Notices

Copyright © 2013, CA. All rights reserved.

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

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.

Documentation Changes

This table describes the version history for this document.

Version	Date	What's New?
7.1	December 2013	Robot selection section has been updated.
7.0	Sept 2013	Configurable HTTP/HTTPS communication between Admin Console and NMS. Simplified deployment of self-signed SSL certificates.
1.0	March 2013	Initial release of Admin Console.

Related Documentation

Documentation for Admin Console compatible probes (../../Probes/AdminConsole/index.htm)

Monitor Metrics Reference Information for CA Nimsoft Probes (../../Probes/ProbeReference/index.htm)

Contents

Chapter 5: Download Probes from Web Archive 37

Chapter 6: Deploy Probes Using Admin Console 39

Chapter 7: General Probe Configuration 43

Appendix A: Troubleshooting SSL Certificates 49

Chapter 1: Getting Started with Admin Console

This topic describes how to display and view data in the Admin Console. You can access the Admin Console either through the Unified Management Portal (UMP) or in a standalone web page.

NMS System Administrators and NMS users with administrator or superuser permissions can access this application.

The standalone version of the Admin Console is installed during your NMS system installation. The Admin Console portlet is installed during your UMP installation.

The Admin Console application allows you to manage and maintain your hubs, robots, and probes on your CA Nimsoft Monitor system.

This section contains the following topics:

Accessing Through UMP

The Admin Console can run within an UMP portlet. Using Admin Console, you can manage and maintain your hubs, robots, and probes on your CA Nimsoft Monitor system.

If this is your first time using Admin Console, you will need to set up the page and portlet by following the procedures in the following section.

Create a Page

You can create custom pages where you control which portlets are displayed and the layout of the page. You can choose whether your pages are private pages, seen only by you, or public pages, which can be viewed by anyone on the Internet. When you first log in, your private pages are displayed. Public pages are accessed by choosing Go to, My Public Pages from the menu bar.

To create a page:

1. Add a page (see page 8).
2. Select a layout (see page 8).
3. Add portlets (see page 8).

Add a Page

1. Choose Add, Page from the menu bar.
2. Enter a name for the page in the text box that is displayed next to the page tabs.
3. Click the green check mark next to the text box.
4. Click on the tab for the page to view it.

Select a Layout

1. Choose Manage, Page Layout from the menu bar.
2. Select the layout you want.
3. Click Save.

Add Portlets

1. Choose Add, Portlet from the menu bar.
2. Click the + sign next to Monitoring.
3. Drag a portlet to the position on the page where you want to display it, or click Add next to the portlet.

Repeat these steps to add more portlets to your layout.

Log in to Admin Console in UMP

Follow these steps:

1. Connect to your UMP application in a web browser.
2. Enter a valid Nimsoft user name and password.

   The CA Nimsoft Unified Management Portal opens to the USM portlet.

3. Click the Admin Console tab.

   Note: If the Admin Console tab is not available, see the Add Portlets (see page 8) section to add this portlet.

   The Admin Console screen appears.

Your NMS system is available for configuration.

Note: If you are accessing Admin Console over a secure HTTPS connection with a self-signed SSL certificate, and you cannot view it in UMP, then you need to open Admin Console in the standalone web page. After opening the standalone version of Admin Console, a message indicating that the security certificate is not trusted displays--click **Proceed anyway**. This only provides a temporary work around. If you close your browser and then go back to the Admin Console application you will need to accept the certificate again.

Accessing Through Standalone Web Page

The Admin Console is available through a web page. The Admin Console allows you to manage and maintain your hubs, robots, and probes on your CA Nimsoft Monitor System.

Log in to Admin Console in a Standalone Web Page

Follow these steps:

1. Enter https://<service_host>:8443/adminconsole in your web browser window.

   Note: <service_host> is the system where the service_host probe is installed.

2. Enter a valid NMS username and password.

   The Admin Console application opens.

Interface Overview

This section introduces you to the Admin Console interface. The main window contains two buttons in the upper left corner to access the list of hubs/robots and the probe archive.

The upper right corner displays the username used to access this application and the help button (?).

Use the arrow next to the username in the upper right corner to change the password for this username or to logout of the Admin Console.

The main window is divided into two sections. The left navigation pane displays the hubs and robots in a tree structure. The right pane displays either robot or probe information based on your selection in the navigation pane.

At the top of each section is a filter you can use to narrow your list. The filters only apply to the appropriate section of the screen.

Infrastructure Interface Overview

To manage your Hubs, select the Infrastructure button in the Admin Console screen.

The navigation pane displays the hubs and robots in a tree structure. The right side of the screen displays the robot information for the hub selected in the navigation pane.

The right pane displays the robot properties. See How to Modify Robot Properties View (see page 12) for more information.

The ? (Help) icon opens the online help for the Admin Console application.

Robot Interface Overview

To manage your robots, select the Infrastructure button in the Admin Console screen then select a robot in the navigation pane.

The right pane provides four options for accessing information about your robot: Robot Properties, Probes, Packages Installed, and Environment variables.

