# Citrix SCOM Management Pack for NetScaler User Guide

**Software version: 1.14**

**Release date: March 2016**

This document provides installation, configuration, and usage instructions for Citrix SCOM Management Pack for NetScaler.

## Legal notices

Citrix, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309
United States of America

**Disclaimers**

This document is furnished "AS IS." Citrix, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix, Inc. and its licensors, and are furnished under a license from Citrix, Inc.

Citrix Systems, Inc., the Citrix logo, and NetScaler are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark office and in other countries. All other trademarks and registered trademarks are property of their respective owners.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

**Trademarks**

Citrix®
NetScaler®
Microsoft®
Windows®

# Contents

# Chapter 1: Quick introduction

## About NetScaler Management Pack

Citrix SCOM Management Pack for NetScaler (**NetScaler Management Pack**) is an availability and performance management solution that extends end-to-end service monitoring capabilities of Microsoft System Center Operations Manager (**SCOM**) to include the Citrix NetScaler (**NetScaler**) infrastructure. It fully integrates topology, health, and performance data into SCOM, providing an end-to-end operations overview across the entire NetScaler estate and enabling delivery of effective business service management.

Some key benefits of NetScaler Management Pack are:

- Agentless monitoring architecture
- Intuitive topology discovery of internal NetScaler components
- Deep monitoring of key virtual servers and services
- Enhanced infrastructure health
- Quick deployment and simple upgrades
- Functioning across physical and virtual NetScaler appliances
- Easy identification and resolution of network-specific issues
- Acceleration of problem resolution
- Scaling management responsibility across your infrastructure and organization
- Automation of routine administration to improve service levels, increase efficiencies, and achieve greater control of the IT environment

### *Topology discovery*

NetScaler Management Pack provides out-of-the-box discovery of the NetScaler configuration:

- Automatically discovers and visualizes the topology of NetScaler devices. The discovery and visualization are based on a defined NetScaler device model. The discovered devices are used as a base for NetScaler component discovery.
- Maintains NetScaler topology while you add or remove devices and their components.

Discovered NetScaler appliance objects are divided into the following major components:

- System

  Shows system settings as well as licensed functionalities on NetScaler and memory pools.
- Network

  Provides details on IP addresses (IPv4 and IPv6), network interfaces, VLANs, channels, and bridge groups.
- Access Gateway

Displays AG virtual servers and related authentication policies.

- Traffic Management

  Contains Load Balancing group which includes LB virtual servers, as well as LB services and service groups.
- SSL

  Covers SSL entities, namely policies, actions, and certificates.
- Authentication Authorization Auditing

  Divides authentication servers into three groups: LDAP, Radius, and TACACS.
- Cloud Bridge

  Contains information about Network Bridges that are configured.

*Monitoring*

NetScaler Management Pack monitors many components out-of-the-box and is designed to be extendable to meet custom monitoring requirements. Some out-of-the-box monitoring capabilities are:

- Settings in detail, monitors per object as well as monitoring of configuration changes.
- Detection of unusual session behavior.
- Detection of NetScaler service failures.
- Identification of internal NetScaler issues and non-responding services.

Monitors are classified into the following groups:

- Appliance

  Includes hardware and system information monitoring:
  - CPU and memory usage
  - Temperature
  - Fan speed
  - Power supply
  - High availability node master state

  General statistics for:
  - Authentication, Authorization, and Auditing
  - Access Gateway
  - Protocols (IPv4, IPv6, SSL, TCP, UDP)

  Monitors the status of the Comtrade Management Pack for Citrix NetScaler license for the appliance.
- Access Gateway Virtual Servers

  Related to a specific virtual server and includes monitoring of:
  - State

    - Number of current users
    - Requests rate
    - Activity in terms of requests and responses
- Load Balancing

  Monitors health states for LB related objects including:
    - Virtual Server
    - Service
    - Service group
- Authentication

  Detects the number of authentication failures in a given time interval for the following authentication protocols:
    - LDAP
    - Radius
    - TACACS
- Network

  Network-related monitors show:
    - State change for interfaces and channels
    - IP address conflicts for both IPv4 and IPv6
- SSL

  SSL-specific monitors are used to monitor:
    - Impending SSL certificate expiry
    - Absence of SSL policy hits (no traffic to trigger the policy)

*Views*

NetScaler Management Pack provides various out-of-the-box views that present alerts, the health state, tasks, and performance.

There are a number of performance collection views:

- Appliance

  The NetScaler appliance is the target.
    - Authentication, Authorization, and Auditing (general)
    - Access Gateway VPN (general)
    - Application Firewall
    - Integrated Cache
    - Compression
    - NetScaler Configuration Changes

    - CPU
    - Disk
    - Memory
    - HTTP Protocol
    - IP Protocol
    - SSL Protocol
    - TCP Protocol
    - UDP Protocol
    - Temperature
- Network

  One of the network components is the target.
    - Channel
    - Interface
- Access Gateway

  The Access Gateway virtual server is the target.
- Load Balancing

  Load Balancing service is the target.
- SSL

  SSL policies or SSL actions are the target.

*Tasks*

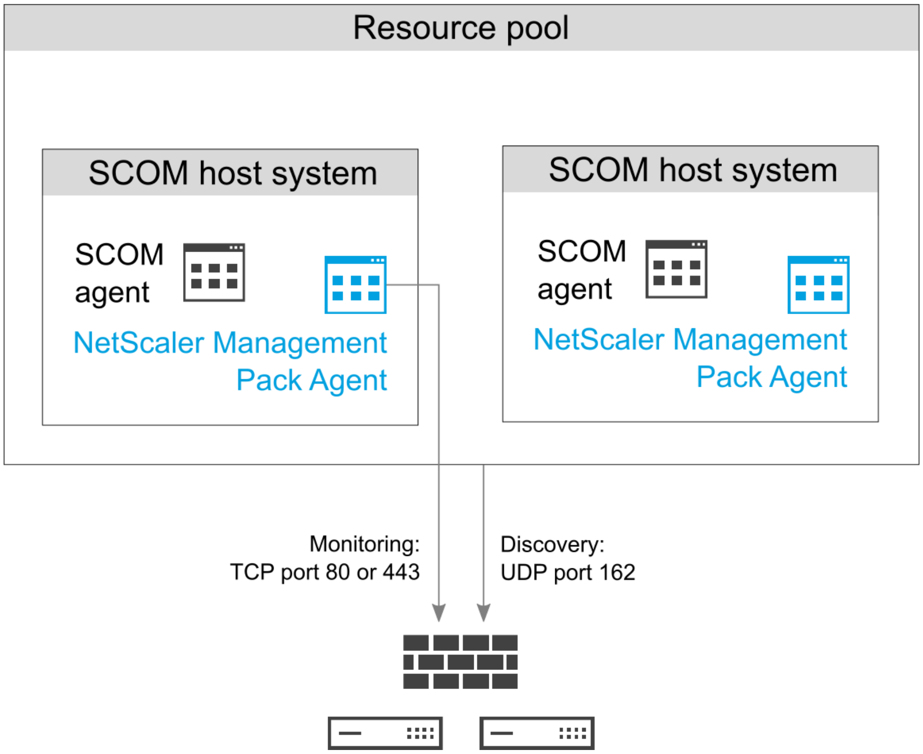
NetScaler Management Pack provides some tasks that can be easily extended:

- Displays all NetScaler events.
- Displays a current list of system sessions.
- Displays a current list of ICA connections.
- Displays all SSL virtual servers.

**Product architecture**

The following diagram shows how NetScaler Management Pack is deployed on SCOM management platform.

**Figure 1.1** NetScaler Management Pack deployment


Resource pool
SCOM host system
SCOM agent
NetScaler Management Pack Agent
SCOM host system
SCOM agent
NetScaler Management Pack Agent
Monitoring: TCP port 80 or 443
Discovery: UDP port 162

NetScaler Management Pack has two main parts:

- Server side (installed on one computer out of management server computers in the SCOM management group)

  The server side of the product contains management packs as well as agent installation packages. When management packs are imported into SCOM, all network devices are targeted and NetScaler devices discovery is based on the network device OID value. Other discovery and monitoring processes use the agent to communicate with NetScaler devices.
- Agent side (installed on each member of the SCOM resource pool dedicated to NetScaler device monitoring)

  The agent is designed to act as a proxy and a data collector between SCOM and Citrix NetScaler environments. The agent uses connections to the NetScaler appliances and provides the caching mechanism for data. To access the NetScaler appliances (based on the NITRO API), the agent uses AJAX technology. The necessary credentials for accessing the NetScaler appliances are sent from SCOM.

