



IBM  
Systems Director Network Control V1.2



---

# Contents

## IBM Systems Director Network Control

### V1.2 . . . . . 1

About this publication . . . . .	1
Who should read this user's guide . . . . .	1
Conventions and terminology . . . . .	1
How to send your comments . . . . .	1
IBM Systems Director Network Control Overview . . . . .	1
What's new in IBM Systems Director Network Control V1.2 . . . . .	2
Product comparison: Network Management and IBM Systems Director Network Control . . . . .	3
Accessibility features . . . . .	4
License information . . . . .	5
Planning for IBM Systems Director Network Control . . . . .	6
Hardware and software requirements . . . . .	6
IBM Systems Director Network Control device and task support . . . . .	9
Configuring SNMP traps to enable network monitoring . . . . .	14
Test logging an SNMP trap as an event in Systems Director. . . . .	16
Installing and uninstalling IBM Systems Director Network Control . . . . .	16
Installing IBM Systems Director Network Control using the installation wizard. . . . .	16
Installing IBM Systems Director Network Control using silent install . . . . .	18
Installing the IBM Systems Director Network Control permanent license key using the installation wizard . . . . .	20
Installing the IBM Systems Director Network Control permanent license key using silent install . . . . .	21

Uninstalling IBM Systems Director Network Control. . . . .	22
Migrating to IBM Systems Director Network Control V1.2. . . . .	23
Updating IBM Systems Director Network Control . . . . .	24
Managing network devices . . . . .	24
Discovering network systems . . . . .	24
Collecting and viewing inventory for network systems. . . . .	25
Configuring network systems with configuration plans and templates . . . . .	27
Managing network systems health. . . . .	28
Managing hardware supported by DCFM . . . . .	29
Working with network device groups. . . . .	37
Collecting and viewing network topology inventory . . . . .	38
IBM Systems Director Network Control troubleshooting . . . . .	40
Using IBM Systems Director Network Control diagnostic tools . . . . .	41
Duplicate events display in the event log view . . . . .	41
Empty window is displayed or nothing happens . . . . .	42
Collect network topology missing connections. . . . .	43
Troubleshooting DCFM problems . . . . .	44
Publications and related information . . . . .	51
Notices . . . . .	52
Trademarks . . . . .	53

## Index . . . . . 55



---

# IBM Systems Director Network Control V1.2

IBM® Systems Director Network Control V1.2 provides facilities to discover, inventory, and monitor network devices, launch vendor applications for configuration of network devices, and view groups of network devices. IBM Systems Director Network Control V1.2 is a priced plug-in product that extends the network management functions of the IBM Systems Director product.

---

## About this publication

This publication provides information about installing, configuring, and using IBM Systems Director Network Control V1.2.

### Who should read this user's guide

This user's guide is for system administrators and operators using IBM Systems Director Network Control to manage network devices in their environment.

### Conventions and terminology

These notices are designed to highlight key information:

**Note:** These notices provide important tips, guidance, or advice.

**Important:** These notices provide information or advice that might help you avoid inconvenient or difficult situations.

**Attention:** These notices indicate possible damage to programs, devices, or data. An attention notice appears before the instruction or situation in which damage can occur.

### How to send your comments

Your feedback is important in helping to provide the most accurate and highest quality information.

If you have any comments about this book or any other IBM Systems Director publication, go to the IBM Systems Director information center Web site at <http://publib.boulder.ibm.com/infocenter/director/v6r2x/index.jsp>. There you can use the feedback page to enter and submit comments.

---

## IBM Systems Director Network Control Overview

IBM Systems Director Network Control V1.2 provides advanced network management functions for network devices. Functions include discovery, inventory, network topology, health and status monitoring, and configuration of network devices.

IBM Systems Director Network Control builds on Network Management base capabilities by integrating the launch of vendor-based device management tools, topology views of network connectivity, and subnet-based views of servers and network devices.

You can use IBM Systems Director Network Control to:

- Discover network devices in your environment.
- Review your network device inventory in tables or a network topology view.
- Launch tasks to configure and manage Brocade hardware in IBM System Storage® Data Center Fabric Manager (DCFM).
- Monitor the health and status of network devices.
- Manage devices by groups: Ethernet switches, Fibre Channel over Ethernet, or Subnet.
- View network device configuration settings, and apply templates to configure devices, including Converged Enhanced Ethernet quality of service (QoS), VLANs, and Link Layer Discovery Protocol (LLDP).
- View systems according to VLAN and subnet.
- Run network diagnostic tools like ping and traceroute.

#### Related reference

 [Supported network devices](#)

 [IBM Systems Director Network Control](#)

## What's new in IBM Systems Director Network Control V1.2

See this topic for new features and enhancements in IBM Systems Director Network Control V1.2. This product is for use with IBM Systems Director V6.2.

**Attention:** The previous product version, IBM Systems Director Network Control V1.1, is not compatible with IBM Systems Director V6.2. See the topic “Migrating to IBM Systems Director Network Control V1.2” on page 23 for migration procedures.

### Hypervisor support

Discovery and inventory of virtual switches is supported for these hypervisor platforms:

- VMware ESXi V4.0 update 1 or later, and ESX V4.0 or later
- PowerVM™ servers managed by HMC

To manage VMWare ESX and ESXi virtual resources, including switches, network adapters, and VLANs, follow these steps:

1. Discover the hypervisor IP address
2. Use **Request Access** to unlock the hypervisor so that the system displays **Access State OK**
3. Collect inventory on the Operating System resource.

To manage HMC Power server virtual resources, including switches, network adapters, and VLANs, follow these steps:

1. Discover the HMC IP address
2. Use **Request Access** to unlock the HMC so that the system displays **Access State OK**
3. Collect inventory on the HMC resource.

These steps are included in the discovery and inventory task topics.

## New views

View combined virtual and physical network topology, and view systems according to VLAN and subnet. See “Working with network device groups” on page 37.

## IPv6 Support

IBM Systems Director Network Control V1.2 support IPv6 when the network devices are fully IPv6-compliant. Use IPv6 for the following network management tasks:

- Discover network devices by IPv6 address.
- Determine IPv6 addresses while collecting inventory on network devices.
- View network devices by IPv6 subnet.

Some network devices are not fully compliant. See the “IBM Systems Director Network Control device and task support” on page 9 topic for details. Ping and traceroute diagnostic functions do not support IPv6.

## Enhanced DCFM Support

IBM Systems Director Network Control V1.2 supports template-based configuration of Converged Enhanced Ethernet (CEE) switches that are managed by IBM System Storage Data Center Fabric Manager (DCFM). Manage the following properties:

- CEE quality of service (QoS)
- VLANs
- Link Layer Discovery Protocol (LLDP)
- Port settings

See “Managing hardware supported by DCFM” on page 29.

## Additional hardware support

IBM Systems Director Network Control V1.2 supports several new network devices. For a full list, see “IBM Systems Director Network Control device and task support” on page 9.

## Product comparison: Network Management and IBM Systems Director Network Control

View a list of basic and advanced network management function to see the differences between network management function provided by IBM Systems Director and the advanced network management function offered by the IBM Systems Director Network Control V1.2 plug-in.

Basic network management function is provided by IBM Systems Director. The IBM Systems Director Network Control V1.2 offers advanced network management function. The following table indicates what functions each product supports.

*Table 1. Tasks supported by network management products in IBM Systems Director*

Task or feature	IBM Systems Director network management	IBM Systems Director Network Control
Network system discovery	Yes	Yes

Table 1. Tasks supported by network management products in IBM Systems Director (continued)

Task or feature	IBM Systems Director network management	IBM Systems Director Network Control
Health summary	Yes	Yes
Request access (SNMP, Telnet)	Yes	Yes
Collect and view inventory	Yes	Yes
View network system properties	Yes	Yes
Network-specific default groups	Yes <sup>1</sup>	Yes <sup>1</sup>
View network problems and events	Yes	Yes
Network monitors and thresholds	Yes	Yes
Event filters and automation plans	Yes	Yes
Network diagnostics (ping, traceroute)	Yes	Yes
Network system configuration	Yes	Yes
Virtual Switch VLAN configuration	No	Yes
Vendor-based management tool integration	No	Yes
Network topology collection <sup>2</sup>	No	Yes
Network topology perspectives <sup>2</sup>	No	Yes
View systems by subnet	No	Yes
<p>1. IBM Systems Director Network Control provides an additional "Subnets" group.                  2. Not supported on Linux<sup>®</sup> on Power Systems<sup>™</sup>.</p>		

#### Related reference

"License information" on page 5

## Accessibility features

This topic provides information about the accessibility features of IBM Systems Director Network Control.

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully. The IBM Systems Director Network Control plug-in for IBM Systems Director supports the accessibility features that are supported in IBM Systems Director.

When using Freedom Scientific JAWS for Windows<sup>®</sup> screen reader with IBM Systems Director Network Control, follow these tips to improve JAWS usability:

- Access IBM Systems Director Server using a supported Mozilla Firefox browser.
- Enable accessibility features in the IBM Systems Director Web interface:

1. Open **Settings** → **Navigation Preferences**.
  2. Turn on the following options:
    - Enable tables for accessibility
    - Play sound when data on the page changes
    - Use resource table view as default view for topology perspectives
  3. Click **OK** or **Apply** to save your settings.
- Use the following JAWS key commands to navigate Actions menus when working with resource tables:
    - To move to the next menu item with focus and control, press and hold Shift + Ctrl keys while using the Up and Down arrow keys.
    - To navigate to a submenu, navigate into a submenu list, press Alt + Right arrow key.

The following list describes Accessibility limitations of IBM Systems Director Network Control

- Limitation: When working with the task Launch DCFM Setup, JAWS may read the entire Summary panel before reading the DCFM dialog. Entering invalid data on the form causes a beep, but returns to the beginning of the Summary panel instead of reading the error first. Use the Tab key to advance to the DCFM form fields or to any error messages.
- Limitation: When launching external configuration managers from the IBM Systems Director Network Control interface, there may be a delay of several minutes while the application loads, and no status alerts are voiced. Wait for the configuration manager to load.

For more information, see the Accessibility features for IBM Systems Director topic.

**Note:** For technical details about the accessibility support in IBM Systems Director, see the Voluntary Product Accessibility Templates (VPATs). You can request VPATs from the Web at [\\*](#).

## License information

This topic describes the licensing for IBM Systems Director Network Control V1.2. You can install IBM Systems Director Network Control for free evaluation. After the evaluation license expires, you must purchase a license in order to continue using the IBM Systems Director Network Control advanced plug-in.

### Evaluation license

When you download, install, and begin using IBM Systems Director Network Control V1.2, you are granted a 60-day evaluation license. The evaluation license enables use of the advanced management functions described in the product overview. During the evaluation, the IBM Systems Director Network Control summary page displays the number of days remaining on the evaluation license, the expiration date, and information about obtaining a license.

The 60-day evaluation period begins the first time you begin using IBM Systems Director Network Control. After the evaluation license expires, you must install a permanent license key to continue using the advanced network management functions. The summary page continues to display the IBM Systems Director Network Control functions, but advanced functions do not operate until the license key is installed. Network Management functions in IBM Systems Director will continue to operate after the evaluation license expires. To remove the disabled

advanced network management functions and restore the Network Management summary page, uninstall IBM Systems Director Network Control.

### **Product license**

The IBM Systems Director Network Control V1.2 license is packaged on a CD-ROM with an authorization key and an install program. After you install the license, the optional management functions are enabled and function just as they did during the evaluation period, with your configurations and settings remaining intact.

IBM Systems Director Network Control V1.2 is a fee-based IBM Systems Director plug-in that enables management of network adapters and switches, enhanced with storage fabric management for Ethernet and Fibre Channel Over Converged Enhanced Ethernet (FCoCEE) IBM Network Switches. It also provides management of virtual LANs and discovery and display of your network topology.

IBM Systems Director Network Control uses per server and per switch charging metrics. A server license is required for the machine running IBM Systems Director Network Control V1.2. Licenses are also required for each switch being managed, based on the size and type of switch. Switches are categorized as small, medium, or large, based on the following criteria:

- Small switches are machines with a fixed number of ports that require 1U or 2U of rack space.
- Medium switches are modular machines that can support up to eight optional interface or controller modules.
- Large switches are modular machines that can support more than eight optional interface or controller modules.

Contact your IBM marketing representative or business partner for detailed licensing and pricing information.

### **Related reference**

“Product comparison: Network Management and IBM Systems Director Network Control” on page 3

---

## **Planning for IBM Systems Director Network Control**

This topic contains information about IBM Systems Director Network Control requirements, including hardware requirements, supported hardware and operating systems, and prerequisites.

### **Hardware and software requirements**

Learn about the system requirements to install and use IBM Systems Director Network Control V1.2.

#### **Hardware requirements**

IBM Systems Director Network Control V1.2 is supported on all IBM systems that are supported by IBM Systems Director Server 6.2.

For detailed information about the systems supported by IBM Systems Director Server, see Supported IBM systems and products.

Disk space and memory requirements:

- The directory containing the installation package requires at least 3 GB of free space for extracting and processing temporary files.
- AIX<sup>®</sup> requires at least 900 MB in free /tmp and 4 GB free in /opt, and 4 GB of RAM
- Linux on Power Systems requires at least 1 GB free in /opt and 2 GB of RAM
- Linux on x86 requires at least 500 MB free in /tmp and 4 GB free in /opt and 4 GB of RAM
- Linux on System z<sup>®</sup> requires at least 500 MB free in /tmp and 4 GB free in /opt and 4 GB of RAM
- Windows requires at least 4 GB free on the C:/ drive and 4 GB of RAM

After you have installed IBM Systems Director Network Control, you can work with supported network devices. The topic Device and task support provides details about the supported switches and the network management tasks they support.