Robot Properties

This screen displays the properties associated with your robot. This screen is a read-only screen and provides the following information for the robot:

OS Major

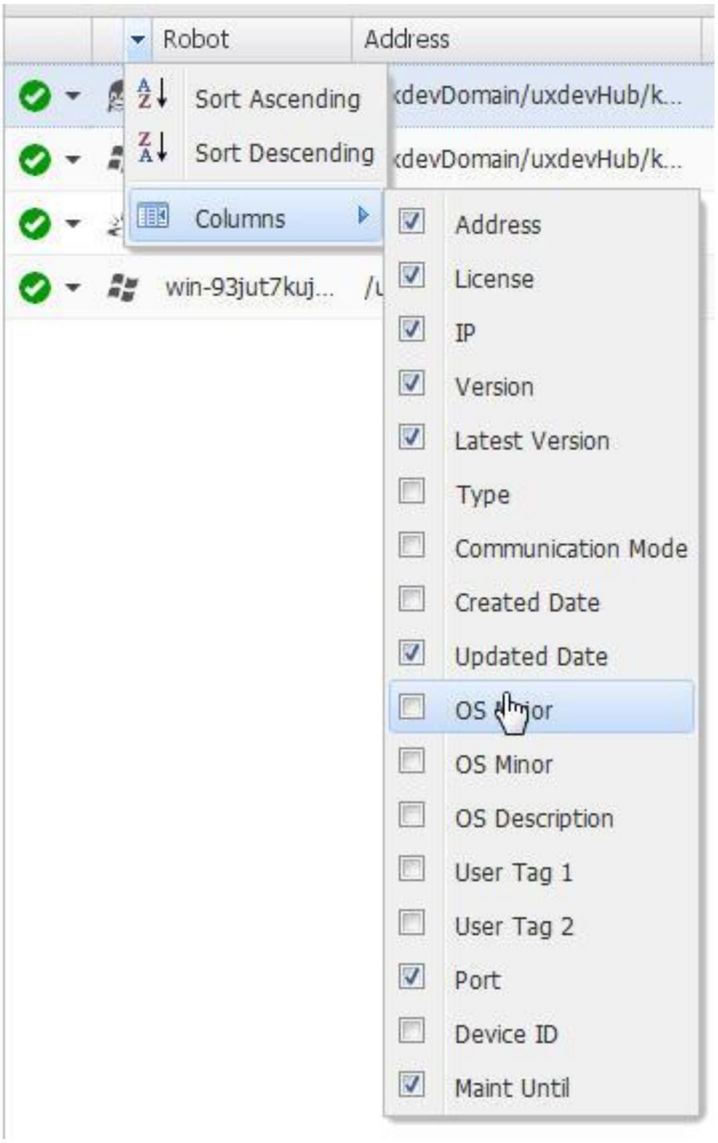
Operating system of the robot.

How to Modify Robot Properties View

Follow these steps:

1. In the right pane, click the arrow next to a column heading.
2. Click **Columns**.

   A list of the available columns appears.



☑ Address
☑ License
☑ IP
☑ Version
☑ Latest Version
□ Type
□ Communication Mode
□ Created Date
☑ Updated Date
□ OS Major
□ OS Minor
□ OS Description
□ User Tag 1
□ User Tag 2
☑ Port
□ Device ID
☑ Maint Until

3. Select the checkbox next to every column you want to display.

Robot Property Fields

Robot

Name of the robot.

Type

Type of robot.

Address

Path to the robot in /<domain name>/<hub name>/<robot name> format.

License

True or False - Indicates if the license is current for the robot.

IP

IP address of the robot.

Version

Version number of the robot.

Latest Version

Latest version of the robot.

Communication Mode

How the robot communications with the hub. The robot can be in one of three modes: passive, normal or none.

Created Date

Date the robot was created.

Updated Date

Date the robot was updated.

User Tag 1

User defined field.

User Tag 2

User defined field.

Port

Port number for the robot. Default is 48000.

Maint Until

Date the robot is scheduled to be returned to active status from maintenance mode.

Note: This field only applies to robots that are placed in maintenance mode.

OS Major

Operating system the robot is installed on.

OS Minor

Version of the operating system running on the robot.

OS Description

Brief description of the operating system. Example: Service Pack 1.

Processor

Processor on the machine.

Started Time

Time the robot was started.

Robot Time

Time at the point you selected the robot properties.

Robot Time Zone

Time zone where the robot system resides.

Probes

This screen displays the probes installed on the robot and is used as the starting point for configuring your probes. The icon next to the probe name provides a drop-down menu with tasks related to the probe. The menu includes:

- Activate
- Deactivate
- Restart
- Delete
- Configure
- Raw Configure
- Probe Utility
- View Log

These tasks are covered in the section on General Probe Configuration (see page 43).

Installed Packages

This screen displays the packages installed on your robot.

The fields are:

Package

Package installed on this robot.

Version

Version number of the installed package.

Build Number

Build number for the package.

Sections

Target platforms for the package.

Install Date

Date the package was installed on the robot.

Environment Variables

This screen displays the environment variables applicable to your robot. This list changes based on the operating system and probes installed on your robot.

Archive Interface Overview

This section describes the local archive, web archive, and distribution activities for the probes on your NMS system.

Local Archive

This screen displays the probes that reside in your local archive. This archive resides on the hub, therefore the list will be the same for all robots connected to the hub. The archive lists the packages that have been downloaded to the local archive along with the version, category, description, and link to the release notes. There can be more than one version of a package on the local archive.