# Chapter 2: Installation and configuration

This chapter contains instructions that you must follow to install and configure NetScaler Management Pack. Perform all procedures in the documented order of precedence.

### Preparing for the installation

Before installing NetScaler Management Pack, make sure the following prerequisites are fulfilled:

- You environment meets the hardware and software requirements.

  For software requirements, see the *Citrix SCOM Management Pack for NetScaler Compatibility Matrix*. For hardware and/or other requirements, see the *Citrix SCOM Management Pack for NetScaler Release Notes*.
- A SCOM management group is chosen for NetScaler monitoring. The computer that hosts the SCOM management server of this management group is referred to as **management server computer**.
- SCOM agent is installed on all the computers that host NetScaler, and these computers are configured as **agent nodes** in the management group.
- All NetScaler devices that are to be monitored are added as network devices to SCOM. For more information, see the How to Discover Network Devices in Operations Manager webpage.
- All computers in the SCOM resource pools that are dedicated to NetScaler device monitoring can access NetScaler devices through the HTTP/HTTPS port (80 or 443) (for monitoring) and through the UDB ports (161 and 162) (for discovery).
- The default management packs that the included management packs depend on are imported in SCOM:
  - `Data Warehouse Library`
  - `Health Library`
  - `Network Management Library`
  - `Performance Library`
  - `System Center Core Library`
  - `System Library`
  - `Windows Core Library`
  - `Windows Service Library`

**Note** If you accidentally delete any of the listed default management packs, you can import them back from the files in the SCOM installation directory.

### Configuring NetScaler for monitoring by NetScaler Management Pack

In order to access and communicate with NetScaler, NetScaler Management Pack needs a NetScaler user account with proper privileges. This step requires administrative access to NetScaler either through the SSH command-line interface (preferred) or through the NetScaler GUI. Depending on your choice, perform only one of the two procedures that follow.

*Set up the NetScaler Management Pack user account by using the NetScaler CLI*

To set up the user account through the NetScaler CLI, do the following (the assumption is that the user account name is `usrNetScalerMonitoring` and the command policy is `polNetScalerMonitoring`):

1. Log on to NetScaler with an existing administrator account and by using an SSH client, for example PuTTY.

2. Run the following command to create a new command policy with proper permissions for NetScaler monitoring:

   ```
   add system cmdPolicy polNetScalerMonitoring ALLOW
   (^show\s+system\s+\S+)|(^show\s+system\s+\S+\s+.*)|(^show\s+configstat
   us)|(^show\s+configstatus\s+.*)|(^shell\s+nsconmsg\s+-K\s+\S+\s+.*)
   ```

   For higher security, run the following command instead:

   ```
   add system cmdPolicy polNetScalerMonitoring ALLOW
   (^show\s+system\s+\S+)|(^show\s+system\s+\S+\s+.*)|(^show\s+configstat
   us)|(^show\s+configstatus\s (^shell\s+nsconmsg\s+-
   K\s+/var/nslog/newnslog\s+-d\s+consmsg\s+\|\s+grep\s+-
   E\s+'IP\s+address\s+conflict\|current\s+time')
   ```

3. Run the following command to verify existence and allowed actions of the *read-only* policy:

   ```
   show cmdPolicy read-only
   ```

   The command should generate an output similar to the following:

   ```
   Command policy: read-only       Action: ALLOW
   cmdspec: (^man.*)|(^show\s+(?!system)(?!configstatus)(?!ns
   ns\.conf)(?!ns savedconfig)(?!ns runningConfig)(?!gslb
   runningConfig)(?!audit messages)(?!techsupport).*)|(^stat.*)

   Done
   ```

   If the *read-only* policy  does not exist, create one with the previously listed permissions. To update the command policy, use the `set system cmdPolicy` command.

4. Run the following command to create a new system user:

   ```
   add system user usrNetScalerMonitoring
   ```

5. Run the following commands to associate the user with the command policies:

   ```
   bind system user usrNetScalerMonitoring read-only 1
   bind system user usrNetScalerMonitoring polNetScalerMonitoring 1
   ```

6. Run the following command to verify configuration of the user account:

   ```
   show system user usrNetScalerMonitoring
   ```

   The command should generate an output similar to the following:

   ```
   User name: usrNetScalerMonitoring
           Command Policy: read-only       Priority:1
           Command Policy: polNetScalerMonitoring   Priority:1
   Done
   ```

*Set up the NetScaler Management Pack user account by using the NetScaler GUI*

---

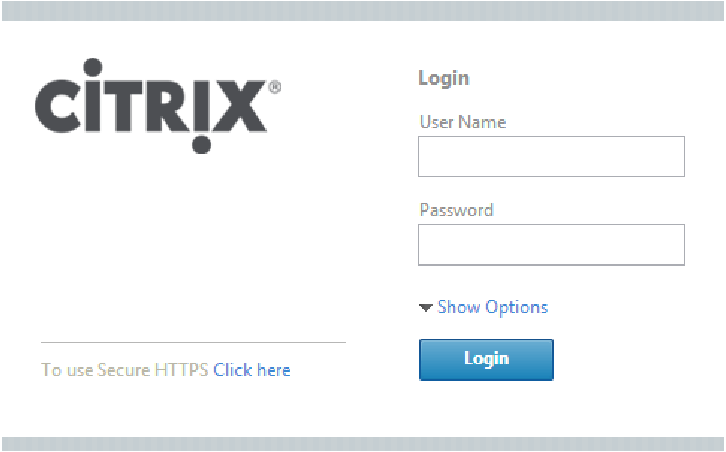
**Note:** The figures in this section reflect the GUI of NetScaler 10.1. The GUI appearance in other NetScaler versions may be different.

---

To set up the user account through the NetScaler GUI, do the following:

1. Launch a web browser and go to the NetScaler management host (host name or IP address). The login screen appears.

   **Figure 2.1** NetScaler login screen.



2. Log in with credentials of an existing administrator account.

3. In the NetScaler GUI, navigate to **Configuration > System > [ User Administration ] > Command Policies**.

4. Add a new command policy with the following command spec regular expression:

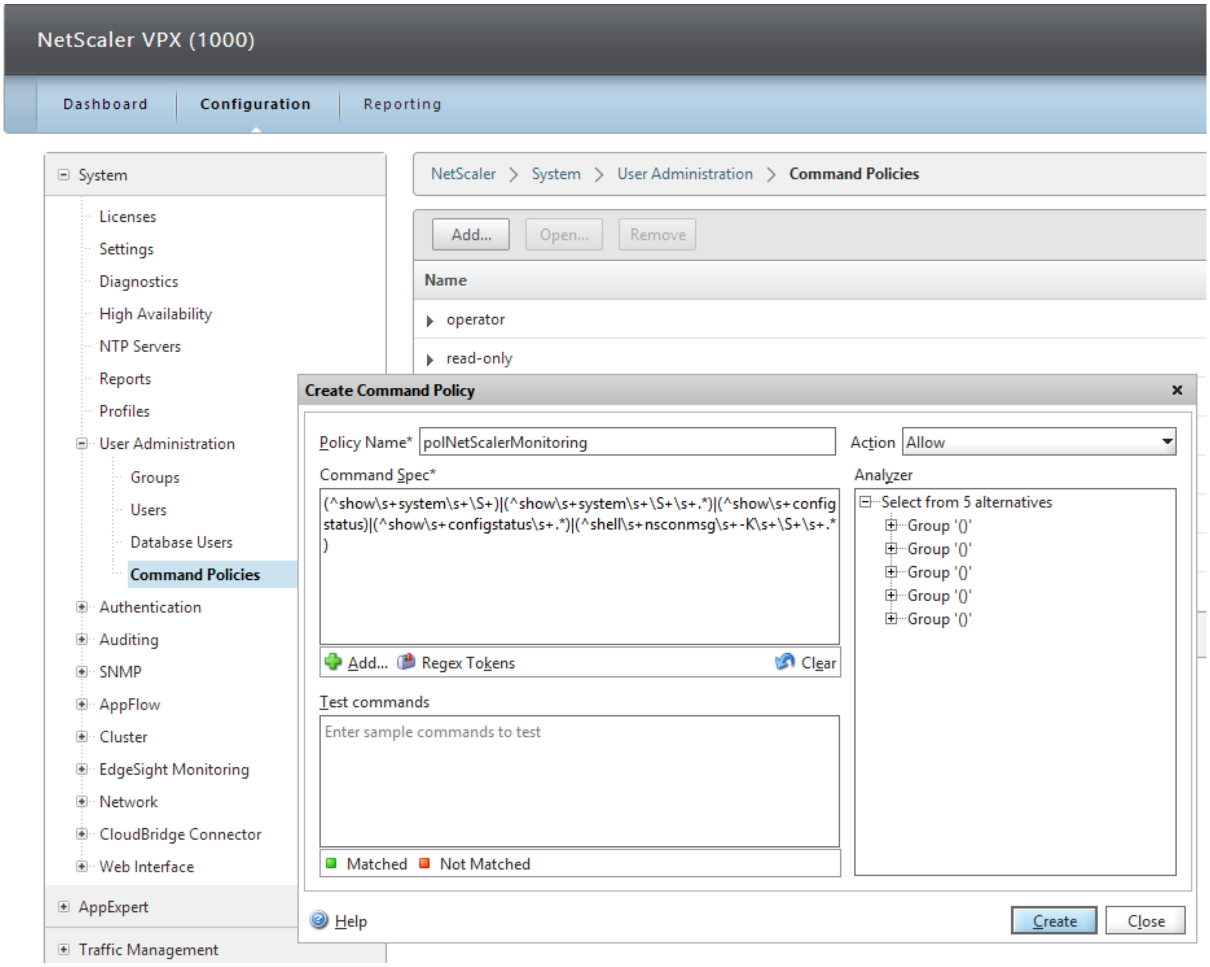
   ```
   (^show\s+system\s+\S+)|(^show\s+system\s+\S+\s+.*)|(^show\s+configstat
   us)|(^show\s+configstatus\s+.*)|(^shell\s+nsconmsg\s+-K\s+\S+\s+.*)
   ```