### Software requirements

- You must have IBM Systems Director Server 6.2 installed before you install IBM Systems Director Network Control V1.2.
- The IBM Systems Director Network Control virtual switch and virtual network adapter support for VMWare ESX and ESXi servers requires the following server levels:
  - VMWare ESX server level 4.0.0 or newer
  - VMWare ESXi server level 4.0.1 or newer
- If your network includes hardware that is supported by DCFM, you can use IBM Systems Director Network Control to work with the IBM System Storage Data Center Fabric Manager (DCFM) application to do certain configuration-oriented tasks. The DCFM Server is required for launch-in-context tasks, and both the DCFM Server and the DCFM SMI Agent (CIMOM) service are required for configuration tasks that are integrated directly in the IBM Systems Director Network Control user interface. Launch-in-context tasks display the DCFM client interface on the same server where the IBM Systems Director console is running. Launching tasks to DCFM requires Sun Java<sup>™</sup> 6 Version 16 or higher installed on the server running the Director console web browser. To obtain versions of the Java Runtime, you can visit the Sun Java archive: \*. IBM System Storage Data Center Fabric Manager (DCFM) 10.4.1a is required for integrated configuration tasks. DCFM 10.3.2 can be used for launch-in-context, but will not support the template-based configuration tasks.

### Operating system requirements

IBM Systems Director Network Control V1.2 is supported for use on the AIX, Linux, and Windows operating systems supported by IBM Systems Director.

**Note:** Advanced network topology functions are not supported for Linux on Power Systems.

For a comprehensive list of supported operating systems, see Operating systems supported by IBM Systems Director 6.2.

Additional steps are required to prepare some operating systems for IBM Systems Director Network Control. Review the following topics for more information.

## Prerequisites for installation of IBM Systems Director Network Control on Red Hat Enterprise Linux

Prepare your system before installing IBM Systems Director Network Control on Red Hat Enterprise Linux.

Before you install IBM Systems Director Network Control on Red Hat Enterprise Linux, you must disable Security-Enhanced Linux (SELinux). When IBM Systems Director Network Control on Red Hat Enterprise Linux is installed, SELinux is optionally enabled.

To disable SELinux, turn off SELinux enforcing by completing the following steps:

1. Open the following file: `/etc/sysconfig/selinux`
2. Find the following line within the `selinux` file: `SELINUX=enforcing`
3. Modify the text to read: `SELINUX=disabled`.
4. Restart the server.

## Prerequisites for installation of IBM Systems Director Network Control on Linux on System z

Prepare your system before installing IBM Systems Director Network Control on Linux on System z.

Before installing IBM Systems Director Network Control on Linux on System z, ensure that the host name is not set to the fully qualified domain name by using the following steps:

1. Check the current value of the host name by running the following command:  
`hostname`
2. If the host name is set to the fully qualified domain name, then change it using the following command: `hostname <Short Name>`

Where `<Short Name>` is the name of the system without the domain information. For example:

```
# hostname
mysystem.ibm.com
# hostname mysystem
# hostname
mysystem
```

## Prerequisites for installation of IBM Systems Director Network Control on AIX 5.3

Prepare your system before installing IBM Systems Director Network Control on AIX 5.3.

IBM Systems Director Network Control is built using the IBM XL C/C++ compiler, version 8. Because the runtime libraries for this version of the compiler are not shipped with AIX 5.3, you must download and install them yourself. In addition, AIX Asynchronous I/O must be enabled. Use the following steps to download and install the compiler, and to enable AIX Asynchronous I/O:

1. Confirm the version of the installed runtime libraries by entering the following command: `ls1pp -l | grep x1C`
2. Download version 8.0.0.0, version 8.0.0.9, or version 9.x from the following location: IBM XL C/C++ Enterprise Edition V8.0 for AIX, Runtime Environment and Utilities. IBM XL C/C++ versions 8.0.0.1 to 8.0.0.8 inclusive do not work with IBM Systems Director Network Control.

3. Follow the instructions in the readme file to install the runtime libraries. You can find the readme file at the following IBM support site: README for IBM XL C/C++ Enterprise Edition V8.0 for AIX, Runtime Environment and Utilities
4. To enable asynchronous I/O, confirm that Kernel Asynchronous I/O is installed by entering the following command: `lslpp -l |grep -i async`
5. Ensure that the output of the previous command is like this example:
 

```
bos.rte.aio 5.1.0.35 COMMITTED Asynchronous I/O Extension
devices.common.IBM.async.diag
bos.rte.aio 5.1.0.10 COMMITTED Asynchronous I/O Extension
```
6. Enter the following command: `smitty chgaio`
7. From the menu, click **STATE** to be configured at system restart.
8. Change the value for this option to available and then press **Enter**.
9. Press **F10** to exit SMIT.
10. Reboot the system to bring these changes into effect.

## IBM Systems Director Network Control device and task support

Find out which tasks are supported by IBM Systems Director Network Control V1.2 for your network devices.

The tables provide lists of network devices, separated by type, and notes which tasks are only supported by IBM Systems Director Network Control. The following tasks are included in the support tables:

### Discovery, Request Access, Inventory, Monitoring, and Alerts

Basic network management functions allow you to locate network devices, request access, gather information, and monitor status and device health. Network adapters do not require discovery. Pass-thru devices do not appear as inventory.

**Note:** To associate physical server subnets and VLANs in the **Systems by VLAN and Subnet** view, the switch inventory must be collected after network topology is collected. Correct VLAN information in views like **Systems by VLAN and Subnet** or the **VLAN ID** column in some groups require that the switch vendor support the standard SNMP Q-Bridge MIB (1.3.6.1.2.1.17.7).

### Packet Internet Groper (ping) and Traceroute

These network diagnostic tools help you test connections between network devices and troubleshoot network systems connectivity. Network diagnostic support is listed in the table, however, they cannot be used on switches configured with a privileged mode password or on IPv6 targets.

### Configuration Management

You can work with the VLAN configuration and Protocol configuration of some devices using IBM Systems Director Configuration Manager. The following tables indicate which devices support these configuration management tasks.

**Note:** Protocol configuration is not supported over IPv6.

### Context launch to vendor management

You can use launch-in-context to access vendor configuration software for some devices directly from the IBM Systems Director interface. This is a task-level launch, with device context, to the vendor management tool.

Tasks can then be completed from within the vendor management tool. This IBM Systems Director Network Control task requires additional steps, refer to the topic Configuring launch to DCFM for more information.

The supported network devices are divided into the following tables:

- Adapter devices
- BladeCenter® Ethernet switch devices
- Non-BladeCenter Ethernet switch devices
- Other network devices, including Fibre Channel over Converged Enhanced Ethernet (FCoCEE) switches, Fast Connection Failover (FCF) bridges, and Security appliances

**Note:** Some switch modules offer stacking to manage individual switches as a single bundled I/O device. IBM Systems Director supports the switch modules only in their individual (non-stacked) configurations, it does not support management of these devices in their stacked configuration.

Table 2. Adapter devices and supported network management tasks

Device	Tasks Supported	
	Inventory	Monitoring
2 Port Ethernet Expansion Card (1xE) for IBM BladeCenter	Yes	Yes
Brocade 10Gb CNA for IBM System x®	Yes	Yes
CIOv 2-port 4Gb FC HBA	Yes	Yes
CIOv 2-port 8Gb FC HBA	Yes	Yes
Emulex Virtual Fabric Adapter (CFFh) for IBM BladeCenter	Yes	Yes
Ethernet Expansion Card (CIOv) for IBM BladeCenter	Yes	Yes
Foxconn CFFv Gb Ethernet Expansion Card	Yes	Yes
Intel® 2-port 10Gb Ethernet Expansion Card (CFFh) for IBM BladeCenter	Yes	Yes
Intel PRO/1000 PF – 1P, PCIe x4, IOAT	Yes	Yes
NetXtreme II 10 GigE Express Fiber SR Adapter	Yes	Yes
QLogic 2-Port 10Gb CFFh Converged Network Adapter for IBM BladeCenter	Yes	Yes
QLogic Dual-port 10Gb CNA for IBM System x	Yes	Yes

Table 3. BladeCenter Ethernet switch devices and supported network management tasks

Device	Tasks Supported			
	Discovery, Inventory, Request Access, Monitoring, and Alerts	Ping	Traceroute	Configuration Management
Blade Network Technologies 1/10Gb Uplink Ethernet Switch Module for IBM BladeCenter (44W4404)	Yes <sup>1</sup>	Yes	Yes	Yes
Blade Network Technologies 10 Gb Uplink Ethernet Switch Module for IBM BladeCenter (32R1783)	Yes <sup>1</sup>	Yes	Yes	Yes

Table 3. BladeCenter Ethernet switch devices and supported network management tasks (continued)

Device	Tasks Supported			
	Discovery, Inventory, Request Access, Monitoring, and Alerts	Ping	Traceroute	Configuration Management
Blade Network Technologies 6-port 10 Gb Ethernet Switch Module for IBM BladeCenter (39Y9267)	Yes <sup>1</sup>	Yes	Yes	Yes
Blade Network Technologies Layer 2/3 Fiber Gb Ethernet Switch Module for IBM BladeCenter (32R1861)	Yes <sup>1</sup>	Yes	Yes	Yes
Blade Network Technologies Layer 2/3 Copper Gb Ethernet Switch Module for IBM BladeCenter (32R1860)	Yes <sup>1</sup>	Yes	Yes	Yes
Blade Network Technologies Layer 2-7 Gb Ethernet Switch Module for BladeCenter (32R1859)	Yes <sup>1</sup>	Yes	Yes	Yes
Blade Network Technologies Virtual Fabric 10Gb Switch Module for IBM BladeCenter (46C7191)	Yes <sup>1</sup>	Yes	Yes	Yes
Cisco Catalyst Switch Module 3012 for IBM BladeCenter (43W4395)	Yes	Yes	Yes	No
Cisco Catalyst Switch Module 3110G for IBM BladeCenter (41Y8523)	Yes	Yes	Yes	No
Cisco Catalyst Switch Module 3110X for IBM BladeCenter (41Y8522)	Yes	Yes	Yes	No
Cisco Nexus 4001I Switch Module for IBM BladeCenter (46M6071) <sup>2</sup>	Yes	Yes	Yes	Yes
Cisco Systems Intelligent Gb Fiber Ethernet Switch module for IBM BladeCenter (32R1888)	Yes	Yes	Yes	No
IBM BladeCenter 4-port Gb Ethernet switch module	Yes	No	No	Yes
IBM Server Connectivity Module for IBM BladeCenter (39Y9324)	Yes <sup>1</sup>	No	No	Yes
Intel Gigabit Ethernet Switch Module for IBM BladeCenter T	Yes	Yes	No	Yes
<b>Note:</b>				
1. Many hardware devices require you to install a vendor plug-in before you can request full access. For information about obtaining and installing vendor plug-ins, see the related topics at the end of this page.				
2. This switch does not support network topology functions of IBM Systems Director Network Control.				

Table 4. Ethernet switch devices, including Internet routers, and supported network management tasks

Device	Tasks Supported				
	Discovery, Inventory, Request Access, Monitoring, and Alerts	Ping	Traceroute	Configuration Management	Context launch to vendor management
Blade Network Technologies RackSwitch G8000	Yes	Yes	Yes	Yes	No

Table 4. Ethernet switch devices, including Internet routers, and supported network management tasks (continued)

Device	Tasks Supported				
	Discovery, Inventory, Request Access, Monitoring, and Alerts	Ping	Traceroute	Configuration Management	Context launch to vendor management
Blade Network Technologies RackSwitch G8124	Yes	No	No	Yes	No
IBM Ethernet Router B04M	Yes	Yes	Yes	No	No
IBM Ethernet Router B08M	Yes	Yes	Yes	No	No
IBM Ethernet Router B16M	Yes	Yes	Yes	No	No
IBM Ethernet Router B32M	Yes	No	No	No	No
IBM Ethernet Router J02M	Yes	Yes	Yes	No	No
IBM Ethernet Router J06M	Yes	Yes	Yes	No	No
IBM Ethernet Router J11M	Yes	Yes	Yes	No	No
IBM Ethernet Switch B08R	Yes	Yes	Yes	No	No
IBM Ethernet Switch B08S	Yes	Yes	Yes	No	No
IBM Ethernet Switch B16R	Yes	No	No	No	No
IBM Ethernet Switch B16S	Yes	Yes	Yes	No	No
IBM Ethernet Switch B24C (Copper)	Yes	No	No	No	No
IBM Ethernet Switch B24C (Fiber)	Yes	No	No	No	No
IBM Ethernet Switch B24X	Yes	Yes	Yes	No	No
IBM Ethernet Switch B04R	Yes	No	No	No	No
IBM Ethernet Switch B48C (Copper)	Yes	Yes	Yes	No	No
IBM Ethernet Switch B48C (Fiber)	Yes	Yes	Yes	No	No
IBM Ethernet Switch B48G	Yes	Yes	Yes	No	No
IBM Ethernet Switch B50C (Copper)	Yes	Yes	Yes	No	No
IBM Ethernet Switch B50C (Fiber)	Yes	Yes	Yes	No	No
IBM Ethernet Switch B50G	Yes	Yes	Yes	No	No
IBM Ethernet Switch J08E	Yes	Yes	Yes	No	No
IBM Ethernet Switch J48E	Yes	Yes	Yes	No	No
IBM System Storage SAN384B	Yes	No	No	Yes <sup>1</sup>	Yes <sup>2</sup>
IBM System Storage SAN768B	Yes	No	No	Yes <sup>1</sup>	Yes <sup>2</sup>
Juniper MX240 (IBM4274M02J02M)	Yes	Yes	Yes	No	No
Juniper E8216 (IBM4274E16J16E)	Yes	Yes	Yes	No	No

Table 4. Ethernet switch devices, including Internet routers, and supported network management tasks (continued)

Device	Tasks Supported				
	Discovery, Inventory, Request Access, Monitoring, and Alerts	Ping	Traceroute	Configuration Management	Context launch to vendor management
SMC Networks 8848M TigerStack II 10/100/1000	Yes	No	No	No	No
SMC Networks 8126L2 TigerSwitch 10/100/1000	Yes	No	No	No	No

**Note:**

1. IBM Systems Director Network Control V1.2 and IBM System Storage Data Center Fabric Manager (DCFM) 10.4.1a configured with SMI-S Agent are required to support Configuration Management of this device.
2. IBM Systems Director Network Control V1.2 and IBM System Storage Data Center Fabric Manager (DCFM) 10.3.2 or higher are required to launch vendor configuration management of this device.