If a newer version of the package exists on the web archive, an update button (⟳) is displayed on the right side of the screen.

You can deploy, import, group, and delete probe packages from this screen. See the section titled Deploy Probes Using Admin Console (see page 39) for more information.

Web Archive

This screen displays the list of probe packages on the Nimsoft support archive. You must have a valid login and password for the Nimsoft support site to download any package. See How to Connect to the Web Archive (see page 16) section for more information.

The archive lists the packages that are currently available for downloading, along with the version, category, description, and link to the release notes.

How to Connect to the Web Archive

Follow these steps:

1. Click the **Archive** button at the top of the Admin Console window.
2. Select the **Web Archive** button on the robot archive screen.
3. Click the key (🔑) icon.
4. Enter your username and password for the Nimsoft support site.
5. Click **Save**.

Distribution Activity

This screen displays a log of your probe package distributions along with the status of each distribution. Your packages can be deployed individually or in groups.

Chapter 2: Manage Licenses

This section describes how to manage your probe licenses. These procedures are typically performed by an NMS Administrator. The robot licenses are managed from the Settings button in the upper-right corner of the Admin Console screen. The hub licenses are managed by clicking the Configure Hub (⚙) icon next to the hub name in the navigation pane.

This section contains the following topics:

How to Add a Hub License

Follow these steps:

1. Log in to the Admin Console.
2. Click the **Configure Hub** (⚙) icon.
3. Cut and paste the hub license into the license field.
4. Click **Save**.

   The hub will need to restart to update the license information.
5. Click **Yes**.

How to View Robot Licenses

Follow these steps:

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down menu appears.
3. Select **Manage Licenses**.

   A Manage Licenses screen appears and contains a list of the probe licenses on your NMS system.

License Property Fields

This screen displays the fields listed below. You can customize the columns that appear by selecting the arrow next to any column heading and right-click. A drop-down menu displays which allows you to sort ascending, sort descending or select the columns to display.

Product

Name of the probe.

Info

License description.

Expiration Date

Date the license expires.

IP

IP mask used to limit the systems the probe is licensed to run on. An * indicates the probe is licensed to run on all systems in this domain.

Number

Number of licenses for the probe package.

Code

Valid license code for the probe.

How to Add a License

Follow these steps:

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down menu appears.
3. Select **Manage Licenses**.

   A Manage Licenses screen appears and contains a list of the probe licenses on your NMS system.
4. Click the **Add** button.

   The Add Licenses screen appears.
5. Click in the window and cut and paste the license key from the email you received from the support team.

How to Delete a License

Follow these steps:

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down menu appears.
3. Select **Manage Licenses**.

   A Manage Licenses screen appears and contains a list of the probe licenses on your NMS system.
4. Select the check box next to the probe license you want to delete.
5. Click the **Delete** button.

   A confirmation message appears.
6. Click **OK** to delete the probe license.

   The screen refreshes and the deleted probe license is no longer in the list.

   Note: If the screen does not refresh, click the ⟳ (Refresh) button.

Chapter 3: Manage Users

This section describes how to manage NMS users. These procedures are typically performed by an NMS Administrator who has Administrator ACL permissions.

This section contains the following topics:

How to View User Properties (see page 21)
How to Add a New User (see page 23)
How to Delete a User (see page 23)
How to Modify a User (see page 24)

How to View User Properties

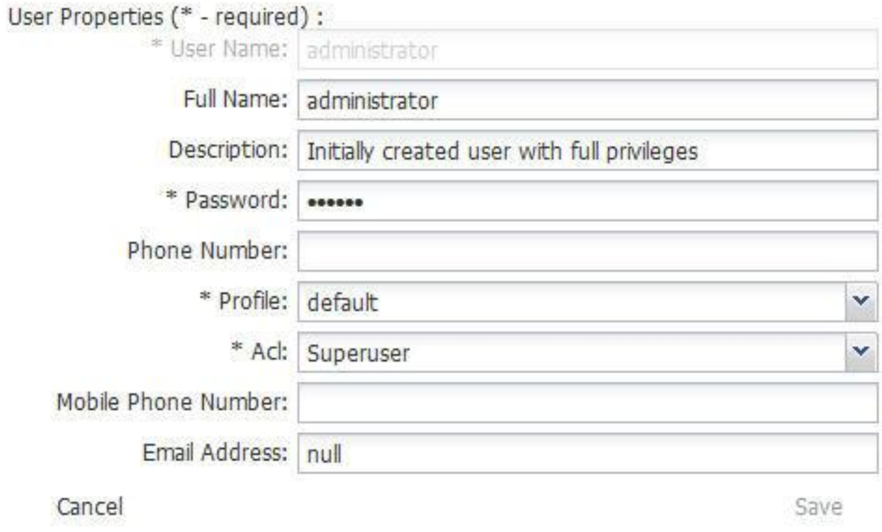
Follow these steps:

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down menu appears.
3. Select **Manage Users**.

   A Manage Users dialog box appears.
4. Select a user name in the left navigation pane.

   The right pane displays the properties for the selected user.



User Properties (* - required) :

* User Name: administrator
Full Name: administrator
Description: Initially created user with full privileges
* Password: ••••••
Phone Number:
* Profile: default
* Acl: Superuser
Mobile Phone Number:
Email Address: null

Fields with an * are required fields. See the User Property Fields (see page 22) section for a description of the fields. To refresh the user list, click **Refresh Users** in the upper left corner of the screen.