   For higher security, use the following regular expression:

   ```
   (^show\s+system\s+\S+)|(^show\s+system\s+\S+\s+.*)|(^show\s+configstat
   us)|(^show\s+configstatus\s+.*)|(^shell\s+nsconmsg\s+-
   K\s+/var/nslog/newnslog\s+-d\s+consmsg\s+\|\s+grep\s+-
   E\s+'IP\s+address\s+conflict\|current\s+time')
   ```

   This command policy grants permissions to execute some `show` commands as well as the `shell nsconmsg -K` command to access the console message log on the NetScaler. The permissions are read-only.

   **Figure 2.2** Creating a NetScaler command policy



Policy Name* polNetScalerMonitoring

Action Allow

Command Spec*

```
(^show\s+system\s+\S+)|(^show\s+system\s+\S+\s+.*)|(^show\s+config
status)|(^show\s+configstatus\s+.*)|(^shell\s+nsconmsg\s+-K\s+\S+\s+.*
)
```

5. Click **Create** to create the command policy.

6. Click **Close** to close the Create Command Policy dialog box.

> **Important:** Steps 7 to 13 apply only in case of a non-LDAP authentication. Steps 14 to 16 apply only in case of the LDAP authentication.

7. From the **System [User Administration]** menu select the **Users** node.

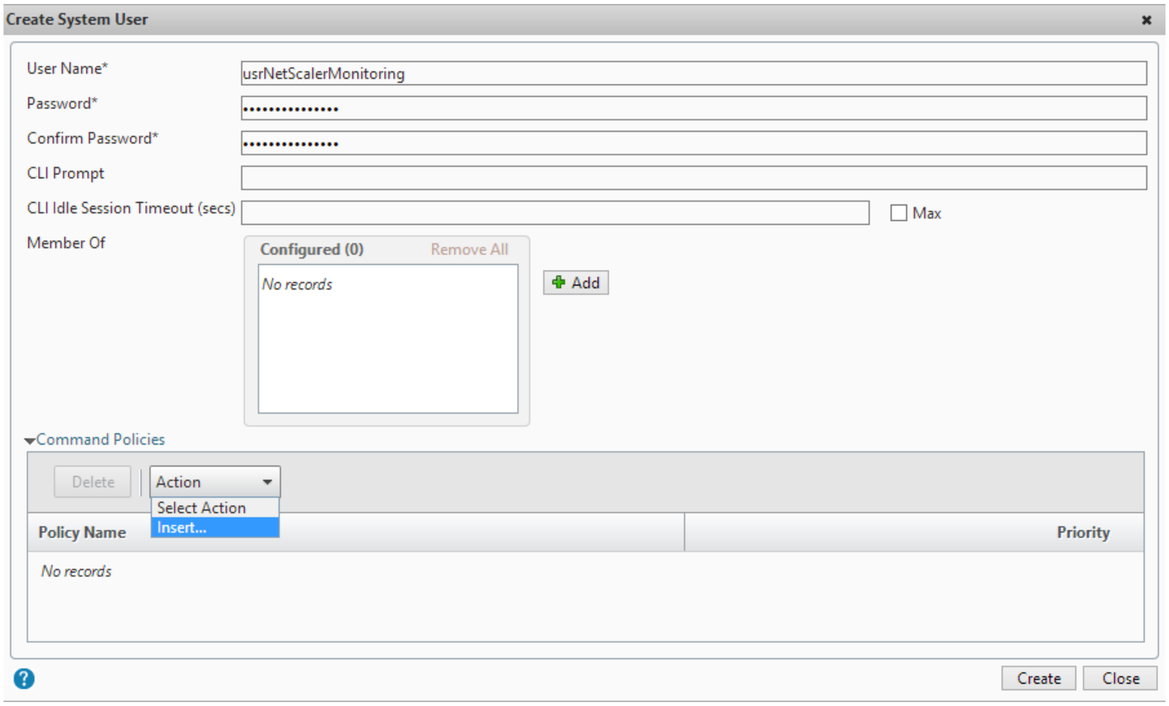
8. Click **Add** to open the Create System User dialog.

9. Type the user name and password for the user account.

10. In the Command Policies section, insert or select the command policy created in the previous steps as well as the read-only policy. The *read-only* command policy should be present in NetScaler by default. If the *read-only* policy is missing, go back to step 3, create the *read-only* command policy and allow the following permissions:

```
(^man.*)|(^show\s+(?!system)(?!configstatus)(?!ns ns\.conf)(?!ns
savedconfig)(?!ns runningConfig)(?!gslb runningConfig)(?!audit
messages)(?!techsupport).*)|(^stat.*)
```