Table 5. Supported network management tasks for other network devices including Fast Connection Failover (FCF) bridge, Fibre Channel over Converged Enhanced Ethernet (FCoCEE) switches, and Security appliances

Device	Device Type	Tasks Supported				
		Discovery, Inventory, Request Access, Monitoring, and Alerts	Ping	Traceroute	Configuration Management	Context launch to vendor management
10Gb Ethernet Pass-Thru Module for IBM BladeCenter	Pass-Thru device	Yes <sup>1</sup>	N/A	N/A	No	No
IBM Converged Switch B32	FCoCEE Switch	Yes	Yes	No	Yes <sup>2</sup>	Yes <sup>3</sup>
Cisco Nexus 5010 Switch for IBM System Storage	Standalone FCoCEE switch	Yes	Yes	Yes	No	No
Cisco Nexus 5020 Switch for IBM System Storage	Standalone FCoCEE switch	Yes	Yes	Yes	No	No
IBM Ethernet Appliance J34S	Security Appliance	Yes	No	No	No	No
IBM Ethernet Appliance J36S	Security Appliance	Yes	No	No	No	No
IBM Ethernet Appliance J56S	Security Appliance	Yes	No	No	No	No
IBM Ethernet Appliance J58S	Security Appliance	Yes	No	No	No	No
QLogic Virtual Fabric Extension Module for IBM BladeCenter (46M6172)	FCF bridge module	Yes	Yes	No	No	No

**Notes:**

1. Pass-Thru devices do not display in inventory.
2. IBM Systems Director Network Control V1.2 and IBM System Storage Data Center Fabric Manager (DCFM) 10.4.1a configured with SMI-S Agent are required to support Configuration Management of this device.
3. IBM Systems Director Network Control V1.2 and IBM System Storage Data Center Fabric Manager (DCFM) 10.3.2 or higher are required to launch vendor configuration management of this device.

## Configuring SNMP traps to enable network monitoring

Use Simple Network Management Protocol (SNMP) traps to monitor your network switches.

Network switches must be configured with the IP address of the IBM Systems Director Server as an SNMP trap address to have the events they produce logged by IBM Systems Director event logging. For fiber channel switches, or network switches that do not have IBM Systems Director I/O module plug-ins, this configuration must be performed using interfaces specific to each switch, such as a Telnet or HTTP interface. Refer to the documentation provided with the network switch for the procedure to set the SNMP trap address on those devices.

Switches that are supported by IBM Systems Director I/O module plug-ins can be configured using the IBM Systems Director Configuration Manager feature. To set the SNMP trap address on switches that are supported by IBM Systems Director I/O module plug-ins, use the following procedure:

1. If you have not already discovered the switch in Systems Director, follow these steps:
  - a. On the IBM Systems Director Welcome page, click the **System Discovery** link under the **Discovery Manager** heading.
  - b. Select **Single IPv4 address** or **Single IPv6 address** and enter the IP address of the switch you want to manage. Some switches cannot be discovered using an IPv6 address. If you are uncertain whether a switch can be discovered with its IPv6 address, or you are unable to discover a switch with its IPv6 address, try discovering it with its IPv4 address.
  - c. Set **Select resource type** to **All** and click **Discover**.
2. If you have not already obtained access to the switch, follow these steps:
  - a. In IBM Systems Director Web interface, click **Navigate Resources** and navigate to the switch that you want to access.
  - b. Right-click the switch for which you want to request access and select **Security** → **Request Access**.
  - c. On the **Request Access** page, type the user ID and password of a user with administrator privileges on the switch.
  - d. Select the access status, such as **no access** or **partially unlocked**, enter the user ID and password and select **Request Access** for IBM Systems Director to obtain access to the switch.
  - e. If the access request is successful, the access status for the managed system changes to **OK**. If the status remains **no access** or **partially unlocked**, click **Help** for more information about requesting access.
3. On the Manage tab of the IBM Systems Director Welcome page, go to **BladeCenter and System x Management** and click **Setup required for I/O module plug-ins**.
4. If the status for the switch you are configuring indicates *Required - Not installed*, you will need to perform the following steps to download and install the plug-in for the switch:
  - a. Click **Download Plug-ins** to open a web page with available plug-in download packages for various switches.
  - b. Download the package and follow the installation instructions contained in the package.
  - c. After the plug-in is installed, the status for the switch you are configuring changes to Active. It may be necessary to restart the Systems Director server for the plug-in to become active.

5. Set the SNMP trap address. If you are setting the SNMP trap address on a single switch, use option 1. If you are setting the SNMP trap address on multiple switches, use option 2.
  - Option 1: Set the SNMP trap address on a specific switch.
    - a. On the IBM Systems Director Welcome page, click the **Navigate Resources** link under the **Discovery Manager** heading.
    - b. Navigate to the network switch you are configuring by selecting **All Network Systems**.
    - c. Click the network switch name.
    - d. On the Current Configuration page, select the switch and click **Edit**.
    - e. On the Switch Module Protocol Configuration page, select the **SNMPv1 Agent** tab.
    - f. Select the entry in the Community Table and click **Edit**. The Edit Selected Community page displays.
    - g. Enter the IP address of the IBM Systems Director Server in the **Trap IP address or host name <#>** field.
 

**Note:** <#> represents the number of SNMP trap addresses (1-3) being specified.
    - h. Click **OK** to save your changes to the Selected Community.
    - i. Click the **Deploy** on the Community Table dialog
    - j. Click **OK** on the **Run <switch name> Protocol Configuration** page.
  - Option 2: Create a configuration template to set the SNMP trap address on a switch.
    - a. On the IBM Systems Director Welcome page, click the **Configuration Templates** link under the **Configuration Manager** heading.
    - b. On the Configuration Templates page, click **Create**.
    - c. On the Create page, select the appropriate template type for the switch you are configuring.
    - d. Select the network switch type for **Configuration to create a template**.
    - e. Specify a name for the template, for example ConfigTrapAddress.
    - f. Enter a description for the template and click **Continue**.
    - g. Select the **SNMPv1 Agent** tab on the Switch Module Protocol Configuration page.
    - h. Click **Create**. The Create New Community dialog displays.
    - i. Set the SNMPv1 agent to **Activate**.
    - j. Enter a **Community Name** and enter the IP address of the IBM Systems Director Server in the **Trap IP address or host name <#>** field.
 

**Note:** <#> represents the number of SNMP trap addresses (1-3) being specified.
    - k. Click **OK** to create the community.
    - l. Click **Save** to save the configuration template.
    - m. Click **Deploy**. The Run - <configuration template=""> dialog box displays.
    - n. Select the targets to which the template is to be deployed and click **Add** to add them to the Selected list.
    - o. When you have finished adding targets, click **OK**.
6. Verify that the SNMP trap address was successfully set.

- a. On the IBM Systems Director Welcome page, click the **Navigate Resources** link under the **Discovery Manager** heading.
- b. Navigate to the network switch you are configuring by clicking **All Network Systems** and selecting the network switch name.
- c. Select the **Configuration** tab and select the configuration name for the switch.
- d. Click the **SNMPv1 Agent** tab and confirm that the IP address of the IBM Systems Director Server appears in the appropriate **Trap IP address or host name** field.

#### **Related tasks**

“Test logging an SNMP trap as an event in Systems Director”

“Collecting network topology using IBM Systems Director Network Control” on page 38

## **Test logging an SNMP trap as an event in Systems Director**

Trigger events to verify your Simple Network Management Protocol (SNMP) trap configuration.

To verify SNMP trap configurations, initiate an event to generate a trap message. Methods can vary depending on the switch, but a common way to generate a trap is by repeatedly attempting to log on through the Telnet interface on the switch with an incorrect password. These steps provide one example for testing SNMP trap logging.

If an event appears in the event log for the failed login attempt Systems Director is successfully logging SNMP traps produced by the switch. If not, it is possible that the SNMP trap address is wrong or has not been correctly configured in the switch, or the switch might not generate SNMP traps for failed login attempts, and some other means of generating SNMP trap events is required.

#### **Related tasks**

“Configuring SNMP traps to enable network monitoring” on page 14

“Discovering network systems” on page 24

---

## **Installing and uninstalling IBM Systems Director Network Control**

You can install the IBM Systems Director Network Control plug-in on IBM Systems Director management servers running AIX, Linux, and Windows.

IBM Systems Director Network Control offers an InstallAnywhere interface for attended installation, or a silent install mode for unattended installation. The product is offered with a 60-day evaluation license. When purchasing a full license, you must first install the evaluation package before you can install the permanent license key. These topics provide instructions for installing the plug-in and the license key with each installation method. You can also use the uninstall instructions to remove the plug-in.

### **Installing IBM Systems Director Network Control using the installation wizard**

Download and install IBM Systems Director Network Control V1.2 with the InstallAnywhere installation wizard.

#### **Prerequisites:**

- Make sure that the target system satisfies all prerequisites. For information, see “Hardware and software requirements” on page 6 for IBM Systems Director Network Control.

Download the IBM Systems Director Network Control installation program using the following steps:

1. Go to the IBM Systems Director Downloads Web site at the following address: <http://www.ibm.com/systems/management/director/plugins/networkcontrol>
2. Click **Download** for the IBM Systems Director Network Control plug-in.
3. Select the IBM Systems Director Network Control v1.2.0 package to download:

Operating system	Download package
AIX	SysDir_NetworkControl_1_2_AIX.tar.gz
Linux on Power Systems	SysDir_NetworkControl_1_2_Linux_Power.tar.gz
Linux for System x	SysDir_NetworkControl_1_2_Linux_x86.tar.gz
Linux for System z	SysDir_NetworkControl_1_2_Linux_System_z.tar.gz
Windows	SysDir_NetworkControl_1_2_Windows.zip

4. Copy the downloaded installation package to a local drive on each IBM Systems Director Server on which you want to install IBM Systems Director Network Control. Be sure that you copy the correct package based on the operating system that is running on the IBM Systems Director Server.
5. To extract the contents of the installation package, enter the following command:

For AIX or Linux:

```
gzip -cd <package_name> | tar -xvf -
```

where <package\_name> is the file name of the installation package.

For Windows: Extract the installation package on your system.

To install IBM Systems Director Network Control, follow these steps:

1. Open a command prompt, then change to the directory that contains the IBM Systems Director Network Control installation file for the appropriate operating system.

Operating system	Installation file name
AIX	Systems_Director_Network_Control_1_2_AIX.sh
Linux on Power Systems	Systems_Director_Network_Control_1_2_Linux_Power.sh
Linux for System x	Systems_Director_Network_Control_1_2_Linux_x86.sh
Linux for System z	Systems_Director_Network_Control_1_2_Linux_System_z.sh
Windows	Systems_Director_Network_Control_1_2_Win.exe

2. Run the installation command. <installation file name> -i GUI This command launches the installation wizard and displays the Welcome page.
3. Follow the instructions in the installation wizard to install IBM Systems Director Network Control. Installation takes 30-35 minutes. When the installation is complete, and the server is restarted, IBM Systems Director Network Control is displayed in the IBM Systems Director Welcome page, and the License section of the IBM Systems Director Network Control summary

page displays an expiration date in the **License** section until you uninstall the plug-in or install a permanent license key.

4. Verify your installation:
  - a. Review the file named *installLog.txt* that appears in the DIRECTOR\_INSTALL\_LOCATION/NetworkControl directory. A user other than root or admin does not have the proper permissions to write a log to the DIRECTOR\_INSTALL\_LOCATION/NetworkControl directory. The installer log is written to the home directory of the user. Review the log file to verify successful installation. The indication of a successful installation appears under the **Summary** heading.
  - b. Check the IBM Tivoli Network Manager installation log in the following path:
    - Windows: C:\IBM\tivoli\netcool\log\install\Configuration.log and C:\IBM\tivoli\netcool\log\install\ncisetup.log
    - Linux: /opt/IBM/tivoli/netcool/log/install/Configuration.log and /opt/IBM/tivoli/netcool/log/install/ncisetup.logIf IBM Tivoli Network Manager failed to install, then uninstall IBM Systems Director Network Control V1.2, restart the IBM Systems Director Server and reinstall the plug-in.
5. The evaluation license allows a 60-day trial for evaluation purposes. If you purchased a license, follow instructions in the related task to install the permanent license key. If you are migrating from IBM Systems Director Network Control V1.1, your license key will not need to be re-installed.

#### Related tasks

“Installing the IBM Systems Director Network Control permanent license key using the installation wizard” on page 20

#### Related reference

“Hardware and software requirements” on page 6

## Installing IBM Systems Director Network Control using silent install

Download and install IBM Systems Director Network Control V1.2 using the silent (unattended) install.

#### Prerequisites:

- Make sure that the target system satisfies all prerequisites. For information, see “Hardware and software requirements” on page 6 for IBM Systems Director Network Control.