User Property Fields

The user property fields are:

User name

The NMS user name. This is a read-only field.

Full name

The full name for the NMS user.

Description

A brief description of the user.

Password

The password associated with the user name. Restrictions are: 6+ characters and cannot equal the user name.

Phone Number

The phone number for the NMS user.

Profile

The profile associated with the NMS user.

ACL

The access control list assigned to the NMS user.

Mobile Phone Number

The mobile phone number for the NMS user.

Email Address

The email address for the NMS user.

How to Add a New User

Follow these steps:

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down menu appears.
3. Select **Manage Users**.

   A Manage Users dialog box appears.
4. Click **New User**.
5. Complete the fields, then click **Save**.

   For field descriptions see the User Property Fields (see page 22) section.

How to Delete a User

Follow these steps:

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down menu appears.
3. Select **Manage Users**.

   A Manage Users dialog box appears.
4. Select a user in the navigation pane.
5. Click **Delete Selected**.

   A confirmation message appears.
6. Click **Yes** to delete the user.

How to Modify a User

Follow these steps:

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down menu appears.
3. Select **Manage Users**.

   A Manage Users dialog box appears.
4. Select the user you want to modify in the navigation pane.
5. Update the fields, then click **Save**.

Chapter 4: Manage Security

This section describes how to manage security for:

Admin Console

By default Admin Console communicates over unsecured HTTP. Admin Console can be configured to use HTTPS with a self-signed (system-generated) SSL certificate, or with a Certificate Authority-signed SSL Certificate.

Probes

When probes access other probes in the same domain, they do so at a defined security level. If a security level is not specified, the probe defaults to the lowest security level set. The lowest security level allows only very limited actions against other probes. Typically the probe security is set during probe installation.

You can also limit the computers a probe has access to by assigning a limited set of IP addresses. A wildcard (*) can be assigned, giving the probe general access rights to all computers within the domain.

This section contains the following topics:

Managing Security for Admin Console

Consult your network security engineers and compliance specialists regarding specific security requirements that impact your use of Admin Console. In general, industry-standard security requirements mandate the use of SSL encryption for client-server communications via an untrusted network. This includes the following situations:

- If users access Admin Console 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.

The service_host probe contains the Admin Console application. Configuring security for Admin Console is done by setting security parameters in the service_host probe GUI.

By default, service_host uses the unsecured HTTP protocol to send information a browser window or UMP portlet. To use HTTPS for secure communications, set service_host to use HTTPS for secure data transport. You must also configure the use of an SSL certificate, either self-signed, or CA (Certificate Authority) -signed, to enable authentication.

- The system makes a self-signed 2048 bit certificate available by default. If this meets your requirements then no additional configuration is required. The system can also generate lower or higher bit level certificates, such as 1024, 3078, or 4096 bit.

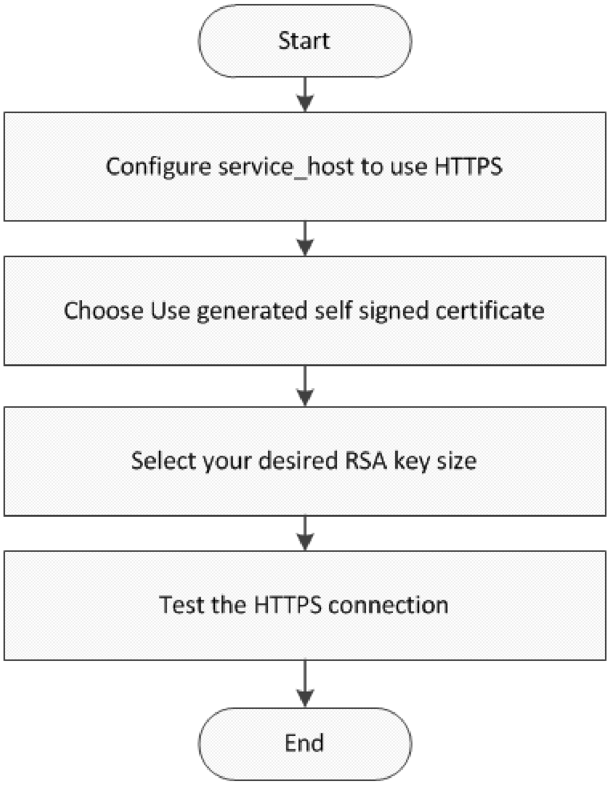
  Note: For high-security environments, it is recommended that you use at least 2048 bit encryption. However, bear in mind that longer RSA key-lengths significantly affect the speed of encryption, and of decryption in particular.

- If you require a CA-signed certificate, you must obtain that certificate from a certificate authority.Your business, institution, or organization may already have CA-signed certificate(s) on hand that can be used.

This section contains the following topics:

Implement a Self-Signed SSL Certificate

This section provides instructions for configuring Admin Console to use a self-signed SSL certificate. Here are the high-level steps involved.


Start
Configure service_host to use HTTPS
Choose Use generated self signed certificate
Select your desired RSA key size
Test the HTTPS connection
End

The steps in the above drawing correspond to the steps in the following section, Self-Signed Certificate Procedure (see page 27).