**Figure 2.3** Creating a system user in NetScaler



Create System User

User Name* usrNetScalerMonitoring

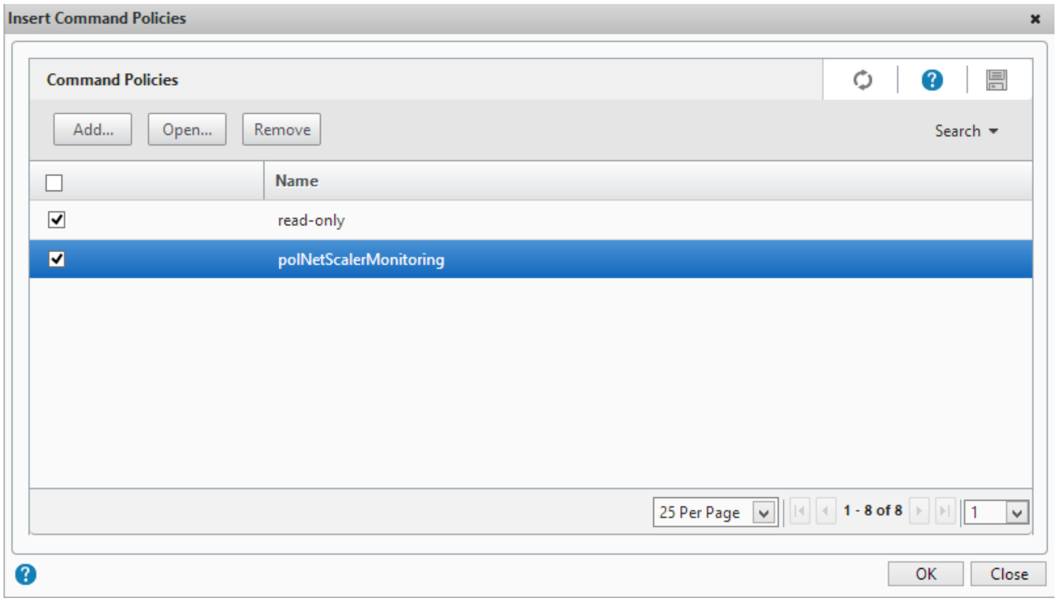
Password* •••••••••••••••

Confirm Password* •••••••••••••••

CLI Prompt

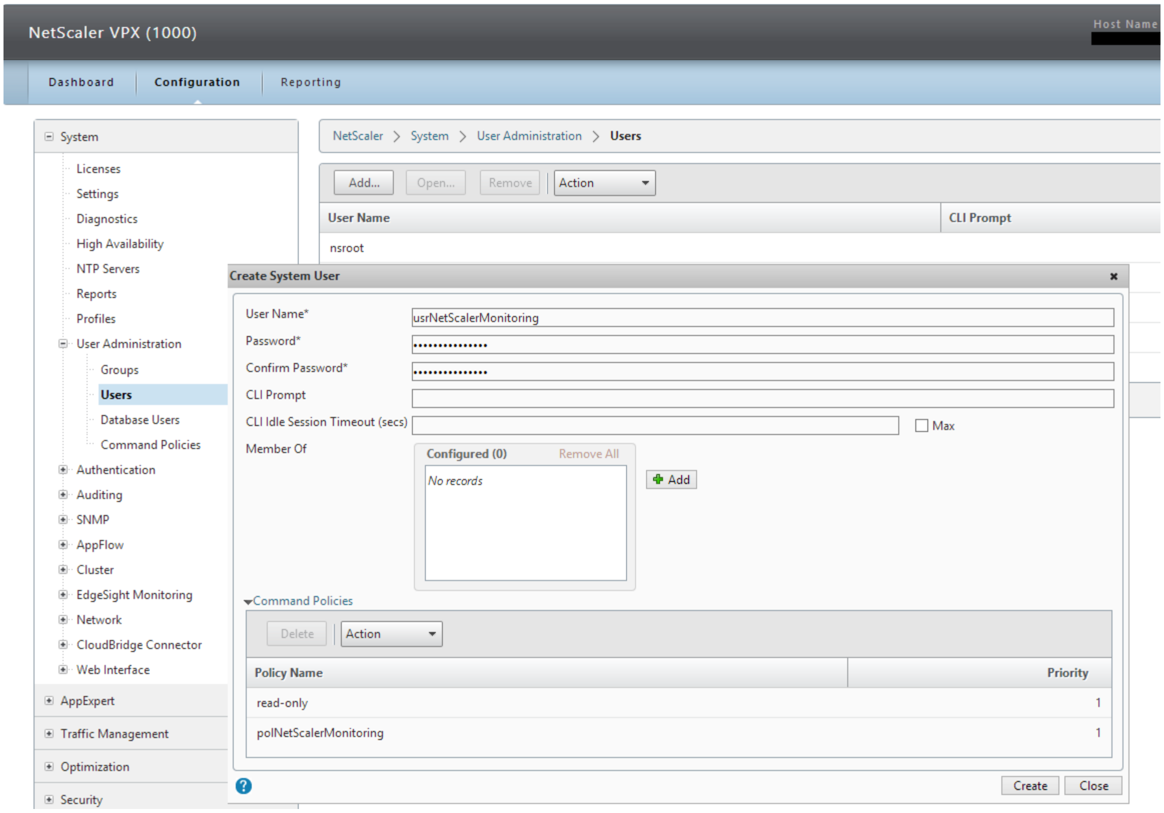
CLI Idle Session Timeout (secs) □ Max

**Figure 2.4** The Insert Command Policies dialog box



| | Name |
|---|---|
| ☑ | read-only |
| ☑ | polNetScalerMonitoring |

**Figure 2.5** Creating and configuring a system user for NetScaler monitoring



[redacted]

User Name* usrNetScalerMonitoring

Password* •••••••••••••••

Confirm Password* •••••••••••••••

CLI Prompt

CLI Idle Session Timeout (secs) □ Max

Member Of

Configured (0) Remove All

*No records*

Add

Command Policies

Delete Action

| Policy Name | Priority |
|---|---|
| read-only | 1 |
| polNetScalerMonitoring | 1 |

11. In the Create System User dialog set the **Priority** for the required command policies to `1`.

12. Click **Create** to create the user account.

13. Click **Close** to close the dialog box.

**Important:** Steps 14 to 16 apply only in case of the LDAP authentication.

14. Run the following command to create necessary authentication policy and perform global binding (the assumption is that the policy is named `Policy_LDAP`):

    ```
    bind system global Policy_LDAP -priority 100
    ```

15. Run the following command to create a user group with the same name as the user group in your Active Directory (as an example, if the Active Directory user account for NetScaler monitoring belongs to the `NetScalerActiveDirectoryUserGroup` group, add the system group `NetScalerActiveDirectoryUserGroup` to NetScaler. The group must therefore exist on both sides: in NetScaler and in Active Directory Users and Computers):

    ```
    add system group NetScalerActiveDirectoryUserGroup
    ```

16. Run the following commands to bind the same command policies to the group as described for the NetScaler user account:

    ```
    bind system group NetScalerActiveDirectoryUserGroup -policy \
    read-only 1
    bind system group NetScalerActiveDirectoryUserGroup -policy \
    polNetScalerMonitoring 1
    ```

### Installing NetScaler Management Pack on the SCOM management server computer

The server-side part of NetScaler Management Pack must be installed on the computer that hosts SCOM management server.

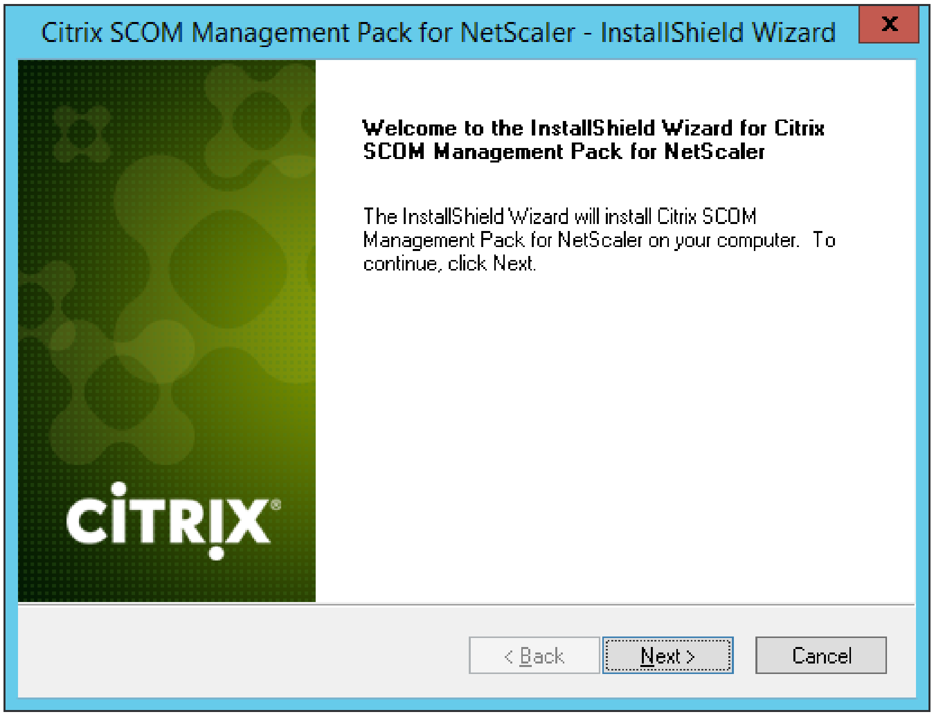
To install NetScaler Management Pack on the SCOM management server computer, do the following:

1. Log on to the management server computer. Use a user account from the local `Administrators` user group that has administrative privileges in SCOM.

2. In Windows Explorer, locate the `Citrix_SCOM_Management_Pack_for_NetScaler_`*`<Version>`*`.exe` file (where *`<Version>`* is the current software version), and double-click it to invoke the installation process. Wait for the Setup Wizard to appear.