Download the IBM Systems Director Network Control installation program using the following steps:

1. Go to the IBM Systems Director Downloads Web site at the following address: <http://www.ibm.com/systems/management/director/plugins/networkcontrol>
2. Click **Download** for the IBM Systems Director Network Control plug-in.
3. Select the IBM Systems Director Network Control v1.2.0 package to download:

Operating system	Download package
AIX	SysDir_NetworkControl_1_2_AIX.tar.gz
Linux on Power Systems	SysDir_NetworkControl_1_2_Linux_Power.tar.gz
Linux for System x	SysDir_NetworkControl_1_2_Linux_x86.tar.gz

Operating system	Download package
Linux for System z	SysDir_NetworkControl_1_2_Linux_System_z.tar.gz
Windows	SysDir_NetworkControl_1_2_Windows.zip

- Copy the downloaded installation package to a local drive on each IBM Systems Director Server on which you want to install IBM Systems Director Network Control. Be sure that you copy the correct package based on the operating system that is running on the IBM Systems Director Server.
- To extract the contents of the installation package, enter the following command:

For AIX or Linux:

```
gzip -cd <package_name> | tar -xvf -
```

where <package\_name> is the file name of the installation package.

For Windows: Extract the installation package on your system.

To install IBM Systems Director Network Control, follow these steps:

- Log on to the operating system as **root** (Linux) or **Administrator** (Windows).
- Extract the contents of the downloaded installer package to a temporary directory.
- Read and acknowledge the software agreements in the */license* directory.
- In an ASCII text editor, open and edit the *installer.properties* file to enable the installation to run silently.
- Open a command prompt, then change to the directory that contains the IBM Systems Director Network Control installation file for the appropriate operating system.

Operating system	Installation file name
AIX	Systems_Director_Network_Control_1_1_AIX.sh
Linux for System p®	Systems_Director_Network_Control_1_1_Linux_Power.sh
Linux for System x	Systems_Director_Network_Control_1_1_Linux_x86.sh
Linux for System z	Systems_Director_Network_Control_1_1_Linux_System_z.sh
Windows	Systems_Director_Network_Control_1_1_Win.exe

- Open a command prompt, then change to the directory that contains the IBM Systems Director Network Control installation file for the appropriate operating system.
- Run the install command. <installation file name> -i silent
- The IBM Systems Director Network Control silent installation starts. Installation will take 30-35 minutes. After the installation is complete and the server is restarted, IBM Systems Director Network Control is displayed in the IBM Systems Director Welcome page. The IBM Systems Director Network Control summary page displays an expiration date in the **License** section until you uninstall the plug-in or install a permanent license key.
- Verify your installation:
  - Review the file named *installLog.txt* that appears in the `DIRECTOR_INSTALL_LOCATION/NetworkControl` directory. A user other than root or admin does not have the proper permissions to write a log to the `DIRECTOR_INSTALL_LOCATION/NetworkControl` directory. The installer log is

written to the home directory of the user. Review the log file to verify successful installation. The indication of a successful installation appears under the **Summary** heading.

- b. Check the IBM Tivoli Network Manager installation log in the following path:
  - Windows: C:\IBM\tivoli\netcool\log\install\Configuration.log and C:\IBM\tivoli\netcool\log\install\ncisetup.log
  - Linux: /opt/IBM/tivoli/netcool/log/install/Configuration.log and /opt/IBM/tivoli/netcool/log/install/ncisetup.log

If IBM Tivoli Network Manager failed to install, then uninstall IBM Systems Director Network Control V1.2, restart the IBM Systems Director Server and reinstall the plug-in.

10. The evaluation license allows a 60-day trial for evaluation purposes. If you purchased a license, follow instructions in the related task to install the permanent license key. If you are migrating from IBM Systems Director Network Control V1.1, your license key will not need to be re-installed.

You can now use IBM Systems Director Network Control.

#### **Related tasks**

“Installing the IBM Systems Director Network Control permanent license key using silent install” on page 21

#### **Related reference**

“Hardware and software requirements” on page 6

## **Installing the IBM Systems Director Network Control permanent license key using the installation wizard**

When the 60-day evaluation license for IBM Systems Director Network Control V1.2 expires, you can purchase a license to continue using the plug-in. If you purchase the license for IBM Systems Director Network Control, you must install the permanent license key.

#### **Prerequisites:**

The IBM Systems Director Network Control V1.2 evaluation package must be installed before you can install the permanent license key.

Contact your IBM sales specialist or IBM business partner to obtain the license key CD.

To install the IBM Systems Director Network Control permanent license key, follow these steps:

1. Copy the installation package to a local drive on each IBM Systems Director Server on which you want to install IBM Systems Director Network Control. Be sure that you copy the correct package based on the operating system that is running on the IBM Systems Director Server.

<b>Operating system</b>	<b>Installation file name</b>
AIX	Systems_Director_Network_Control_1_x_AIX_full.sh
Linux on Power Systems	Systems_Director_Network_Control_1_x_Linux_Power_full.sh
Linux for System x	Systems_Director_Network_Control_1_x_Linux_x86_full.sh

Operating system	Installation file name
Linux for System z	Systems_Director_Network_Control_1_x_Linux_System_z_full.sh
Windows	Systems_Director_Network_Control_1_x_Win_full.exe

2. Launch the installation file <installation file name> -i GUI
3. Follow the instructions in the installation wizard to install the permanent license key for IBM Systems Director Network Control. After the installation is complete, IBM Systems Director Network Control is displayed in the IBM Systems Director Welcome page, and the License section of the IBM Systems Director Network Control summary page displays **Installed** status.

#### Related tasks

“Installing IBM Systems Director Network Control using the installation wizard” on page 16

#### Related reference

“Hardware and software requirements” on page 6

## Installing the IBM Systems Director Network Control permanent license key using silent install

Download the permanent license key for IBM Systems Director Network Control V1.2 and install using the silent (unattended) install.

#### Prerequisites:

The IBM Systems Director Network Control V1.2 evaluation package must be installed before you can install the permanent license key.

Contact your IBM sales specialist or IBM business partner to obtain the license key CD.

To install the IBM Systems Director Network Control permanent license key, follow these steps:

1. Log on to the operating system as **root** (Linux) or **Administrator** (Windows).
2. Extract the contents of the downloaded installer package to a temporary directory.
3. In an ASCII text editor, open and edit the *installer.properties* file to enable the installation to run silently.
4. Follow the instructions in the sections marked Edit the following lines to enable the installation to run silently.
5. Open a command prompt, then change to the directory that contains the IBM Systems Director Network Control installation file for the appropriate operating system.

Operating system	Installation file name
AIX	Systems_Director_Network_Control_1_x_AIX_full.sh
Linux for System p	Systems_Director_Network_Control_1_x_Linux_Power_full.sh
Linux for System x	Systems_Director_Network_Control_1_x_Linux_x86_full.sh
Linux for System z	Systems_Director_Network_Control_1_x_Linux_System_z_full.sh
Windows	Systems_Director_Network_Control_1_x_Win_full.exe

6. Open a command prompt, then change to the directory that contains the IBM Systems Director Network Control installation file for the appropriate operating system.
7. Run the install command. `<installation file name> -i silent`
8. The IBM Systems Director Network Control permanent license key silent installation starts.

**Note:** The installation is complete when a file named *installLog.txt* appears in the *DIRECTOR\_INSTALL\_LOCATION/NetworkControl* directory. A user other than root/admin does not have the proper permissions to write a log to the *DIRECTOR\_INSTALL\_LOCATION/NetworkControl* directory. The installer log is written to the home directory of the user.

When the installation is complete, IBM Systems Director Network Control is displayed in the IBM Systems Director Welcome page, and the License section of the IBM Systems Director Network Control summary page displays **Installed** status.

#### **Related tasks**

“Installing IBM Systems Director Network Control using silent install” on page 18

#### **Related reference**

“Hardware and software requirements” on page 6

## **Uninstalling IBM Systems Director Network Control**

Uninstall IBM Systems Director Network Control V1.2 from your IBM Systems Director server.

### **Uninstalling IBM Systems Director Network Control on a Windows system**

Uninstall IBM Systems Director Network Control V1.2 from your IBM Systems Director server.

To uninstall IBM Systems Director Network Control on a Windows system, follow these steps:

1. Using an account with Administrator authority, log on to the operating system.
2. Click **Start** → **Settings** → **Control Panel**. The Control Panel window opens.
3. Double-click **Add/Remove Programs** or **Programs and Features**, depending on your version of Windows. The Programs window opens.
4. Select IBM Systems Director Network Control, then click **Change/Remove** or **Uninstall/Change**. The **IBM Systems Director Network Control** uninstallation wizard begins.
5. Follow the instructions and prompts to complete the uninstallation.

If you plan to reinstall the same version of IBM Systems Director Network Control, delete the `Director_Root\NetworkControl\eclipse` folder, if it exists, then restart the IBM Systems Director Server before starting the installation.

### **Uninstalling IBM Systems Director Network Control on a Linux or AIX system**

Uninstall IBM Systems Director Network Control V1.2 from your IBM Systems Director server.

To uninstall IBM Systems Director Network Control on an AIX or Linux system, follow these steps:

1. Log on to the operating system as root.

2. From the command prompt, launch the uninstaller by typing the following command and pressing **Enter**: `/opt/ibm/director/NetworkControl/Uninstall_IBM_NetworkControl/Uninstall_IBM_NetworkControl`

If you plan to reinstall the same version of IBM Systems Director Network Control, delete the `Director_Root\NetworkControl\eclipse` folder, if it exists, then restart the IBM Systems Director Server before starting the installation.

### **Uninstalling IBM Systems Director Network Control using silent (unattended) uninstall**

Uninstall IBM Systems Director Network Control V1.2 from your IBM Systems Director server.

To uninstall IBM Systems Director Network Control in unattended mode, follow these steps:

1. Using an account with Administrator authority, log on to the operating system.
2. In the `NetworkControl/uninstall_NetworkControl` directory, edit the `installer.properties` file such that: `INSTALLER_UI=silent START_SERVER=true`
3. Run `<Uninstaller_name> -i silent`

If you plan to reinstall the same version of IBM Systems Director Network Control, delete the `Director_Root\NetworkControl\eclipse` folder, if it exists, then restart the IBM Systems Director Server before starting the installation.

---

## **Migrating to IBM Systems Director Network Control V1.2**

This topic describes migrating from IBM Systems Director Network Control V1.1.

**Attention:** IBM Systems Director Network Control V1.1 is not compatible with IBM Systems Director V6.2. After you install IBM Systems Director V6.2, you will not be able to access IBM Systems Director Network Control V1.1. The Welcome page displays Network Management instead. However, you can migrate your existing IBM Systems Director Network Control V1.1 configuration to IBM Systems Director Network Control V1.2

Use the following steps to migrate your IBM Systems Director Network Control V1.1 configuration to IBM Systems Director Network Control V1.2:

1. Upgrade from IBM Systems Director V6.1.x to IBM Systems Director V6.2 as described in "Installing IBM Systems Director".
2. Install IBM Systems Director Network Control V1.2 as described in "Installing IBM Systems Director Network Control V1.2". The installer detects your IBM Systems Director Network Control V1.1 installation and automatically migrates your configuration during install.
3. If you configured IBM Systems Director Network Control V1.1 to launch DCFM, with or without single sign-on, all DCFM-related configuration settings were not preserved during the upgrade process. To reconfigure this information, open the IBM Systems Director Network Control **Summary** page and click **Launch DCFM setup**.

### Related reference

“Installing and uninstalling IBM Systems Director Network Control” on page 16

---

## Updating IBM Systems Director Network Control

IBM Systems Director update manager plug-in enables you to acquire, install, and manage updates, as well as to monitor your systems to ensure that they remain current.

Use the IBM Systems Director update manager plug-in to update IBM Systems Director Network Control V1.2. For information, see [Updating IBM Systems Director](#).

IBM Systems Director Network Control updates may require you to update IBM Systems Director Network Management as well.

After installing updates for IBM Systems Director Network Control, you can view the updates on the IBM Systems Director Welcome page.

---

## Managing network devices

Use IBM Systems Director Network Control to manage network devices in your managed systems environment.

### Discovering network systems

Use the Discovery task to collect an extended set of resources and relationships for network systems.

Use these steps to discover resources, then collect inventory for discovered resources to view device information and health.

To discover network devices, open the IBM Systems Director Network Control summary page and complete the following steps:

1. In the Manage tab of the IBM Systems Director Web interface, click **IBM Systems Director Network Control**.
2. Open the System Discovery page using either of these two methods:
  - On the **IBM Systems Director Network Control** summary page, click **System discovery** under Common tasks.
  - In the IBM Systems Director Web interface navigation area, expand **Inventory** and then click **System Discovery**.

The System Discovery page is displayed.

3. Select a discovery method:
  - Single IPv4 address
  - Single IPv6 address
  - Single host name
  - Range of IPv4 addresses
  - Range of IPv6 addresses
  - Select a discovery profile to run

The page updates to display input fields depending on your selection.

4. Enter the IP address or range, host name, or discovery profile for the system or device that you want to discover.

- For VMWare ESX and ESXi virtual resources, specify the hypervisor IP address.
- For HMC Power server virtual resources, specify the HMC IP address.

**Note:** Support for discovering network devices by IPv6 address varies, depending on the device and firmware level.

5. Select **Switch** from the **Select resource type** list. This field is not available when you use a discovery profile.
6. Click **Discover**. The **Processing discovery protocols** message is displayed and the progress of the discovery process is displayed as a spinning graphic.

**Note:** The time it takes for discovery to finish processing varies depending on such factors as network performance and the number of systems that are discovered.

7. Optional: If you want to stop the discovery process, click **Stop** during discovery.

As systems are discovered, they are displayed in the **Discovered Systems** table. Verify that the server has authority to access to the resources. After systems are discovered, collect and view inventory for those systems.

#### **Related tasks**

“Test logging an SNMP trap as an event in Systems Director” on page 16

“Collecting network topology using IBM Systems Director Network Control” on page 38

## **Collecting and viewing inventory for network systems**

Use the View and Collect Inventory task in IBM Systems Director Network Control to view and manage an extended set of resources and relationships for network systems that have already been discovered.

#### **Prerequisites:**

Before you can view inventory for a network device, you must discover that network device using System Discovery. Inventory collection uses inventory collection profiles. You can use an existing profile to collect inventory for a system. If the inventory collection profile does not exist for the type of inventory data you want to collect, you must first create the inventory collection profile and make sure that it contains the appropriate settings.