Self-Signed Certificate Procedure

This section describes how to configure service_host to use HTTPS-Secure communications with Admin Console. When these changes take effect, a self-signed certificate is automatically generated and stored in the service_host.keystore.

Follow these steps:

1. Configure service_host to use HTTPS.
    a. Open Admin Console.
    b. Navigate to the server running NMS, and locate the service_host probe.
    c. Open the probe configuration GUI for service_host by clicking the icon next to the probe, then selecting **Configure** from the pop-menu that displays.

   d. Navigate to the section labeled **Tomcat Server**.

   e. Select **HTTPS - Secure** under **Transport Guarantee**.

   f. Unless you have a need to modify Port, Connection Timeout(ms), or Maximum number of request threads, leave these set to their defaults.

2. Choose **Use generated self-signed certificate** under **SSL Certificate**.

3. Select your desired RSA key size **(RSA key size (bits))** from the drop-down menu:

   - 2048 bit is the default
   - 1024 bit is less secure but allows encryption and decryption to run faster
   - 3072 and 4096 bit options are more secure, but run slower, particularly decryption.

   Click **Save.** A self-signed certificate is generated and stored in the ssl.keystore file, and service_host is configured to use the certificate.

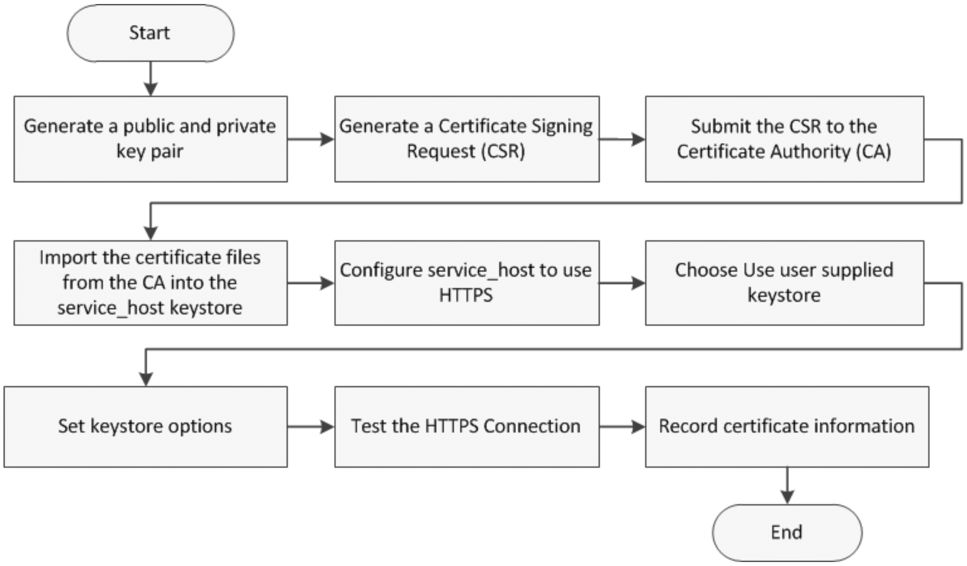
   Note: The automatically-generated SSL certificate has a validity period of one year.

4. Test the HTTPS connection:

   1. Verify that Admin Console is now using HTTPS.
   2. Click the lock icon to the left of the URL in the browser address window to view information about the connection. The browser may display a warning about self-signed certificates being unsecure. Communication is encrypted, however.
   3. The service_host probe is now configured to use SSL with a self-signed certificate of your selected key size.

Implement a Certificate Authority-Signed SSL Certificate

This section provides instructions for configuring Admin Console to use an SSL certificate signed by a Certificate Authority (CA). Here are the high-level steps involved.


Start
Generate a public and private key pair
Generate a Certificate Signing Request (CSR)
Submit the CSR to the Certificate Authority (CA)
Import the certificate files from the CA into the service_host keystore
Configure service_host to use HTTPS
Choose Use user supplied keystore
Set keystore options
Test the HTTPS Connection
Record certificate information
End

The steps in the above drawing correspond to the steps in the section CA-Signed Certificate Procedure (see page 30).

Note: Before using this scenario, ensure that you meet the following prerequisites:

- Your environment is configured to run keytool commands. This means that the $PATH system variable includes a path to java.exe and keytool.
- You are familiar with public key infrastructure (PKI) and system administration.

CA-Signed SSL Certificate Procedure

This section describes how to configure service_host to use HTTPS-Secure communications with a CA-issued SSL certificate.

Follow these steps:

1. Generate the public and private key pair with the key size you require:

   ```
   <Java_installation>/bin/keytool -genkeypair -alias
   <user_specified> -keyalg RSA -keysize <key_size> -keystore
   <user_specified> -validity <days_cert_is_valid>
   ```

   Note that <user_specified> can be whatever you choose.

   a. When prompted for first and last name, enter the FQDN

   b. When prompted, provide entries for the following

      a. Organizational unit

      b. Organization

      c. City or Locality

      d. State or Province

      e. Two-letter country code

   Confirm that the information entered is correct.