3. In the Welcome page of the Setup Wizard, click **Next**.

**Figure 2.6** Initial Setup Wizard page of NetScaler Management Pack



Citrix SCOM Management Pack for NetScaler - InstallShield Wizard

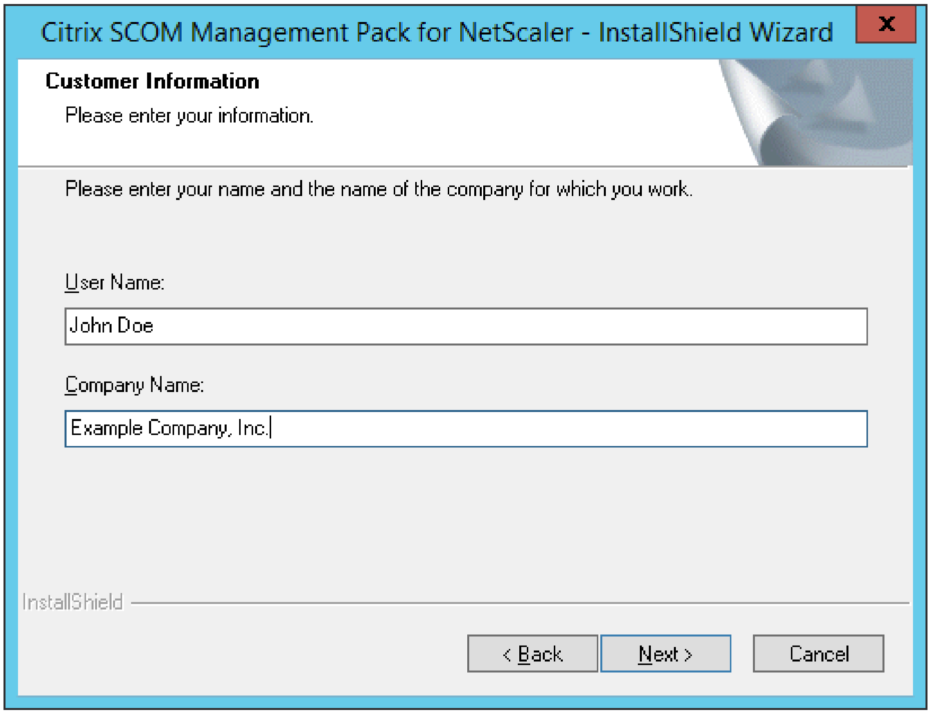
**Welcome to the InstallShield Wizard for Citrix SCOM Management Pack for NetScaler**

The InstallShield Wizard will install Citrix SCOM Management Pack for NetScaler on your computer. To continue, click Next.

4. In the Product Configuration page, click **Next**.

5. In the Customer Information page, type valid information into the **User Name** and **Company Name** text boxes. Click **Next**.

**Figure 2.7** The Customer Information page


Citrix SCOM Management Pack for NetScaler - InstallShield Wizard
Customer Information
Please enter your information.

Please enter your name and the name of the company for which you work.

User Name: John Doe

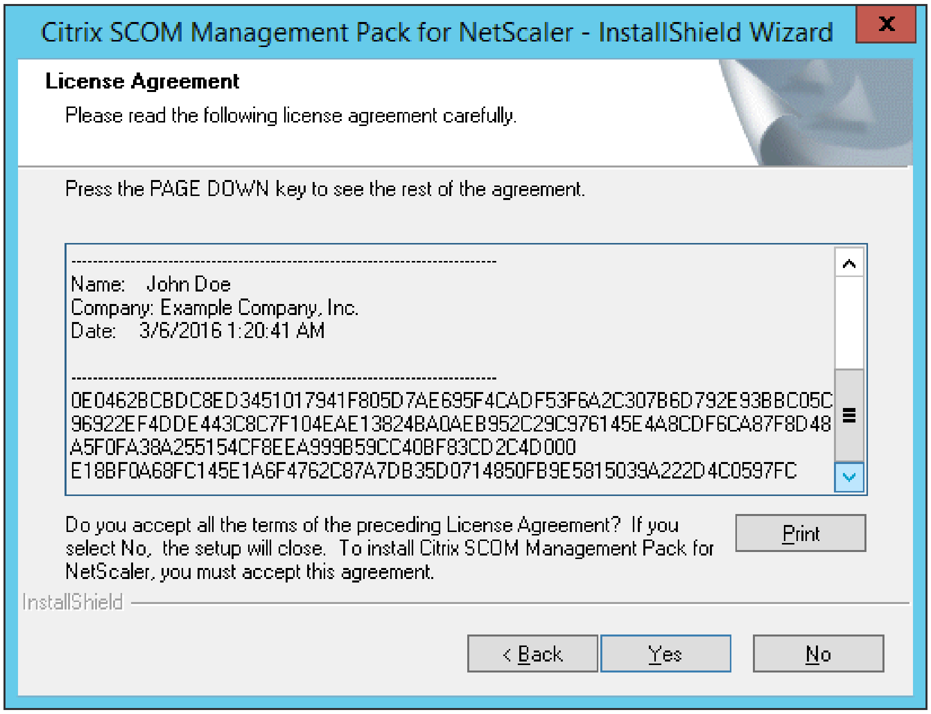
Company Name: Example Company, Inc.

InstallShield
< Back
Next >
Cancel

6. In the Registration Confirmation dialog box, verify that the provided information is correct and click **Yes**.

7. In the License Agreement page of the Setup Wizard, carefully read the end user license agreement. If you accept the terms of the agreement, click **Yes**.

**Figure 2.8** The License Agreement page


Citrix SCOM Management Pack for NetScaler - InstallShield Wizard

**License Agreement**

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

```
--------------------------------------------------------------------------------
Name:    John Doe
Company: Example Company, Inc.
Date:    3/6/2016 1:20:41 AM

--------------------------------------------------------------------------------
0E0462BCBDC8ED3451017941F805D7AE695F4CADF53F6A2C307B6D792E93BBC05C
96922EF4DDE443C8C7F104EAE13824BA0AEB952C29C976145E4A8CDF6CA87F8D48
A5F0FA38A255154CF8EEA999B59CC40BF83CD2C4D000
E18BF0A68FC145E1A6F4762C87A7DB35D0714850FB9E5815039A222D4C0597FC
```

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install Citrix SCOM Management Pack for NetScaler, you must accept this agreement.

8. In the Choose Destination Location page, define the NetScaler Management Pack installation folder. Citrix recommends that you install NetScaler Management Pack to the default folder.

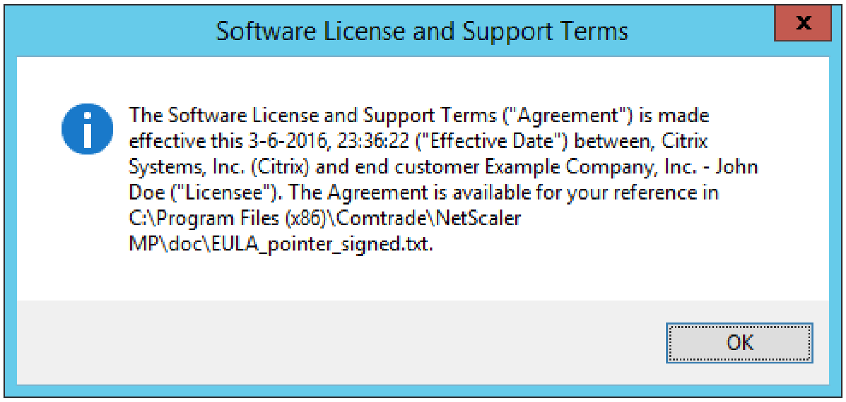
   Proceed as follows:

   - To install the product to the default folder listed in the Setup Wizard, no special actions are required.
   - To install the product to a different folder, follow the substeps:
     a. Click **Browse**.
     b. In the Choose Folder dialog box, browse to a desired installation folder, select it, and click **OK**.

   Click **Next**.

9. In the Software License and Support Terms dialog box, read the message and click **OK**.

**Figure 2.9** The Software Licenses and Support Terms dialog box

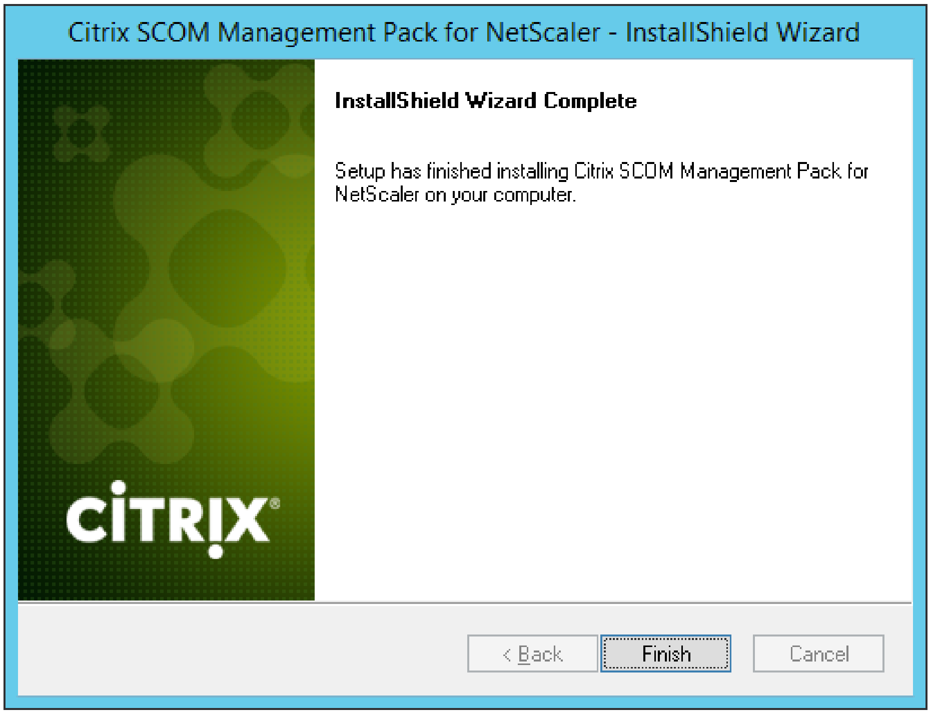


The Software License and Support Terms ("Agreement") is made effective this 3-6-2016, 23:36:22 ("Effective Date") between, Citrix Systems, Inc. (Citrix) and end customer Example Company, Inc. - John Doe ("Licensee"). The Agreement is available for your reference in C:\Program Files (x86)\Comtrade\NetScaler MP\doc\EULA_pointer_signed.txt.