#### **Notes:**

##### **Note:**

- Inventory of network resources is obtained from the devices using the SNMP protocol. In some cases, certain devices may not report some values over SNMP, and the corresponding inventory fields in IBM Systems Director will be blank.
- Inventory displays for only those systems that are in a state other than no access. To change the access state, select the system or systems and click **Actions** → **Security** → **Request Access**.
- To associate physical server subnets and VLANs in the **Systems by VLAN and Subnet** view, the switch inventory must be collected after network topology is collected. Correct VLAN information in views like **Systems by VLAN and Subnet** or the **VLAN ID** column in some groups require that the switch vendor support the standard SNMP Q-Bridge MIB (1.3.6.1.2.1.17.7).

To collect inventory for one or more network systems, complete the following steps:

1. Open the View and Collect Inventory page using either of these two methods:
  - On the Welcome page, click **Collect and view inventory** under Optional tasks.
  - In the IBM Systems Director Web interface navigation area, expand **Inventory** and then click **View and Collect Inventory**.

The View and Collect Inventory page is displayed.

2. In the **Target Systems** list, select the system for which you want to view or collect inventory data. If the target system that you want to view is not in the target systems list, complete the following steps to add the system to the list.
  - a. Click **Browse** to open the Context Chooser. The Context Chooser displays a list of system groups.
  - b. In the list of groups, drill down to the individual target system for which you want to view inventory data in the group that contains that target system.
  - c. Select one or more target systems that you want to add.
    - For VMWare ESX and ESXi virtual resources, select the Operating System resource.
    - For HMC Power server virtual resources, select the HMC resource.

**Note:** You can select the entire group or you can drill down to select individual target systems as targets within a group.

- d. Click **Add**. The selected target systems are displayed in the **Selected** list.
  - e. Click **OK**.
3. In the **Manage inventory profiles** list, select the inventory profile that you want to use.
  4. Click **Collect Inventory**. The Run - Collect Inventory page is displayed.
  5. Use the Run - Collect Inventory page to set up optional functions and options of your inventory collection task:

#### **Schedule**

Use the Schedule tab to set the inventory collection task to run immediately or at a specified time and date in the future. You can also schedule the task to repeat at a specified frequency.

#### **Notification**

Use the Notification tab to choose options for an e-mail notification that you can receive as the inventory collection process progresses.

#### **Options**

Use the Options tab to specify the time to use for the system time and how to handle unavailable systems.

6. When you are finished with the Run - Collect Inventory page, click **OK**. An inventory collection job is created and a message is displayed with buttons and information about the job.

**Note:** Click **Display Properties** if you want to view the properties of the job. The Active and Scheduled Jobs page is displayed and provides information about the job including status, progress, a list of targets, a history, and error logs.

When inventory collection is completed, you can view the inventory data list and table by clicking **Refresh View**.

## Configuring network systems with configuration plans and templates

You can use the configuration manager to create, view, edit, delete, deploy, and schedule VLAN and protocol configuration templates to be deployed on supported network resources.

See the related reference topic, *Device and task support*, to determine whether your hardware devices support configuration manager tasks, and whether there are configuration prerequisites for your network device. The support tables indicate which devices support these configuration management tasks.

**Note:** Protocol configuration is not supported over IPv6.

To create a configuration template, complete the following steps:

1. From the Network Management or IBM Systems Director Network Control summary page, click the Common Tasks link **View and apply Ethernet network templates**. The **Configuration Templates** page is displayed.
2. Click **Actions** → **Create**. The **Create Template** page is displayed.
3. Choose a target type in the **Template type** field. You can use the following target types for network systems:
  - Ethernet Switch
  - Fibre Switch
  - InfiniBand Switch
  - Storage Switch
4. Select a configuration template type from the **Configuration** drop-down list.
5. Type a unique name for the new configuration template. The name must be unique and have a maximum length of 100 characters. The name of the configuration template cannot contain the following XML special characters:
  - The ampersand character (&)
  - The apostrophe or single quotation mark character (')
  - The double quotation mark character (")
  - The greater-than character (>)
  - The less-than character (<)
  - The vertical bar character (|)
  - The back slash character (\)
  - The slash character (/)
  - The asterisk character (\*)
  - The colon character (:)
  - The question mark character (?)
  - The percent character (%)
6. Type a meaningful description for the new configuration template. The maximum length is 500 characters. The description of the configuration template cannot contain the following XML special characters:
  - The ampersand character (&)
  - The apostrophe or single quotation mark character (')
  - The double quotation mark character (")

- The greater-than character (>)
  - The less-than character (<)
7. Optional: If you want this configuration template to be run automatically when a new device with a type that matches this configuration template is added or removed, or when an event related to this type of device occurs, select **Automatically deploy this configuration template when notified of a matching resource**.  
If you enable automatic deploy, the template is appended to the end of the automatic deploy sequence list for the relevant type. To change the order of the list, go to **Actions** → **Automatic Deploy Sequence**.
  8. Click **Continue**. The Configuration Settings page is displayed. The configuration settings available depend on the Configuration type selected on the **Create Template** page.
  9. Enter configuration information.
  10. Click **Save** to create configuration template. The new configuration template displays in the configuration template table.

After you define the configuration template, you can deploy it to a target system. You can use configuration plans to deploy the template to target systems, or you can manually deploy the template. See the related tasks to deploy a configuration template.

## Managing network systems health

IBM Systems Director provides facilities to monitor and troubleshoot network systems health.

### Prerequisites:

Before you can view and manage network systems health, you must complete the following tasks:

- Discover and inventory the devices you want to monitor
- Configure devices to send SNMP trap events to IBM Systems Director for monitoring.

If you do not configure SNMP traps properly, device status always displays OK, and cannot alert you to device problems.

You can use IBM Systems Director Network Control to monitor the health of your network systems.

1. On the Welcome page, click the **Manage** tab.
2. Select **IBM Systems Director Network Control**. The IBM Systems Director Network Control summary page appears.
3. The IBM Systems Director Network Control summary page displays a pie chart to represent the status of your network devices.

There are four status categories, represented by icons:

### Status chart

A pie chart represents the status of your network devices. To see your resources based on status, click one of the links in the list or its corresponding section in the pie chart.

There are four status categories, represented by icons:



**Critical**



**Warning**



**Informational**



**OK**

#### **Devices with no inventory collected**

Number of discovered network devices for which inventory has not been collected. Click to open a table view.

To see your resources based on status, click one of the links in the list or its corresponding section in the pie chart. You can also use the Common tasks links on the page to quickly access frequently used tasks such as System discovery, Monitors, Thresholds, and Event logs.

## **Managing hardware supported by DCFM**

Use launch tasks to view and work with Brocade hardware in your network using IBM System Storage Data Center Fabric Manager (DCFm).

If your network includes hardware that is supported by DCFM, you can use IBM Systems Director Network Control to work with the IBM System Storage Data Center Fabric Manager (DCFm) server for device configuration. IBM Systems Director Network Control supports the following methods of integrating with DCFM:

#### **Context launch to vendor configuration**

You can select actions on some network devices and launch the DCFM user interface to complete the operations. Operations such as Converged Enhanced Ethernet (CEE) configuration or network topology, which

support launch-in-context, are indicated by an icon  in the System Configuration menu for hardware that is supported by DCFM. For launch-in-context operations, a single sign-on (SSO) authentication can be configured to allow the context-specific DCFM screens to be displayed directly. Without SSO, a DCFM user ID and password are required each time you use launch-in-context actions.

After you set up IBM Systems Director Network Control to launch DCFM, you can open the DCFM interface to configure supported hardware.

#### **Template-based configuration management**

You can use the IBM Systems Director interface to perform template-based configuration functions that are integrated directly into the user interface of IBM Systems Director Network Control. You can configure CEE quality of service (QoS), VLANs, Link Layer Discovery Protocol (LLDP), and port settings using configuration templates to deploy new or modified configurations to Brocade CEE switches. You can also view configuration properties for the managed devices.

After you set up IBM Systems Director Network Control and DCFM to enable the DCFM SMI Agent (CIMOM) service, you can perform template-based configuration functions.

Both of these methods require configuration of the DCFM Server and IBM Systems Director Network Control to enable communication between the applications. Use the following topics to enable these network device management features:

**Related tasks**

“Enabling DCFM for single sign-on” on page 32

“Updating the single sign-on configuration” on page 34

**Related reference**

“Troubleshooting DCFM problems” on page 44

## **Set up IBM System Storage Data Center Fabric Manager (DCFM) to integrate with IBM Systems Director Network Control**

Complete this one-time configuration to enable IBM System Storage Data Center Fabric Manager (DCFM) to work with hardware that is supported by DCFM.

You must have the following products installed on your systems:

- IBM Systems Director Network Control V1.2
- IBM System Storage Data Center Fabric Manager (DCFM)

If your network includes hardware that is supported by DCFM, you can use IBM Systems Director Network Control to work with the IBM System Storage Data Center Fabric Manager (DCFM) application to do certain configuration-oriented tasks. The DCFM Server is required for launch-in-context tasks, and both the DCFM Server and the DCFM SMI Agent (CIMOM) service are required for configuration tasks that are integrated directly in the IBM Systems Director Network Control user interface. Launch-in-context tasks display the DCFM client interface on the same server where the IBM Systems Director console is running. Launching tasks to DCFM requires Sun Java 6 Version 16 or higher installed on the server running the Director console web browser. To obtain versions of the Java Runtime, you can visit the Sun Java archive: \*. IBM System Storage Data Center Fabric Manager (DCFM) 10.4.1a is required for integrated configuration tasks. DCFM 10.3.2 can be used for launch-in-context, but will not support the template-based configuration tasks.

For detailed information about the systems supported by IBM Systems Director Server, see Supported IBM systems and products.

To configure IBM Systems Director Network Control to operate with DCFM for certain tasks, complete the following steps:

1. In the Manage tab of the IBM Systems Director Web interface, click **IBM Systems Director Network Control**.
2. On the IBM Systems Director Network Control summary page, click **Launch DCFM setup** from the Common Tasks list.
3. Follow the on-screen instructions to specify the DCFM host and DCFM port information.

**Note:**

- Launch-in-context-based integration requires that you connect to the IBM Systems Director server with a fully qualified host name or an IPv4 address to access the server. An IPv6 address is not supported. For example, use `https://system.domain.com:8422/ibm/console/` or `https://111.222.33.44:8422/ibm/console`.

- Single sign-on requires that you connect to the IBM Systems Director server with a fully qualified host name to access the server instead of an IP address. For example, use `https://system.domain.com:8422/ibm/console/` instead of `https://111.222.33.44:8422/ibm/console`.
4. (Optional) To enable template-based configuration functions for DCFM hardware, enter the DCFM user ID, DCFM password, and SMI Agent port fields.
  5. (Optional) You can choose to enable single sign-on for DCFM. If you activate this option, additional configuration steps are required. If you enable single sign-on, specify the SSO authentication information.

**Note:** If you do not enable single sign-on, each time you use DCFM launch-in-context, a panel displays requesting your DCFM server user ID and password. After you have connected to DCFM once, the DCFM server stores and pre-fills the login fields.

6. Click **OK** to save DCFM Launch configuration.
7. If you changed the single sign-on setting, you must restart IBM Systems Director.

#### **Next steps:**

(Optional) If you are configuring single sign-on, you must complete additional configuration steps as described in the topic “Configuring single sign-on for IBM System Storage Data Center Fabric Manager (DCFm).” Proceed to the next step: Enable DCFM for single sign-on.

After you complete this task, you can work with hardware that is supported by DCFM.

#### **Related tasks**

“Configuring users for single sign-on” on page 33

“Updating the single sign-on configuration” on page 34

#### **Related reference**

“Troubleshooting DCFM problems” on page 44

### **Configuring single sign-on for IBM System Storage Data Center Fabric Manager (DCFm):**

Learn more about how to configure single sign-on to simplify requests to launch the IBM System Storage Data Center Fabric Manager (DCFm) configuration interface.

Single sign-on (SSO) is an authentication process you can use to access more than one system or application by entering a single user ID and password. It is used to automate access to multiple resources by requiring a user to authenticate only once.

**Note:** If you do not enable single sign-on, each time you use DCFM launch-in-context, a panel displays requesting your DCFM server user ID and password. After you have connected to DCFM once, the DCFM server stores and pre-fills the login fields.

The single sign-on process uses one basic authentication user ID to enable secure authentication between the IBM Systems Director server and the DCFM server. As part of SSO setup, define the same user ID and password to both IBM Systems

Director and DCFM. Additionally, for each IBM Systems Director user that you want to participate in single sign-on launch to DCFM, you must ensure that user ID is defined in both IBM Systems Director and DCFM with the same credentials.

To configure single sign-on, you must complete the following tasks:

1. Configure IBM Systems Director Network Control to launch DCFM for supported hardware.
2. Enable DCFM for single sign-on.
3. Configure users for single sign-on.
4. Select a DCFM launch-in-context action to verify the DCFM SSO is working. See “Context launch to configure switches managed by DCFM” on page 35 for a list of supported actions.

**Related tasks**

“Updating the single sign-on configuration” on page 34

**Related reference**

“Troubleshooting DCFM problems” on page 44

*Enabling DCFM for single sign-on:*

Learn more about how to configure IBM System Storage Data Center Fabric Manager (DCFMM) to allow single sign-on.

**Prerequisites:**

You must have the following products installed on your systems:

- IBM Systems Director Network Control V1.2
- IBM System Storage Data Center Fabric Manager (DCFMM) 10.4.1a, available from \*. DCFMM 10.3.2 can be used for launch-in-context, but does not support the template-based configuration tasks.