2. Generate a Certificate Signing Request (CSR)

   ```
   <Java_installation>/bin/keytool -certreq -alias <whatever
   alias you choose> -validity <days_cert_is_valid> -keystore
   <whatever keystore file you chose>  -file <your_domain>.csr
   ```

3. Submit the CSR to the Certificate Authority (CA)

   a. Paste the CSR into the web form of the CA

   b. Remove any characters before

      ----BEGIN CERTIFICATE REQUEST

         and after

      END CERTIFICATE REQUEST----

4. Import the certificate files from the CA into the keystore file that is being used

Note: All keystore entries must use a unique alias. You can specify what alias to use in the service_host GUI. If your CA provides multiple intermediate certificates, each intermediate certificate must also use a unique alias.

a. If your CA provided a root certificate, import the root certificate

```
< Java_installation>/bin/keytool -import -trustcacerts -alias
<root_certificate_alias> -file  <root_certificate>.cer
-keystore <the keystore file in use>
```

b. Import the first intermediate certificate

```
<Java_installation>bin/keytool -import -trustcacerts -alias
<first_intermediate_certificate_alias> -file
<first_intermediate_certificate>.cer -keystore <the keystore
file in use>
```

c. Repeat the previous step for each additional intermediate certificate

d. Import the signed certificate. This is the entity certificate if you received a chained certificate

```
<Java_installation>bin/keytool -import -trustcacerts -alias
<whatever alias is chosen> -file <your_domain>.crt –keystore
<the keystore in use>
```

5. Configure service_host to use HTTPS

   a. Open Admin Console

   b. Navigate to the server running NMS, and locate the service_host probe

   c. Open probe configuration GUI for service_host by clicking the icon next to the probe, then selecting **Configure** from the pop-menu that displays

   d. Navigate to the section labeled **Tomcat Server**

   e. Select **HTTPS - Secure** under **Transport Guarantee**

   f. Unless you have a need to modify Port, Connection Timeout(ms), or Maximum number of request threads, leave these set to their defaults.

6. Choose **Use user supplied certificate** under **SSL Certificate**

7. Set keystore options

   Note: Your certificate must be stored in a keystore file in a format supported by service_host (formats include, but are not limited to, Java Keystore (JKS) and PKCS12).

   - **Keystore file ***: Provide the path to the location of the keystore file. This can be an absolute path, or a path relative to the probes/service/service_host directory
   - **Keystore type ***: Specify the type of keystore. These are supported types: JKS, PKCS12 (case sensitive). Default is JKS
   - **Keystore password ***: Provide the keystore password

    - Key alias: Provide a key alias, if your keystore contains multiple certificates and you need to use a specific one. If not provided, the first certificate found is used
    - Key password: Specify the password that allows access to the key alias. If not given, the keystore password is used. Note that it is common for keystores to be created with a single password that allows access to the store itself, as well as the key, or keys, inside the store.

   Click **Save** to configure service_host to use the CA-issued certificate, or **Discard** these settings.

8. Test the HTTPS connection:
   a. Verify that Admin Console is now using HTTPS
   b. Click the lock icon to the left of the URL in the browser address window to view information about the connection.
9. Record certificate information:
   a. Ensure that you record the validity period you set for the certificate
   b. Back up the certificate files to a secure location
   c. Make a record of your passwords.

The service_host probe is now configured to use your CA-issued SSL certificate.

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.