10. In the Start Copying Files page of the Setup Wizard, click **Next**. The Setup Wizard starts copying the installation files.

11. After the installation completes, the installation completion page is displayed.

**Figure 2.10** Final Setup Wizard page



Citrix SCOM Management Pack for NetScaler - InstallShield Wizard
CiTRIX
< Back
Finish
Cancel

**InstallShield Wizard Complete**

Setup has finished installing Citrix SCOM Management Pack for NetScaler on your computer.

12. Click **Finish** to close the Setup Wizard.

### Verifying the installation on the management server computer

To verify that the NetScaler Management Pack installation on the management server computer is correct, do the following:

1. Log on to the management server computer.

2. Go to **Start > Control Panel**, click **Programs**, and then click **Programs and Features**.

3. Check for the presence of the following entry in the Name column:

   `Citrix SCOM Management Pack for NetScaler`

4. Check if there is the `CitrixMPShare` shared folder on the computer and whether it points to the `%`*`ProgramData`*`%\Citrix\CitrixMPShare` location.

   The shared folder is vital for communication between the management server and the agent node during installation of the agent.

### Configuring access to the shared folder for agent installation

**Note:** Steps of this procedure must be followed only once on a SCOM management server computer. In case you previously installed the following Citrix Management Pack product on the same computer, you do *not* need to repeat the steps:

- CloudBridge Management Pack

To configure access to the shared folder for agent installation, do the following:

1. Log on to the SCOM management server computer. Use a user account from the local `Administrators` user group.

2. Choose a local user account (local to the computer with the shared folder) or a domain user account that will have access to the shared folder.

   **Important:** Citrix recommends creating a new, dedicated user account that you will use only for deployment of the Management Pack agent to managed computers.

3. Using an operating system administrative tool, add the user account to the local `CitrixMPShareUsers` user group.

To check whether access to the shared folder is enabled for the chosen user account, run the following command by using this user account:

```
dir \\<ManagementServerHostName>\CitrixMPShare
```

In the above instance, `<ManagementServerHostName>` is the host name of the management server computer. If the command reports no errors, the access is enabled.

### Installing NetScaler Management Pack on the SCOM resource pool members

NetScaler Management Pack Agent is a Windows service that acts as a data collector for NetScaler Management Pack. It is a layer between the management packs and NetScaler instances in the monitoring process. All requests initiated by the NetScaler Management Pack and coming from SCOM flow though the NetScaler Management Pack Agent. The agent optimizes the requests, optimizes sessions with the NetScaler instances, and collects and caches data from these instances.

A single NetScaler Management Pack Agent can handle monitoring of multiple NetScaler appliances. You can also have more than one node dedicated for the NetScaler monitoring. However, NetScaler Management Pack Agent has to be installed on all members in a resource pool for monitoring NetScaler devices.

**Note:** Resource pool is a feature introduced in SCOM 2012. A resource pool is a collection of management servers or gateways used to distribute work amongst themselves and take over work from a failed member. NetScaler Management Pack Agent must reside on all members of a resource pool.

To install the product on the members of a resource pool, do the following:

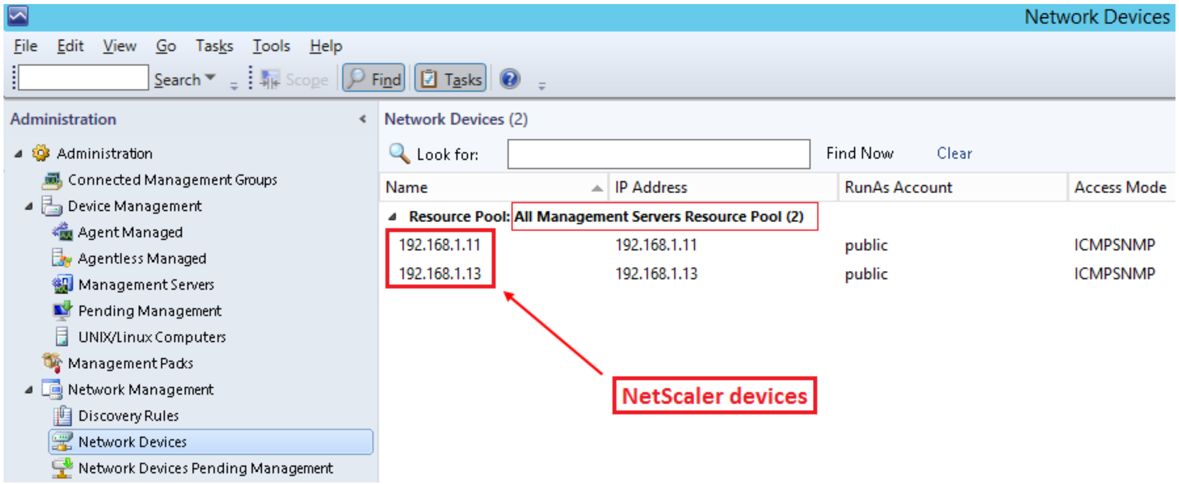
1. Log on to the management server computer.

2. Launch the SCOM Operations console.

3. In the **Administration** view, expand **Device Management > Network Management**, and then click **Network Devices**.

4. Identify discovered NetScaler network devices and the corresponding resource pool names.

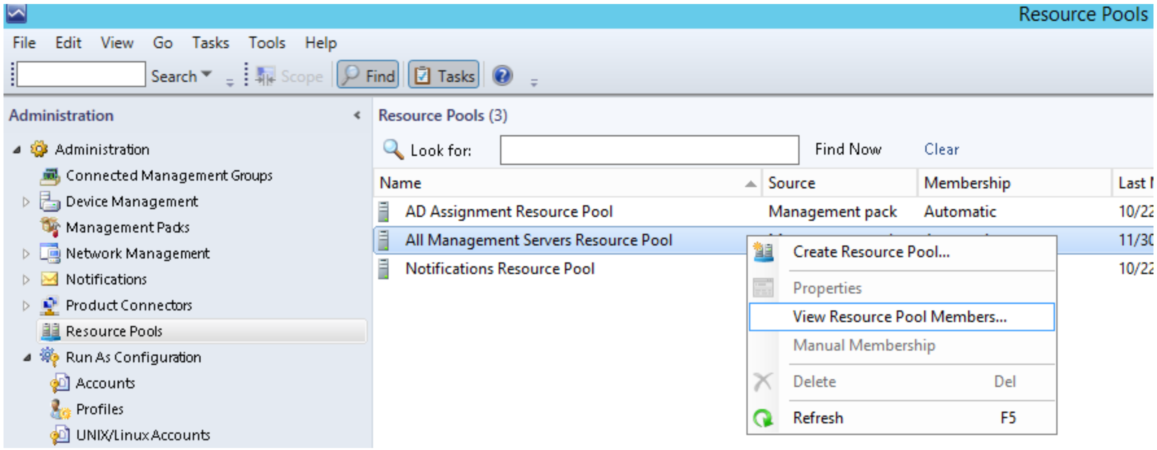
**Figure 2.11** NetScaler network devices in SCOM Operations console



| Name | IP Address | RunAs Account | Access Mode |
|---|---|---|---|
| Resource Pool: All Management Servers Resource Pool (2) | | | |
| 192.168.1.11 | 192.168.1.11 | public | ICMPSNMP |
| 192.168.1.13 | 192.168.1.13 | public | ICMPSNMP |

5. For the identified resource pools, find out their members.

**Figure 2.12** Displaying resource pool members in SCOM Operations console



| Name | Source | Membership | Last I |
|---|---|---|---|
| AD Assignment Resource Pool | Management pack | Automatic | 10/22 |
| All Management Servers Resource Pool | | | 11/30 |
| Notifications Resource Pool | | | 10/22 |

6. Log on to a member of the resource pool. Use a user account from the local `Administrators` user group.

7. Depending on the hardware architecture of the resource pool member, copy the appropriate file from the `\CitrixMPShare\NetScaler MP` shared folder on the management server computer to a location on the member: `mpns_x64.msi` or `mpns_x86.msi`.