**Note:** You can only configure one IBM Systems Director server to work with a single DCFMM server.

Although single sign-on is not required, it creates a more seamless experience between the DCFMM server and IBM Systems Director. There are several functions within the IBM Systems Director Network Control that launch the DCFMM client. If single sign-on is not enabled, each time the DCFMM client is launched, you must verify your DCFMM credentials. By enabling single sign-on, DCFMM can authenticate against IBM Systems Director Network Control and launch directly into the specified dialog. This reduces the number of authentication steps required by the user.

To configure IBM System Storage Data Center Fabric Manager (DCFMM) to enable single sign-on (SSO), follow these steps:

**Note:** These instructions assume the DCFMM server runs on Windows. If your DCFMM server is running on another platform, similar steps are needed, except the script must be run in a shell with `sh tpcssosetup`. Refer to the DCFMM Enterprise User Manual for detailed single sign-on configuration instructions.

1. Run the `tpcssosetup` command
  - a. Copy the file `<DIRECTOR ROOT>\lwi\security\keystore\ibmjssse2.jks` from the IBM Systems Director Server to the `<DCFMM Root>\bin\tpc` folder on the DCFMM server.

- b. Open a console or command prompt for the system that hosts the DCFM Server and navigate to the DCFM directory <DCFm Root>\bin\tpc\
- c. Run the command *tpcssosetup* with the following parameters:
  - First parameter: IBM Systems Director server IP address (ex. 111.222.33.44)
  - Second parameter: IBM Systems Director HTTPS port number (typically 8422)
  - Third parameter: Truststore file that was moved from the IBM Systems Director Server to the <DCFm Root>\bin\tpc folder on the DCFM Server (ibmjsse2.jks)
  - Fourth parameter: The password for the truststore file. The default password for the truststore is 'ibmpassw0rd'. Use the default password unless you used the command-line interface to update the truststore password.
  - Fifth parameter: Single sign-on user ID. This parameter must match the value defined in the Launch DCFM Setup page.
  - Sixth parameter: Single sign-on password. This parameter must match the value defined in the Launch DCFM Setup page

Example command: 'tpcssosetup 111.222.33.44 8422 ibmjsse2.jks  
ibmpassw0rd Administrator Passw0rd'

2. Create or modify a user ID account DCFM. To do this, go to the DCFM client application, select **Open Server** → **Users** and add or edit a user ID to be used for single sign-on. The user ID and password must match the SSO User ID and SSO password that are configured on the **Setup Launch to DCFM** page in the IBM Systems Director Network Control interface.
3. Ensure that any switches that are to be managed are added to the DCFM client. Add switch/fabric into DCFM by selecting **Discovery** → **Setup** → **Add Fabric**.
4. Restart the DCFM Service.

**Next step:**Configure users for single sign-on.

#### **Related tasks**

“Managing hardware supported by DCFM” on page 29

“Updating the single sign-on configuration” on page 34

“Configuring users for single sign-on”

#### **Related reference**

“Troubleshooting DCFM problems” on page 44

*Configuring users for single sign-on:*

Configure user IDs to allow users to sign in to the IBM Systems Director Server and launch DCFM configuration using the same credentials.

#### **Prerequisites:**

You must have the following products installed on your systems:

- IBM Systems Director Network Control V1.2
- IBM System Storage Data Center Fabric Manager (DCFm) Server 10.4.1a

Single sign-on (SSO) allows users to sign in seamlessly from IBM Systems Director Network Control into IBM System Storage Data Center Fabric Manager (DCFm). When configuring DCFm, one user ID is specified to be used as the basic authentication user ID to handle secure communication between the two systems.

Additional IBM Systems Director users can be configured to use single sign-on to launch DCFM. Typically, a user is assigned a unique user ID and password for signing in to IBM Systems Director. When using SSO, you map the user ID to the associated DCFM account. To configure other users to authenticate to DCFM with SSO, follow these steps:

1. Configure the user to use IBM Systems Director.
2. (Optional.) If needed, create a user ID on the IBM Systems Director host system. The user ID and password must match the SSO user ID and SSO password that are configured on the **Setup Launch to DCFM** page in the IBM Systems Director Network Control interface.
3. Assign the user the 'smuser' role in Windows, or the 'smuser' group in Linux.

**Next steps:** Select a DCFM launch-in-context action to verify the DCFM SSO is working. See “Context launch to configure switches managed by DCFM” on page 35 for a list of supported actions.

#### **Related tasks**

“Set up IBM System Storage Data Center Fabric Manager (DCFM) to integrate with IBM Systems Director Network Control” on page 30

“Enabling DCFM for single sign-on” on page 32

“Updating the single sign-on configuration”

#### **Related reference**

“Troubleshooting DCFM problems” on page 44

*Updating the single sign-on configuration:*

Manage the single sign-on configuration used to launch the IBM System Storage Data Center Fabric Manager (DCFM) configuration interface.

To complete this task, you must have the following products installed with single sign-on (SSO) configured:

- IBM Systems Director Network Control V1.2
- IBM System Storage Data Center Fabric Manager (DCFM)

**Note:** Single sign-on requires the following:

1. The DCFM host name must be specified as a fully-qualified host name, not an IP address.
2. The SSO domain must match the domain specified in the DCFM host name field.
3. To use DCFM launch-in-context operations, you must connect to IBM Systems Director using the fully-qualified host name, for example `https://myhost.mydomain.com:8422/ibm/console` instead of `https://111.222.33.44:8422/ibm/console`.

You can configure IBM Systems Director Network Control to log on and launch the DCFM configuration interface using single sign-on. Single sign-on is not required, but it creates a more seamless experience between the DCFM server and IBM Systems Director. There are several functions within the IBM Systems Director Network Control that launch the DCFM client. If single sign-on is not enabled, each time the DCFM client is launched it requests DCFM credentials from the user. By enabling single sign-on, DCFM can authenticate the user against IBM Systems Director Network Control and launch directly into the specified dialog. This reduces the number of authentication steps required by the user.

**Note:** The SSO user ID specified with the setup must be an IBM Systems Director user ID, and the same user ID and password must exist within the DCFM Server. To enable or change single sign-on configuration from IBM Systems Director Network Control, use the following steps:

1. In the Manage tab of the IBM Systems Director Web interface, click **IBM Systems Director Network Control**.
2. On the IBM Systems Director Network Control summary page, click **Launch DCFM setup** from the Common Tasks list.
3. Select **Enable single sign-on**.
4. To set or change the single sign-on values, enter the SSO user ID, password, and domain information.
5. Stop and restart the IBM Systems Director server.
6. If you change the SSO user ID or SSO password you must run the `tpcssosetup` command again on the DCFM server. For more details on running this command, click the **Enabling DCFM for single sign-on** topic in the related tasks section.

After you have configured the IBM Systems Director Network Control single sign-on properties, ensure that your DCFM user ID and password settings match the values you set in this task.

#### **Related tasks**

“Set up IBM System Storage Data Center Fabric Manager (DCFM) to integrate with IBM Systems Director Network Control” on page 30

“Enabling DCFM for single sign-on” on page 32

“Configuring users for single sign-on” on page 33

“Managing hardware supported by DCFM” on page 29

#### **Related reference**

“Troubleshooting DCFM problems” on page 44

“Configuring single sign-on for IBM System Storage Data Center Fabric Manager (DCFM)” on page 31

“IBM Systems Director Network Control troubleshooting” on page 40

### **Context launch to configure switches managed by DCFM**

Launch tasks to view and work with hardware that is supported by DCFM in your network using IBM System Storage Data Center Fabric Manager (DCFM).

Context launch is a task-level launch, with device context, to the DCFM user interface. Tasks can then be completed from within the DCFM user interface.

**Prerequisites:** You must have the following products installed on your systems:

- Install IBM Systems Director Network Control V1.2.
- Install IBM System Storage Data Center Fabric Manager (DCFM)
- Configure launch to DCFM.
- Perform discovery and inventory on the target switch in IBM Systems Director, and discover the switch in DCFM.

To launch network device management tasks from IBM Systems Director Web interface and complete the following steps:

1. Expand **Navigate Resources** to locate a managed endpoint that is supported by DCFM.

2. Right-click the managed endpoint and select a task by selecting **System Configuration**, followed by one of the following operations.
  - CEE Configuration
  - Device Connectivity
  - Fabric Port Report
  - Network Topology
  - Top N Talkers
  - Trace Route

Operations that support launch-in-context are indicated by an icon 

3. If you have not configured single sign-on, a DCFM login window displays, requesting your DCFM server user ID and password. After you have connected to DCFM once, IBM Systems Director stores and pre-fills the login fields.

**Note:** It may take several minutes for the DCFM application to load, and additional screens may open before the DCFM screen appears.

**Related reference**

- “Launch-in-context operations fail” on page 48
- “Troubleshooting DCFM problems” on page 44

**Use templates to configure switches managed by DCFM**

Use the IBM Systems Director interface to perform template-based configuration functions on hardware that is supported by DCFM.

**Prerequisites:** You must have the following products installed on your systems:

- Install IBM Systems Director Network Control V1.2.
- Install IBM System Storage Data Center Fabric Manager (DCFM) Server 10.4.1a and DCFM SMI Agent (CIMOM) service
- Configure launch to DCFM and enable DCFM SMI Agent (CIMOM) service.
- Perform discovery and inventory on the target switch in IBM Systems Director, and discover the switch in DCFM.

You can use the IBM Systems Director interface to perform template-based configuration functions that are integrated directly into the user interface of IBM Systems Director Network Control. You can configure CEE quality of service (QoS), VLANs, Link Layer Discovery Protocol (LLDP), and port settings using configuration templates to deploy new or modified configurations to Brocade CEE switches.

To perform template-based configuration operations, complete the following steps in the IBM Systems Director Web interface:

1. In the IBM Systems Director Web interface navigation area, select **System Configuration** → **Configuration Templates**.
2. On the **Configuration Templates** page, click **Create**.
3. Specify the following details on the **Create** page, then click **Continue**:

Option	Description
Template type	Ethernet switch

Option	Description
Configuration to create a template	Select the hardware type: <ul style="list-style-type: none"> <li>• IBM Converged Switch B32 Configuration</li> <li>• IBM System Storage SAN384B Configuration</li> <li>• IBM System Storage SAN768B Configuration</li> </ul>
Configuration template name	Unique template name
Configuration template description (optional)	Description of the template

The **CEE Switch Configuration wizard** appears.

4. Use the wizard to define the configuration tasks for the CEE switch configuration template, and click **Finish** to save the template. The new configuration template appears on the **Configuration Templates** page.
5. To deploy the template, select the configuration template from the list and click **Actions** → **Deploy**. The **Deploy Configuration Templates Job** page opens.
6. Specify target systems and choose **Run Now** or **Schedule**.
7. The current configuration of the CEE switch, including the ports, VLAN, QoS, and LLDP settings displays.

To view the current configuration of a CEE switch, right-click hardware that is supported by DCFM from a **Navigate Resources** page and select **System Configuration** → **Current Configuration**. The current configuration of the CEE switch displays, including the VLAN, QoS, LLDP, and port settings.

#### Related reference

“Switch login fails during template-based configuration” on page 50

“Troubleshooting DCFM problems” on page 44

## Working with network device groups

Use the **Navigate Resources** task to view and manage network systems in IBM Systems Director.

You must have IBM Systems Director Network Control installed. Refer to “Installing and uninstalling IBM Systems Director Network Control” on page 16 for installation and prerequisites information.

Before you can view a network resource, you must discover and collect the inventory data for that resource, and you must configure devices to send SNMP trap events to IBM Systems Director for monitoring.

To work with a network device group, follow these steps

1. From the IBM Systems Director Network Control **Summary page**, select one of these network system groups from the **Manage** task list:
  - Ethernet Switches
  - Ethernet to Fibre Channel Bridges
  - Fibre Channel over Ethernet Switches
  - Subnets
  - VLANs
  - Systems by VLAN and Subnet

2. Alternate methods: You can also access device groups by from the navigation area by selecting **Navigate Resources** → **Groups by System Type** → **Network Systems**. To view Systems by VLAN and Subnet, expand **Inventory** → **Views** → **Systems by VLAN and Subnet**.
3. To work with resources displayed in the selected group, right-click a system or use the **Actions** menu and select an action.

#### Related tasks

“Collecting and viewing network topology inventory”

## Collecting and viewing network topology inventory

Use IBM Systems Director Network Control to work with network inventory in a topology view.

#### Related tasks

“Working with network device groups” on page 37

### Collecting network topology using IBM Systems Director Network Control

Collect topological information about the network devices in your IBM Systems Director Network Control environment.

To complete this task you must meet the following prerequisites:

- Install IBM Systems Director Network Control V1.2.
- Enable SNMP on target devices. You cannot view relationships for target devices that do not have SNMP enabled, including operating systems.
- Discover and collect inventory on the devices you want to include in your topology collection and views.

**Note:** Network topology function is not available on Linux on Power Systems.

1. Open the IBM Systems Director Network Control summary page.
2. In the **Status** section, select **Network Topology Inventory** from the **Common Tasks** list. The **Network Topology Inventory** page opens.
3. Select **Collect network topology for SNMP-enabled resources** and use the **Add** and **Remove** buttons to select systems or groups to scan for topology information about discovered devices.
4. Click **Collect Topology**. The **Run** page appears.
5. Specify when to run this job and click **OK**.
  - Run now
  - Schedule

Job status is displayed in the Active and Scheduled job list.

#### Note:

- The collection job can take several hours to complete depending on the number of devices. To monitor job progress, refer to the task topic for viewing the Collect Network Topology activation log.
- The same SNMP security credentials are required for all managed endpoints in the same subnet as the IPv4 resources submitted to the topology collection job.

You can now view your network topology.

### Related tasks

“Discovering network systems” on page 24

“Viewing network topology using IBM Systems Director Network Control”

“Configuring SNMP traps to enable network monitoring” on page 14

### Viewing Collect Network Topology activation log:

View the activation log to monitor network topology collection job progress.

You must start a task to collect network topology before viewing the log file.