View Root Certificates

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 NMS.
2. Change directories as follows:
   ```
   cd <NMS_installation>/jre/<jre_version>/lib/security
   ```
3. Issue the following command:
   ```
   <NMS_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.

Additional Resources

In addition to the appendix Troubleshooting SSL Certificates, the following websites provide helpful tools and resources for setting up and managing SSL certificates:

- http://docs.oracle.com/javase/1.5.0/docs/tooldocs/windows/keytool.html
- www.sslshopper.com

Managing Security for Probes

This section contains the following topics:

This section describes how to manage security for probes.

How to View Probe Security Settings

Follow this procedure to view a list of the probes installed on your system and their respective access permissions.

Follow these steps:

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down menu appears.
3. Select **Probe Security**.

   The Probe Security screen appears. See the Probe Security Access Fields (see page 34) section for more information.

Probe Security Access Fields

The probe security access fields are:

Probe

Name of the probe.

Access

Access permissions.

IP Mask

IP addresses of systems the probe is allowed to access. This field allows for the use of regular expressions. A wildcard (*) in this field allows access to all systems within the domain.

How to Assign Probe Security Access to a Probe

Use this procedure when a probe has not been assigned access permissions. If the probe already has access permissions see How to Modify Probe Security Access Levels (see page 35).

Follow these steps:

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down menu appears.
3. Select **Probe Security**.

   The Probe Security screen appears.
4. Click the **New** button.

   A pop-up dialog box appears.
5. Select the probe name from the drop-down menu.

   Note: Only probe names without access permissions will be listed in this drop-down menu.
6. Select the appropriate Access permissions from the drop-down menu.
7. Click the **Create** button.

   The security access permissions are now assigned to the probe.

How to Modify Probe Security Access Levels

Follow these steps:

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down menu appears.
3. Select **Probe Security**.

   The Probe Security screen appears.
4. Click on the access level next to the probe you want to modify.

   The field refreshes and a drop-down menu button appears.
5. Click the drop-down arrow and select the appropriate access level.

   The screen refreshes with the new access level assigned to the probe.

How to Delete Probe Security Access Levels

Follow these steps:

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down menu appears.
3. Select **Probe Security**.

   The Probe Security screen appears.
4. Select the checkbox next to the probe you want to delete the security access.
5. Click the **Delete** button.

   A confirmation message appears,
6. Click **OK**.

   The screen refreshes and the probe has been removed from the list.

Chapter 5: Download Probes from Web Archive

Use this section to connect to the web archive and download probes.

This section contains the following topics:

How to Connect to the Web Archive

Follow these steps:

1. Click the **Archive** button at the top of the Admin Console window.
2. Select the **Web Archive** button on the robot archive screen.
3. Click the key (🔑) icon.
4. Enter your username and password for the Nimsoft support site.
5. Click **Save**.

How to Download a Probe

Follow these steps:

1. Click the **Archive** button at the top of the Admin Console window.
2. Click **Web Archive**.
3. Select the check box next to the probe you want to download.
4. Click **Download**.

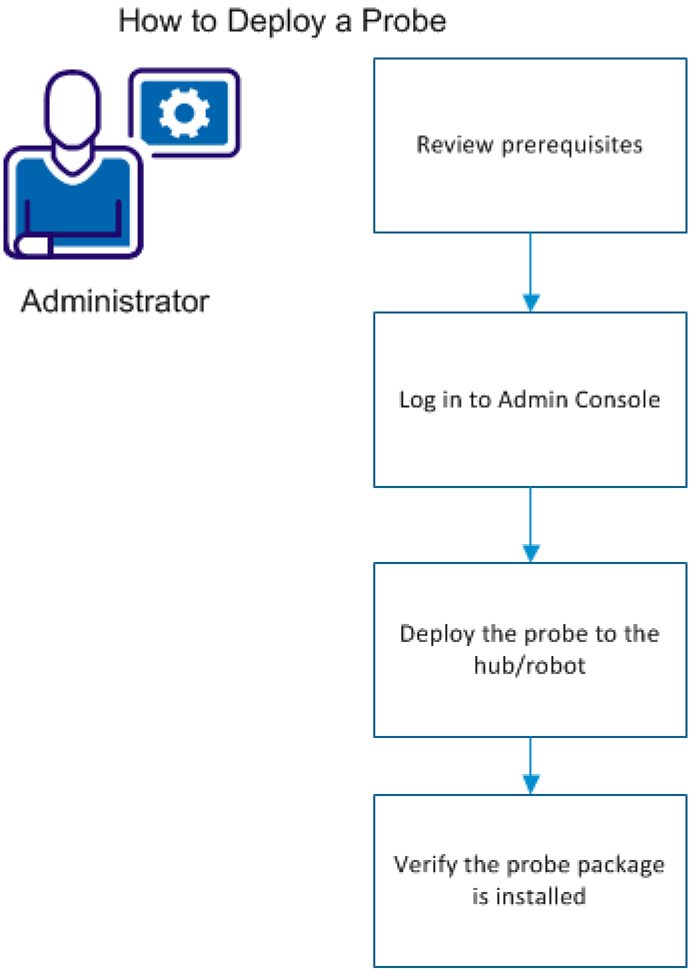
   You will receive a confirmation message.

   Note:If your credentials are not entered you will receive an error message. See the How to Connect to the Web Archive (see page 16) section for more information.
5. Click **Yes**.

The probe package is downloaded to your local archive.

Chapter 6: Deploy Probes Using Admin Console

As a Nimsoft Monitor System (NMS) Administrator, you deploy probes using the Admin Console application. The NMS uses probes to monitor your system, send alarms and provide dashboards that display the status of your system. After deploying a probe you will need to configure the probe for your specific monitoring requirements.



This section contains the following topics:

Review Probe Prerequisites

The administrator reviews the prerequisites for each probe before they deploy the probe to a hub or robot. Reviewing this information enables the administrator to foresee environmental issues so probe deployment occurs smoothly. The probe prerequisite information can be found in the individual probe release notes and configuration document.

Log in to Admin Console

Admin Console can be accessed either through a standalone web page or through UMP. The procedure for accessing your Admin Console application depends on the version of the Admin Console installed on your system.

Log in to Admin Console in UMP

Follow these steps:

1. Connect to your UMP application in a web browser.
2. Enter a valid Nimsoft user name and password.

   The CA Nimsoft Unified Management Portal opens to the USM portlet.
3. Click the Admin Console tab.

   Note: If the Admin Console tab is not available, see the Add Portlets (see page 8) section to add this portlet.

   The Admin Console screen appears.

Your NMS system is available for configuration.

Note: If you are accessing Admin Console over a secure HTTPS connection with a self-signed SSL certificate, and you cannot view it in UMP, then you need to open Admin Console in the standalone web page. After opening the standalone version of Admin Console, a message indicating that the security certificate is not trusted displays--click **Proceed anyway**. This only provides a temporary work around. If you close your browser and then go back to the Admin Console application you will need to accept the certificate again.

Log in to Admin Console in a Standalone Web Page

Follow these steps:

1. Enter https://<service_host>:8443/adminconsole in your web browser window.

   Note: <service_host> is the system where the service_host probe is installed.
2. Enter a valid NMS username and password.

   The Admin Console application opens.

Deploy a Probe to the Hub/Robot

Follow these steps:

1. Click the **Archive** button at the top of the Admin Console window.
2. Click **Local Archive** or **Web Archive**.

   Note: If the probe is not listed in the local archive and you deploy from the Web Archive, the probe will be download to your local archive.