8. In Windows Explorer, locate the `mpns_x64.msi` or `mpns_x86.msi` file, and double-click it to invoke the installation process.

9. Follow instructions of the Setup Wizard.

10. Repeat steps 6 to 9 for each additional resource pool member.

### Configuring agent nodes to act as SCOM proxies

Each node where NetScaler is installed must be configured to act as a SCOM proxy computer (proxy). This configuration enables the node to relay or forward information from or about other computes or network devices to the management server. Depending on where the agent is installed, perform the corresponding procedure.

To configure the SCOM management server computer to act as a proxy, do the following:

1. Log on to the management server computer.
2. Launch the SCOM Operations console.
3. In the **Administration** view, expand **Device Management**, and then click **Management Servers**.
4. Right-click the management server host name, and select **Properties**.
5. Click the **Security** tab.
6. Select the **Allow this agent to act as proxy and discover managed objects on other computers** option.
7. Click **OK**.

To configure the SCOM gateway computer to act as a proxy, do the following:

1. Log on to the management server computer.
2. Launch the SCOM Operations console.
3. In the **Administration** view, expand **Device Management**, and then click **Agent Managed**.
4. Right-click the agent computer host name, and select **Properties**.
5. Click the **Security** tab.
6. Select the **Allow this agent to act as proxy and discover managed objects on other computers** option.
7. Click **OK**.

### Verifying the installation on the agent-managed computers

To verify that the NetScaler Management Pack installation on an agent-managed computer is correct, do the following:

1. Log on to the agent-managed computer.

2. Go to **Start > Control Panel**, click **Programs**, and then click **Programs and Features**.

3. Check for the presence of the following entry in the Name column:

   `Citrix SCOM Management Pack Agent for NetScaler`

4. Go to **Start > Administrative Tools** and double-click **Services**.

5. In the Name column of the Services window, locate the `Citrix MPNS Agent` service, and make sure that its status is to `Started`.

### Manually importing included management packs into SCOM

For general instructions about how to import management packs into SCOM, see the How to Import an Operations Manager Management Pack webpage on the Microsoft TechNet website.

To import the sealed management packs for NetScaler, do the following:

1. Log on to the management server computer.

2. Launch the SCOM Operations console.

3. In the Administration view, click **Management Packs**.

4. Make sure all required default management packs are present in the list in the middle pane. For a list of requirements, see “Preparing for the installation”.

5. In the Tasks pane, expand **Actions**, and then click **Import Management Packs**.

6. In the Import Management Packs dialog box, click **Add**, and then select **Add from disk**.

7. In the Online Catalog Connection, click **No**.

8. In the Select Management Packs to import dialog box, browse to the `%PrograFiles(x86)%\ComTrade\NetScaler MP\ManagementPacks` folder, select the following management pack files, and then click **Open**.

   - `Comtrade.Citrix.Library.mp`
   - `Comtrade.Citrix.NetScaler.Device.mp`
   - `Comtrade.Citrix.NetScaler.Library.mp`
   - `Comtrade.Citrix.NetScaler.Monitoring.mp`
   - `Comtrade.Citrix.NetScaler.Appliance.9.Library.mp`
   - `Comtrade.Citrix.NetScaler.Appliance.10.Library.mp`
   - `Comtrade.Citrix.NetScaler.Appliance.10.Monitoring.mp`
   - `Comtrade.Citrix.NetScaler.Appliance.9.Discovery.mp`
   - `Comtrade.Citrix.NetScaler.Appliance.10.Discovery.mp`

9. Click **Install**.

### Verifying the import of the included management packs

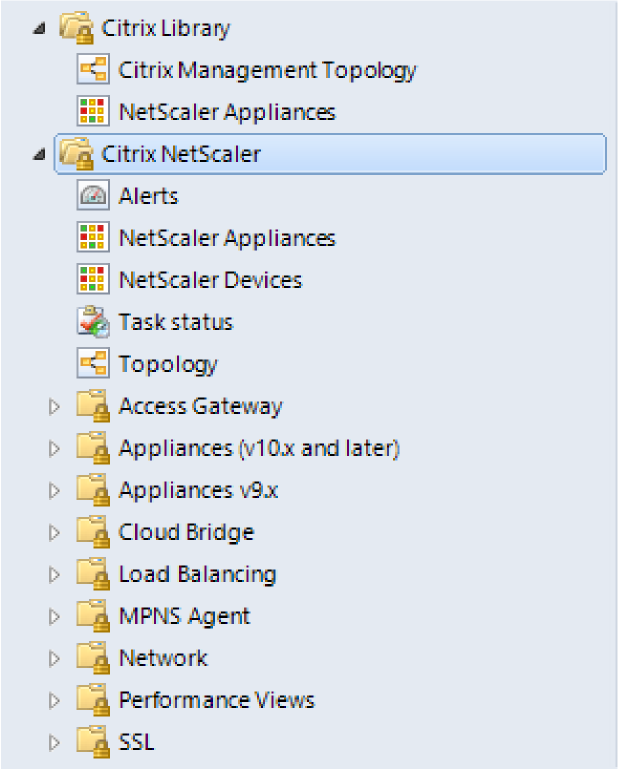
To verify that the import of the sealed management packs included in NetScaler Management Pack was successful, do the following:

1. Log on to the management server computer.

2. Launch the SCOM Operations console.

3. In the Monitoring view, expand the items in the left pane until they match the following figure.

**Figure 2.13** Elements of NetScaler Management Pack, as seen in the SCOM Operations console



- Citrix Library
  - Citrix Management Topology
  - NetScaler Appliances
- Citrix NetScaler
  - Alerts
  - NetScaler Appliances
  - NetScaler Devices
  - Task status
  - Topology
  - Access Gateway
  - Appliances (v10.x and later)
  - Appliances v9.x
  - Cloud Bridge
  - Load Balancing
  - MPNS Agent
  - Network
  - Performance Views
  - SSL

### Configuring the NetScaler Appliance action account in SCOM

To configure Run As account in SCOM, do the following:

1. Log on to the SCOM management server computer. Use a user account from the local `Administrators` user group.

2. Launch the SCOM Operations console.

3. In the **Administration** view, in the left pane, expand **Run As Configuration**, and then click **Accounts**.

4. In the Tasks pane, expand **Actions**, and then click **Create Run As Account**.

5. In the Create Run As Account Wizard window, click **Next**.

6. In the General Properties page, in the **Run As account type** drop-down menu, select `Basic`, `Simple`, or `Windows`. If you are using LDAP, leave the default selection (`Windows`).

7. In the **Display name** text box, type a name that the SCOM Operations console will use to refer to the newly created SCOM user account. Click **Next**.

8. In the Credentials page, type user name, password, and domain of the user account that you used in “Configuring NetScaler for monitoring by NetScaler Management Pack”. Click **Next**.

9. In the Distribution Security page, select a distribution security option.

   Citrix recommends that you select the **More secure** option. In this case, you must subsequently edit the Run As account to include all NetScaler devices (nodes).

10. Click **Create** to save the configuration data of the new account.

11. Click **Close** to close the wizard.

To assign the configured Run As account  to NetScaler devices, do the following:

1. Log on to the SCOM management server computer. Use a user account from the local `Administrators` user group.

2. Launch the SCOM Operations console.

3. In the **Administration** view, in the left pane, expand **Run As Configuration**, and then click **Profiles**.

4. In the middle pane, in the Name column, double-click **Citrix NetScaler Appliance Action Account**.

5. In the Run As Profile Wizard window, click **Next** and then click **Next** again.

6. In the Run As Accounts page, click **Add**.

7. In the Add a Run as Account dialog box, from the Run As account drop-down list, select the display name of the newly created Run As account.

8. Select the **A selected class, group, or object** option (more secure).

9. Click **Select** and then select **Object**.

10. In the Object Search dialog box, in the Look for drop-down list, select **Node** and then click **Search**.

11. In the Available items list, select the NetScaler network device, and then click **Add**.

12. Click **OK** to close the dialog box.

13. Click **OK** to close the Add a Run As Account dialog box.

14. Click **Save** to save the changes.

15. Click **Close** to close the Run As Profile Wizard window.

16. Distribute the Run As account to the appropriate agent-managed computers. Do the following:

    a. In the Administration view, double-click the user account.

    b. In the Run As Account Properties dialog box, click the **Distribution** tab.

    c. Click **Add**.

    d. In the Computer Search dialog box, search for and add the computers. Click **OK**.

    e. In the Run As Account Properties dialog box, click **Apply** and then click **OK**.