To view the progress of a collect network topology task, follow these steps:

1. In the IBM Systems Director Web interface navigation area, click **Task Management** → **Active and Scheduled Job**.
2. In the Active and Scheduled Jobs table, double-click the Collect Network Topology job to view the job properties.
3. Select the **Logs** tab and review the activation logs.

### Viewing network topology using IBM Systems Director Network Control

View a graphical representation of the network devices in your IBM Systems Director Network Control environment.

**Prerequisites:** You must collect network topology data before viewing your network topology.

**Note:** Network topology function is unavailable on Linux on Power Systems.

When collecting topology inventory, the target resources must be SNMP-enabled, but SNMP is not required to view network topology. Operating system resources can be used when collecting the information, but do not display any topology information in the system-level view. Use the server resource associated with the operating system resource when using the system-level view for network topology information. The operating system resource is valid for the port-level and subnet views.

To view Layer 2 network topology inventory, complete the following steps:

1. Open the IBM Systems Director Network Control summary page.
2. In the **Status** section, select **Network Topology Inventory** from the **Common Tasks** list. The **Network Topology Inventory** page opens.
3. Select **View Network Topology** and use the **Add** and **Remove** buttons to select 1-5 targets for which you want to view the topology.
4. Specify the network topology perspective.
  - **System-level:** A high-level view, showing systems and the relationships between them. This view displays up to 12 devices in the topology of the 1-5 targets selected.
  - **Port-level:** This view provides low-level detail, for example LAN Connection 1, on system 1, is connected to port 3, on switch 3.
  - **Subnet:** A system-level view, showing all systems in the same subnets as the selected systems.
5. Click **View Topology**. The **Topology Viewer** page opens to display the specified topology.

## Related tasks

“Collecting network topology using IBM Systems Director Network Control” on page 38

---

## IBM Systems Director Network Control troubleshooting

This section provides information for specific problems and workarounds associated with IBM Systems Director Network Control in the IBM Systems Director environment.

The IBM Systems Director Network Control summary page displays a pie chart to represent the status of your network devices. There are four status categories, represented by icons:

### Status chart

A pie chart represents the status of your network devices. To see your resources based on status, click one of the links in the list or its corresponding section in the pie chart.

#### Note:

Before you can view and manage network systems health, you must complete the following tasks:

- Discover and inventory the devices you want to monitor
- Configure devices to send SNMP trap events to IBM Systems Director for monitoring.

If you do not configure SNMP traps properly, device status always displays OK, and cannot alert you to device problems.

There are four status categories, represented by icons:

### Status chart

A pie chart represents the status of your network devices. To see your resources based on status, click one of the links in the list or its corresponding section in the pie chart.

There are four status categories, represented by icons:



**Critical**



**Warning**



**Informational**



**OK**

### Devices with no inventory collected

Number of discovered network devices for which inventory has not been collected. Click to open a table view.

To see your resources based on status, click one of the links in the list or its corresponding section in the pie chart. You can also use the Common tasks links on the page to quickly access frequently used tasks such as System discovery, Monitors, Thresholds, and Event logs. The following topics describe specific problems and troubleshooting techniques.

#### **Related tasks**

“Updating the single sign-on configuration” on page 34

## **Using IBM Systems Director Network Control diagnostic tools**

Use ping and traceroute utilities in IBM Systems Director to confirm network connectivity and response time from one endpoint to another.

You must have IBM Systems Director Network Control installed. Refer to “Installing and uninstalling IBM Systems Director Network Control” on page 16 for installation and prerequisites information.

To use these diagnostic tools, you must first discover supported Ethernet-type network systems. The supported systems must have an access state of OK.

Use these tools to test connections between network devices and troubleshoot network systems connectivity. Ping and traceroute from the Network Diagnostics page are not supported for all hardware types, and diagnostic tools cannot be used on switches configured with a privileged mode password. Refer to the device and task support page for details.

1. In the IBM Systems Director Web interface navigation area, click **Navigate Resources**.
2. In the Navigate Resources groups view, select **All Network Systems** and choose **View Members** from the **Actions** menu.
3. Right-click a supported network system and select **System Status and Health** → **Network Diagnostics**.
4. Use the Network Diagnostics page to activate ping or traceroute on a target system.

**Note:** Ping and traceroute are not supported for IPv6 address targets.

#### **Related reference**

“IBM Systems Director Network Control device and task support” on page 9

## **Duplicate events display in the event log view**

This problem affects all IBM Systems Director Network Control V1.2 users.

### **Problem**

There are two events reflected on the IBM Systems Director events log page for each trap generated from the switch. One of the events is the mapped event and the other event is the unmapped event. The mapped event has all the properties of the event populated with appropriate values such as the sender, text, severity, date, and time and details of the trap. The unmapped event has "No Text" as the text of the event and the severity is "Unknown" in this case. The unmapped event entry is a duplicate entry for the mapped event entry on the event log page.

### **Resolution**

Ignore the event with the name “No Text”.

## Empty window is displayed or nothing happens

This problem affects the Microsoft® Internet Explorer and Mozilla Firefox browsers.

### Problem

When you try to start a launched task, an empty window is displayed or nothing happens in your Web browser.

### Resolution

Complete one or more of the following actions:

#### For all browsers

- Java Web Start (JWS) software is required to enable the launched-tasks feature in IBM Systems Director. If the error message includes a link to a Web site, click the link to download JWS. Alternatively, complete the steps in “Downloading Java Web Start” in the *IBM Systems Director Systems Management Guide*.
- Make sure that the system on which IBM Systems Director Server is installed is not blocked by a pop-up blocker on your browser system. For example, check for a pop-up blocker displayed under the Address bar, and make sure it is turned off.

#### For Internet Explorer

- Click **Tools** → **Internet Options** → **Advanced**. Make sure that **Do not save encrypted pages to disk** is *not* selected.
- (Internet Explorer 7 only) Complete the following steps:
  1. Click **Tools** → **Internet Options** → **Security**.
  2. Click **Custom level**.
  3. In the Security Settings - Internet Zone window, make sure that **Downloads** → **Automatic prompting for file downloads** → **Enable** is selected.

- The .jnlp extension might not be mapped to the Java Web Start executable file.

To map the .jnlp extension to the Java Web Start executable file, complete the procedure detailed in “Updating the Microsoft Internet Explorer Web browser to use the IBM Java Web Start program” in the *IBM Systems Director Systems Management Guide*.

- The .jnlp extension is mapped to the Java Web Start executable file, but the Launch action is not defined.

To define the Launch action, complete the following steps:

1. In Windows Explorer, click **Tools** → **Folder Options**.
2. Click the **File Types** tab, select JNLP in the **Registered file types** list, and click **Advanced**.
3. In the Edit File Type window, clear the **Confirm open after download** check box and click **New**.
4. In the New Action window, specify the following information and click **OK**:
  - In the **Action** field, type **&Launch**.
  - In the **Application used to perform action** field, click **Browse**, select and specify the javaws.exe under a JRE that is installed on your browser system using the following format:

```
"XXXXXXXX" "%1"
```

- Select **Use DDE**. The window expands.
  - In the **Application** field, type javaws.
  - In the **Topic** field, type System.
- 5. In the Edit File Type window, click **OK**.
- 6. In the Folder Options window, click **OK**.
- 7. Close Windows Explorer.
- 8. Retry to the affected launched task.

#### **For Mozilla Firefox**

Complete the procedure detailed in “Updating the Firefox Web browser to use the IBM Java Web Start program” in the *IBM Systems Director Systems Management Guide*.

Try the task again. The Opening launch.jnlp message might be displayed. The message asks you what you want to do with the .jnlp file. To make sure that the launched task can proceed and that this message will not be displayed in the future, it is recommended that you select **Open with Java Web Start Executable** and **Do this automatically for files like this from now on**.

## **Collect network topology missing connections**

This topic affects the IBM Systems Director Network Control Collect Network Topology function.

### **Problem**

Known relationships between network devices are not displayed when viewing the system-level or port-level network topology perspectives for these devices.

### **Explanation**

IBM Systems Director Network Control uses IBM Tivoli Network Manager (ITNM) to discover and construct the topology data for all network devices within the same subnet as the target network devices supplied to a IBM Systems Director Network Control network topology collection job. ITNM may not discover all the network devices on a class A or class B subnet after a single discovery is performed for a given subnet. If ITNM does not discover a device managed by IBM Systems Director, then the IBM Systems Director Network Control system-level and port-level network topology perspectives cannot display relationships for the corresponding device.

### **Resolution**

To collect inventory for NICs that are assigned to a BladeCenter chassis, complete the following steps:

1. Verify that a network topology collection was previously run without error and the devices in question were supplied as targets.
2. Verify that the devices in question are SNMP enabled. If a device is not SNMP enabled, then ITNM cannot collect topology data for it.

**Note:** The same SNMP security credentials are required for all managed endpoints in the same subnet as the IPv4 resources submitted to the topology collection job.

3. Make sure the server with IBM Systems Director Network Control installed meets the 4GB of memory and other system requirements. See IBM Systems Director Network Control requirements and Hardware requirements for running IBM Systems Director Server.
4. Repeat the network topology collection task. Additional devices may be discovered by ITNM after every network topology collection.
5. Increase the IBM Tivoli Network Manager (ITNM) InterPingTime from 100 ms to 400 ms. Increasing the InterPingTime from 100 ms to 400 ms increases the duration of the network topology collection job by 400%. Follow these instructions to update the InterPingTime:
  - a. Change m\_InterPingTime from default 100 - 400 and save the file:
    - On Linux and AIX, edit '/opt/IBM/tivoli/netcool/etc/precision/DiscoPingFinderSchema.ISDNM.cfg'
    - On Windows, edit 'C:\IBM\tivoli\netcool\etc\precision\DiscoPingFinderSchema.ISDNM.cfg'

The entry is located at the end of the file:

```
insert into pingFinder.configuration
  ( m_NumThreads, m_TimeOut, m_InterPingTime, m_NumRetries, m_Broadcast, m_Multicast, m_Udp)
values
  ( 10, 250, 100, 1, 0, 0, 14003 );
```

- b. Restart ITNM by performing a system reboot, or by following these steps:
  - On Linux and AIX, run the following commands:
    - 1) /opt/IBM/tivoli/netcool/precision/bin/itnm\_stop
    - 2) sh . /opt/IBM/tivoli/netcool/env.sh
    - 3) /opt/IBM/tivoli/netcool/precision/bin/itnm\_start ncp
  - On Windows, stop then start the 'ncp\_ctrl' service
- c. Wait a few minutes for ITNM to start before submitting another SDNC network topology collection job.

## Troubleshooting DCFM problems

This section provides information about problems when working with launch-in-context and template-based configuration functions of IBM System Storage Data Center Fabric Manager (DCFM).

IBM Systems Director Network Control V1.2 supports two methods of working with DCFM. After configuring DCFM and IBM Systems Director Network Control to work together, some actions provide launch-in-context links to the DCFM configuration interface. Other functions are integrated directly into the IBM Systems Director Network Control user interface for management of hardware with configuration templates.

### Ensuring IP address settings match

Mismatching IP addresses, ports, and host names can prevent IBM System Storage Data Center Fabric Manager (DCFM) and IBM Systems Director Network Control from working together.

Launch-in-context operations are affected by the DCFM server IP configuration. By default, the DCFM server listens for client connections on all possible known IP addresses for the server, including localhost and addresses corresponding to secondary Ethernet adapters. However, changing the IP configuration through the DCFM configuration wizard or by changing the IP configuration options of the DCFM client can cause problems when using launch-in-context. In some cases,

connection problems are not obvious when the DCFM configuration screen probes the DCFM server. These problems can range from Java Webstart errors indicating it cannot find the DCFM server, to indications that the host name is unknown. Unknown host names can also occur because of inconsistencies in Domain Name System (DNS) resolution between the DCFM server, the IBM Systems Director Server and the server running the IBM Systems Director Web interface.

DCFM template-based configuration tasks are affected by the DCFM SMI Agent (CIMOM) IP configuration. By default, the SMI Agent (CIMOM) process listens for CIM client connections on all possible known IP addresses for the server, including localhost and addresses corresponding to secondary Ethernet adapters. Changing the IP configuration through the DCFM configuration wizard or CIMOM IP configuration in the Systems Management Console can cause connection problems when the DCFM Configuration screen probes the DCFM CIMOM.

The IP addresses that the DCFM Server and CIMOM listen for connections on can be modified through several mechanisms. It is important that IP addresses and ports be configured properly, or the DCFM process may not accept connections from Director. IP addresses can be modified in the following ways:

- DCFM Configuration Wizard: From the **Server IP Configuration** panel. This modifies only the DCFM server IP address and the DCFM CIMOM IP address. This wizard is used at installation time to configure several things for the DCFM server, the DCFM CIMOM, and the DCFM database. The default option is to use the server's non-qualified base host name.
- DCFM Client user interface: Select **Server** → **Options** → **Software Configuration** → **IP Configuration**. This modifies only the DCFM server IP address. The default is the **All** option.
- SMIA Configuration Tool: From the DCFM Server Management Console, click the **Configure SMI Agent** button on the **Services** tab and log on to the SMIA Configuration Tool. In the SMIA Configuration tool, select the **CIMOM** tab. In the **IP Configuration** area, locate the **Bind Network Address** field. The default option is to use the non-qualified base host name of the server. This setting modifies only the DCFM CIMOM IP address.

### Director cannot connect to DCFM Server

This problem can occur when the IBM System Storage Data Center Fabric Manager (DCFM) Configuration page is submitted.

#### Problem

Error message indicating that Director cannot connect to DCFM Server (DNZNMC242E).

#### Explanation

Director cannot access DCFM service.

#### Investigation and Resolution

Error message indicating that Director cannot connect to DCFM Server (DNZNMC242E). Use the following table to troubleshoot the problem:

Possible Cause	Recovery Actions
Firewall blocking access between Director and DCFM Server.	Check that no firewall is blocking access.