3. Click the arrow button next to the hub name in the navigation pane to display the robots on the hub.
4. Select the check box(es) next to the name of the targeted robot(s) in the navigation pane.

   The right pane displays the probes available on the archive you selected above.
5. Select the check box(es) next to the name of the probe(s) you want to deploy.
6. Click the **Deploy** button at the top of the probe listing.

   You will receive a confirmation message.
7. Click **OK** to deploy the probe to the selected robot.

Verify the Probe Package Deployed

Follow these steps:

1. Click the **Infrastructure** button at the top of the Admin Console screen.
2. Select the name of the robot where you deployed the probe.
3. Select the **Probes** button at the top of the right pane.

   The probe should be listed in the right pane.

The probe is now ready for you to configure.

Chapter 7: General Probe Configuration

This section describes the general probe administration tasks you can perform in the Admin Console application. For specific probe configuration information, see the individual probe configuration documents included in the Admin Console Probe Catalog.

This section contains the following topics:

How to Activate a Probe

Use this procedure to activate a probe that has been deactivated.

Follow these steps:

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane.

   You may have to expand the navigation tree to see the robot.
3. Click on the icon next to the probe name.

   A pop-up menu displays.
4. Select **Activate**.

   The probe will be activated.

How to Deactivate a Probe

Follow these steps:

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane.

   You may have to expand the navigation tree to see the robot.
3. Click on the icon next to the probe name.

   A pop-up menu displays.
4. Select **Deactivate**.

   The probe will be deactivated.

How to Restart a Probe

Follow these steps:

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane.

   You may have to expand the navigation tree to see the robot.
3. Click on the icon next to the probe name.

   A pop-up menu displays.
4. Select **Restart**.

   The probe will be restarted.

How to Delete a Probe

Follow these steps:

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane.

   You may have to expand the navigation tree to see the robot.
3. Click on the icon next to the probe name.

   A pop-up menu displays.
4. Select **Delete**.

   The probe will be removed from the robot.

How to Configure a Probe

The probe must be running in order

Follow these steps:

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane.

   You may have to expand the navigation tree to see the robot.
3. Click on the icon next to the probe name.

   A pop-up menu displays.
4. Select **Configure**.

   The configuration GUI for the probe appears. Refer to the specific probe documentation for more information on probe configuration.

Raw Configure Utility

Many probes have their own custom configuration utility. For those that do not, Admin Console presents the probe configuration data in an editor similar to regedit.

Raw configure lets you add, delete and modify the nodes in the configuration file, as well as the variable name/value elements.

Note: You can use this method for any probe.

How to Use Raw Configure

Follow these steps:

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane.

   You may have to expand the navigation tree to see the robot.
3. Click on the icon next to the probe name.

   A pop-up menu displays.
4. Select **Raw Configure**.

   The Raw Configure screen appears.

Probe Utility

The Probe utility allows you run the selected probe's command set and watch the output in the right pane. This is useful for debugging purposes.

How to Use Probe Utility

Follow these steps:

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane.

   You may have to expand the navigation tree to see the robot.
3. Click on the icon next to the probe name.

   A pop-up menu displays.
4. Select **Probe Utility**.

   The probe utility screen appears.
5. Select a command from the drop down menu, then click the **green arrow** button to execute the command.

   The results are displayed in the right pane.

Probe Log Files

Each probe has a log file. This file contains information on the probe and is used for debugging purposes. A default of 500 lines displays in the Log viewer window. You can set this value to any number between 100 and 10,000 lines.

How to View a Probe Log File

Follow these steps:

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane.

   You may have to expand the navigation tree to see the robot.
3. Click on the icon next to the probe name.

   A pop-up menu displays.
4. Select **View Log**.

   The Log Viewer screen appears.

How to Download a Log File

Follow these steps:

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane.

   You may have to expand the navigation tree to see the robot.
3. Click on the icon next to the probe name.

   A pop-up menu displays.
4. Select **View Log**.

   The Log Viewer screen appears.
5. Select the **Download Log** (📥) icon to start the download.

How to Clear a Log File

Follow these steps:

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane.

   You may have to expand the navigation tree to see the robot.
3. Click on the icon next to the probe name.

   A pop-up menu displays.
4. Select **View Log**.

   The Log Viewer screen appears.
5. Click the **Clear** () icon to clear the contents of the log file.

Appendix A: Troubleshooting SSL Certificates

This section provides information to help you troubleshoot issues implementing SSL with Admin Console.

This section contains the following topics:

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 service_host.
2. Issue this command in the same directory as the service_host probe, typically <NMS_*installation*>/probes/service/service_host
   ```
   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 CA issued a *chained* certificate, but the intermediate certificate(s) was not uploaded. You must upload the entity certificate *and* any intermediate certificates your CA provides.

Issue this keytool command in the same directory as your keystore, typically <*NMS_installation*>/probes/service/service_host

```
<NMS_installation>/jre/<jre_version>/bin/keytool -import -keystore
<user keystore file> -trustcacerts -file <intermediate_cert>.CER
-alias <chosen alias>
```

Note: All keystore entries must use a unique alias. If your CA provides multiple intermediate certificates, each intermediate certificate must also use a unique alias.

See the section Entity, Intermediate, and Root Certificates (see page 32) for additional information.