**Note:** After saving the updated Run As profile, it may take up to 10 minutes for the configuration to get distributed to all specified computers.

For more information on management of Run As accounts and Run As profile, see the Managing Run As Accounts and Profiles webpage on the Microsoft TechNet website.

# Chapter 3: Uninstallation

This chapter contains instructions that you must follow to effectively uninstall NetScaler Management Pack. Perform all procedures in the documented order of precedence.

### Removing dependent management packs (customizations)

To remove the customizations that you made to the management packs included in NetScaler Management Pack, do the following:

1. Log on to the management server computer.

2. Launch the SCOM Operations console.

3. In the Administration view, click **Management Packs**.

4. In the middle pane, locate the management packs that depend on the management packs included in NetScaler Management Pack.

5. For each such dependent management pack, follow the steps:

    a. Right-click it and then click **Delete**.

    b. On the message stating that deleting the management pack might affect the scoping of some user roles, click **Yes**.

### Removing included management packs

To remove the management packs included in NetScaler Management Pack, do the following:

1. Log on to the management server computer.

2. Launch the SCOM Operations console.

3. In the Administration view, click **Management Packs**.

4. Remove references to the included management packs from the `Microsoft.SystemCenter.SecureReferenceOverride` management pack. To do this perform the following steps:

    a. Identify which included management packs are referenced. In the **Administration > Management Packs** context of the SCOM Operations console, right-click **Microsoft.SystemCenter.SecureReferenceOverride** and select **Properties**. In the dialog box, click the **Dependencies** tab.

    b. For each such referenced management pack, find out its ID. Right-click the referenced management pack. In the dialog box, take note of the value in the ID text box on the General tab.

    c. Export the `Microsoft.SystemCenter.SecureReferenceOverride` management pack.

    d. Make a copy of the file you exported the management pack to.

    e. Edit the originally exported file to remove all dependencies to the management packs from the `Manifest > References` context (the `<Reference>` elements) and the `Monitoring > Overrides` context (the `<SecureReferenceOverride>` elements), and then save the changes.

    f. Import back the altered `Microsoft.SystemCenter.SecureReferenceOverride` management pack from the modified file.

5. In the SCOM Operations console, in the middle pane, right-click **Citrix NetScaler Appliance (v10.x and later) Monitoring Library**.

6. On the message stating that deleting the management pack might affect the scoping of some user roles, click **Yes**.

7. Repeat steps 5 and 6 with the following management packs (in the presented order of precedence):

   - **Citrix NetScaler Monitoring Library**
   - **Citrix NetScaler Appliance (v10.x and later) Discovery Library**
   - **Citrix NetScaler Appliance (v9.x) Discovery Library**
   - **Citrix NetScaler Appliance (v10.x and later) Component Library**
   - **Citrix NetScaler Appliance (v9.x) Component Library**
   - **Citrix NetScaler Appliance Component Library**
   - **Citrix NetScaler Device Discovery  Library**

8. Check if other Citrix SCOM Management Pack products are installed on the management server computer. If none of them is installed, repeat steps 5 and 6 with **Citrix Management Pack Library**.

### Uninstalling NetScaler Management Pack from the SCOM resource pool members

To uninstall NetScaler Management Pack from a member of a resource pool, do the following:

1. Log on to the member of the resource pool with a user account from the local `Administrators` user group.

2. Make sure no other users are logged on to the computer.

3. Go to **Start > Control Panel**, click **Programs**, and then click **Programs and Features**.

4. Right-click **Citrix SCOM Management Pack Agent for NetScaler** and select **Uninstall**.

   **Important:** If a warning informs you about other logged on users, the program might not uninstall completely.

5. In the Programs and Features dialog box, click **Yes** to confirm uninstallation.

### Uninstalling the product from the SCOM management server computer

To uninstall NetScaler Management Pack from the SCOM management server computer, do the following:

1. Log on to the management server computer. Use a user account from the local `Administrators` user group that has administrative privileges in SCOM.

2. Make sure no other users are logged on to the computer.

3. Go to **Start > Control Panel**, click **Programs**, and then click **Programs and Features**.

4. Right-click **Citrix SCOM Management Pack for NetScaler** and select **Uninstall**. Wait for the Setup Wizard to appear.

   **Important:** If a warning informs you about other logged on users, the program might not uninstall completely.

5. In the Welcome page of the Setup Wizard, click **Uninstall**.

6. In the Uninstalling the product page, the Setup Wizard reports the uninstallation progress.

7. In the Completion page of the Setup Wizard, click **Finish**.

8. Check if other Citrix SCOM Management Pack products are installed on the management server computer. If none of them is installed, follow the steps:

   a. Stop sharing the `CitrixMPShare` shared folder.

   b. Delete the `%`*`ProgramData`*`%\Citrix\CitrixMPShare` folder.

   c. Using an operating system administrative tool, delete the local `CitrixMPShareUsers` user group.

# Chapter 4: Usage

### Optional configuration

*Tuning thresholds for performance monitors and rules*

Some monitors and rules have default thresholds that might need additional tuning to suit your environment. You should evaluate monitors and rules to determine whether the default thresholds are appropriate for your environment. If a default threshold is not appropriate for your environment, you should baseline the relevant performance counters, and then adjust the threshold by overriding them.

In the *Citrix SCOM Management Pack for NetScaler Reference Guide*, which you can find in the `Citrix_MPNS_ReferenceGuide.html` file, you can find details about the following items:

- Discoveries
- Monitors
- Roll-up Monitors
- Rules
- Tasks
- Scripts
- Enabled and disabled items by default

*Discovering objects*

For general information about discovering objects in SCOM, see the Object Discoveries in Operations Manager 2007 webpage on the Microsoft TechNet website.

The following table lists the object types that NetScaler Management Pack discovers in the managed environment.

**Table 4.1** Discovered NetScaler object types

| Object type | Description |
|---|---|
| AAA | An Authentication Authorization Auditing object. |
| Access Gateway | The root object for Access Gateway. |
| Access Gateway Virtual Server | The Access Gateway Virtual Server object. |
| Action | An Action object. |
| Authentication Server | An Authentication Server object. |

| | |
|---|---|
| Bridge | A Bridge object. |
| Channel | A Channel object. |
| Cloud Bridge | A group of NetBridge objects. |
| Group | A group of related objects. |
| Interface | An Interface object. |
| IP | A group of IPv4 and IPv6 objects. |
| LDAP Policy | A LDAP Policy object. |
| LDAP Server | A LDAP Server object. |
| License | A License object. |
| Load Balancing | The root object for Load Balancing. |
| Load Balancing Virtual Server | A  Load Balancing Virtual Server object. |
| Memory Pool | A Memory Pool object. |
| NetBridge | A Network Bridge object. |

| | |
|---|---|
| NetScaler Appliance | The root object for topology of NetScaler appliance. |
| Network | A Network object. |
| Policy | A Policy object. |
| Radius Policy | A RADIUS Policy object. |
| Radius Server | A RADIUS Server object. |
| Service | A Service object. |
| Service Group | A Service Group object. |
| Settings | HTTP, Global, Timeout, Feature, Modes, TCP and other settings. |
| SSL | An SSL object. |
| SSL Action | An SSL Action object. |
| SSL Certificate | An SSL Certificate object. |
| SSL Policy | An SSL Policy object. |
| System | A System object. |

| | |
|---|---|
| TACACS Policy | A TACACS Policy objects. |
| Traffic Management | The Root object for Traffic Management. |
| VLAN | A Virtual LAN object. |

### Customizing sealed management packs

Similarly to customizing the default SCOM management pack, you can customize the sealed management packs that NetScaler Management pack provides. For details, see the Microsoft TechNet website:

- For general information about customization of management packs, see the Customizing Management Packs webpage.
- For instructions on how to customize a management pack, see the Create a New Management Pack for Customizations webpage.

# Chapter 5: Support

### General support resources

Citrix® offers a variety of resources for support with your Citrix environment, including the following:

- The Knowledge Center is a self-service, Web-based technical support database that contains thousands of technical solutions, including access to the latest hotfixes, service packs, and security bulletins.
- Technical Support Programs for both software support and appliance maintenance are available at a variety of support levels.
- The Subscription Advantage program is a one-year membership that gives you an easy way to stay current with the latest product version upgrades and enhancements.
- Citrix Education provides official training and certification programs on virtually all Citrix products and technologies.

For more information about Citrix services and support, see the Citrix Support Services and Resources website.

You can also participate in and follow technical discussions offered by the experts on various Citrix products at the Welcome to the Citrix Community, Citrix Discussions, and Citrix Services websites.

### Contacting Citrix Customer Service

To contact Citrix Customer Service, see the Contact Support website.