Possible Cause	Recovery Actions
DCFM Server is not running.	Use ping or a similar tool to check that DCFM Server is running, and restart the server if necessary.
DCFM service is not running on DCFM Server.	Restart the DCFM service.
DCFM Configuration page information is wrong.	Check that the DCFM Host/IP Address is correct and DCFM Port matches the configured HTTP port for DCFM.
DCFM Service may not be listening on appropriate IP addresses.	Check the DCFM IP Configuration using the following steps: <ol style="list-style-type: none"> <li>1. Launch the DCFM Client interface.</li> <li>2. Expand <b>Server</b> → <b>Options</b> → <b>Software Configuration</b> → <b>IP Configuration</b> and check the Server IP Configuration setting.</li> <li>3. Several of the available IP addresses work, but the <b>All</b> setting causes the DCFM Server to listen on all possible IP addresses. Set the appropriate IP address, then restart DCFM Service.</li> </ol>

## Director cannot connect to the SMI Agent

This problem can occur when the IBM System Storage Data Center Fabric Manager (DCFM) Configuration page is submitted.

### Problem

Error message indicating that Director cannot connect to SMI Agent (DNZNM251E).

### Investigation and Resolution

Use the following table to troubleshoot the problem:

Possible Cause	Recovery Actions
Firewall blocking access between Director and DCFM Server.	Check that no firewall is blocking access.
DCFM Server is not up.	Use ping or a similar tool to check that DCFM Server is up, and restart the server if necessary.
DCFM SMI Agent (CIMOM) service is not installed on the DCFM Server.	If DCFM CIMOM service was not installed, install it. <b>Note:</b> DCFM CIMOM service is available for DCFM V10.4 and later.
DCFM SMI Agent (CIMOM) service is not running on the DCFM Server.	Restart the DCFM CIMOM service.
DCFM Configuration page information is wrong.	Check that the following values are correct: <ul style="list-style-type: none"> <li>• DCFM Host/IP Address</li> <li>• SMI-A port matches the configured SMI-A port for DCFM</li> <li>• DCFM user ID and DCFM password</li> </ul>

Possible Cause	Recovery Actions
DCFM SMI Agent (CIMOM) service is not be listening on appropriate IP addresses.	<p>Check the DCFM SMI Agent (CIMOM) IP Configuration using the following steps:</p> <ol style="list-style-type: none"> <li>1. Launch the DCFM System Management Console.</li> <li>2. Select <b>Configure SMI Agent</b> and log on to the SMI Configuration Tool.</li> <li>3. In the SMI Configuration Tool, click the <b>CIMOM</b> tab.</li> <li>4. In the <b>IP Configuration</b> section, set the <b>Bind Network Address</b> to the correct IP address.</li> <li>5. Restart DCFM SMI Agent (CIMOM) service.</li> </ol>

## Unknown host when launching DCFM

This problem can occur on certain systems while running the IBM System Storage Data Center Fabric Manager (DCFM) server. It occurs because the host name is used as the default JNDI and the RMI return address.

### Problem

This problem manifests in one of two ways:

1. When launching into the DCFM client from IBM Systems Director with single sign-on disabled, the DCFM login screen appears. However, the DCFM login screen displays the error message Unknown host <system> and the **Login** button is disabled.
2. If single sign-on is configured, when the user launches into the DCFM client from IBM Systems Director, a DCFM window displays the following message:  

```
javax.naming.CommunicationException [Root exception is java.rmi.UnknownHostException: Unknown
```

### Resolution

To resolve this issue, update your hosts file. The host file is commonly found in one of the following locations:

Operating System	Location
Windows	C:\Windows\system32\drivers\etc\hosts
Linux	/etc/hosts
AIX	/etc/hosts

The exact hosts file location might be dependent on your distribution or version of your operating system.

Open the hosts file on the IBM Systems Director Server and add the host information for the system that the DCFM client states that it cannot locate.

Add two lines to the end of the file to ensure that the client can resolve the host address:

```
<IP Address of the DCFM Server> <Fully qualified domain name of the DCFM Server>
<IP Address of the DCFM Server> <Hostname of DCFM Server>
```

No reboot of the IBM Systems Director Server is required when this change is made. All client systems that want to use the DCFM client must also update their local hosts file to communicate directly with the server. For more information about this issue, consult the IBM System Storage Data Center Fabric Manager (DCFM) documentation.

## Launch-in-context operations fail

These problems can occur when a launch-in-context operation is launched, with or without single sign-on.

### Problem

Launch-in-context operations fail with error messages described below.

### Explanation

Use the information in the following table to determine the cause of the error and solve the problem:

Error message	Resolution
Error message indicating Director cannot connect to DCFM Server (DNZNYMC242E)	<p>Director cannot access the DCFM Server. Possible resolutions:</p> <ul style="list-style-type: none"> <li>• Check that no firewall is blocking access between Director and DCFM Server.</li> <li>• Use ping or a similar tool to check that the DCFM Server is up, and restart the server if necessary.</li> <li>• If the DCFM service is not running on the DCFM Server, restart the DCFM service.</li> <li>• Check that the DCFM Host and IP address are correct and DCFM Port specified on the <b>Set up launch to DCFM page</b> matches the configured HTTP port for DCFM.</li> </ul>
After Java Webstart download of DCFM client, get DCFM error message indicating "Select a Fabric, Switch or Ports to view Historical Graph" instead of getting appropriate DCFM screen.	No switch WWN was available to identify the target switch. In Director, collect inventory on the target switch. The WWN is part of collected inventory.
After Java Webstart download of DCFM client, get DCFM login screen with an error "Unknown Host XXXXX" and Login button is disabled.	<p>DNS system of the Web browser host cannot resolve the server name. To correct this, post the DCFM server host name posted in the local DNS server. Alternative: Add that DCFM server IP address and host name to the hosts file on the web browser host:</p> <pre>AAA.BBB.CCC.DDD    fully-qualified host name AAA.BBB.CCC.DDD    base host name</pre> <p><b>Note:</b> On Linux/AIX, the hosts file is /etc/hosts. On Windows, it is C:\WINDOWS\system32\drivers\etc\hosts.</p>
After Java Webstart download of DCFM client, get DCFM login screen with an error "Failure to connect to server XXXXX", an IPv6 address shown for Server Address, and Login button is disabled.	DCFM cannot use connections from remote DCFM Client process using a raw IPv6 address. On the DCFM Configuration page, specify a fully-qualified host name.

Error message	Resolution
Java Webstart error shows "Unable to launch application" and "Requesting JRE 1.6+" indications (with Name="DCFM 10.4.X (server hostname)" and Publisher="Data Center Fabric Manager" and From=<DCFM Server URL>	Java 1.6 is unavailable on the Director console server. The possible resolutions: <ul style="list-style-type: none"> <li>• If Java 1.6 is not installed, uninstall the old version of Java and install and enable Sun Java 1.6 or later.</li> <li>• To enable Java 1.6 on Windows, go to <b>Control Panel</b> → <b>Java</b>. Click the <b>Java</b> tab and then <b>View...</b> to display the Java Runtime Environment Settings. Click to enable Java 1.6 item, then click <b>OK</b>. Restart your browser and try again.</li> </ul>
Browser message indicates a download of dcfm.jnlp was requested (from DCFM host), but there is no file association for.jnlp files. You can download and save the file, but cannot open it.	No version of Java is installed on this Director console server. Install newest version of Sun Java 1.6.
After Java Webstart download of DCFM client, DCFM error message states "Client is not compatible with the Server" and a DCFM Login screen with an error indicating "Client/Server version mismatch".	The Java Webstart cache contained a previously downloaded version of the DCFM client that was not compatible with a newly installed DCFM server. Flush the Java Webstart cache. On Windows, go to <b>Control Panel</b> → <b>Java</b> . On the <b>General</b> tab, click <b>Temporary Internet Files</b> → <b>Settings</b> → <b>Delete Files</b> . Alternative: Restart the Director console server to flush the Java Webstart cache.
After Java Webstart download of DCFM client, DCFM error message states "XX:XX:XX:XX:XX:XX:XX:XX is not managed by DCFM, add switch via <b>Discover</b> → <b>Setup</b> ."	The switch has not been discovered in DCFM. The XX:XX:XX:XX:XX:XX:XX:XX is the World Wide Name (WWN) of the switch. Discover the switch in DCFM using <b>Discover</b> → <b>Setup</b> .

### Related reference

"Single sign-on fails during launch-in-context"

### Single sign-on fails during launch-in-context

These problems can occur when a launch-in-context action is launched with single sign-on (SSO) enabled.

### Problem

After Java Webstart of IBM System Storage Data Center Fabric Manager (DCFM) client, the following DCFM message is displayed: "Unable to retrieve the LTPA token. Make sure that you have specified the DCFM server using fully qualified name". After dismissing the DCFM message, the DCFM login screen opens, indicating that automatic SSO authentication failed.

### Explanation

The LtpaToken cookie was not found in the browser. The LtpaToken cookie contains authentication information used to implement single sign-on between IBM Systems Director and DCFM.

When SSO authentication fails, you can enter the DCFM user ID and password directly to proceed with launch-in-context.

## Resolution

Use the following table to troubleshoot single sign-on failure:

Possible Cause	Recovery Actions
Cookies were disabled in the browser.	Enable cookies in the browser.
IBM Systems Director was not restarted after enabling SSO.	Restart IBM Systems Director. This restarts the security-related plug-ins to allow SSO authentication.
You changed any of DCFM Host or IP address, DCFM port, SSO user ID, SSO password.	On the DCFM Server, run the tpcssosetup tool with the new IP address, port, SSO user ID, and SSO password.
The user ID and password do not match the ID and password configured on DCFM.	Create the same user ID and password in DCFM that are being used for SSO and run the tpcssosetup tool.
The DCFM server, IBM Systems Director server, and IBM Systems Director console server are not in the DNS domain specified in the DCFM Configuration page.	Open the DCFM Configuration page and enter an SSO domain that encompasses the Director server, the DCFM server, and the server on which the browser-based Director console is being run.
You are not logged on to the IBM Systems Director console with a fully-qualified host name.	Log out of IBM Systems Director and log back in using a fully-qualified host name in the URL.
The Brocade-branded version of DCFM was being used instead of the IBM-branded version.	The Brocade-branded version does not support SSO with IBM Systems Director. Uninstall the Brocade-branded version of DCFM, then download and install the IBM-branded version of DCFM.

### Related reference

“Launch-in-context operations fail” on page 48

## Switch login fails during template-based configuration

These problems can occur when using template-based configuration for IBM System Storage Data Center Fabric Manager (DCFM).

### Problem

Error message indicating switch login failed (DNZCP1626E)

### Explanation

Could not communicate with the DCFM SMI Agent (CIMOM) process.

### Resolution

Use the following table to troubleshoot the problem:

Possible Cause	Recovery Actions
A firewall is blocking access between IBM Systems Director and DCFM Server	Check that no firewall is blocking access.
DCFM Server is not running.	Use ping or a similar tool to check that DCFM Server is up, and restart the server if necessary

Possible Cause	Recovery Actions
DCFM SMI Agent (CIMOM) service was not installed on DCFM Server.	If DCFM CIMOM service was not installed, install it. <b>Note:</b> DCFM CIMOM service is available for DCFM V10.4 and later.
DCFM CIMOM Service is not running on DCFM Server.	Restart the DCFM service.
DCFM Configuration page information is wrong.	Check that the following values are correct and match DCFM settings <ul style="list-style-type: none"> <li>• DCFM Host or IP address</li> <li>• SMI-A port</li> <li>• DCFM user ID and DCFM Password</li> </ul>
A firewall is blocking access between DCFM Server and switch.	Check that no firewall is blocking access.
The switch was not discovered in DCFM.	Discover the switch in DCFM.
DCFM Configuration page information is correct, but CIMOM access information in RSAP for the switch is wrong.	Due to current limitations, Remote Service Access Point (RSAP) information for each DCFM-managed switch is not updated when the DCFM host or IP address, DCFM user ID, DCFM Password, or SMI Agent port values are changed on the DCFM Configuration page. The only workaround is to delete the switch in Director, rediscover it and request access. The rediscovery of the switch recreates the RSAP with the correct information. Inventory collection is not needed for template-based DCFM integration operations, although it may be useful for DCFM launch-in-context operations.

---

## Publications and related information

You can view the same IBM Systems Director Network Control content that resides in the Information Center in a PDF document.

To view a PDF file, you need Adobe® Acrobat Reader, which can be downloaded for free from the Adobe Web site at [www.adobe.com/products/acrobat/readstep.html](http://www.adobe.com/products/acrobat/readstep.html).

### IBM Systems Director Network Control resources on the World Wide Web

- **IBM Systems Director Network Control V1.2 information center**  
[http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.sdnm.adv.helps.doc/fnc0\\_p\\_network\\_ctrl.html](http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.sdnm.adv.helps.doc/fnc0_p_network_ctrl.html)  
Find information for installing and using IBM Systems Director Network Control.
- **IBM Systems Director Network Control V1.2 Web site**  
[www.ibm.com/systems/management/director/plugins/networkcontrol/](http://www.ibm.com/systems/management/director/plugins/networkcontrol/)  
See an overview of IBM Systems Director Network Control and links to download the product.
- **IBM Systems Director Web site**

[www.ibm.com/systems/management/director/](http://www.ibm.com/systems/management/director/)

Get overview information, demonstrations, and downloads for the IBM Systems Director product, and its plug-ins.

- **IBM Systems and servers: Technical support page**

[www.ibm.com/systems/support/](http://www.ibm.com/systems/support/)

Locate support for IBM hardware and Systems Management software.

---

## Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation  
Licensing 2-31 Roppongi 3-chome, Minato-ku  
Tokyo 106-0032, Japan

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web

sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation  
MW9A/050  
5600 Cottle Road  
San Jose, CA 95193  
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

## Trademarks

IBM, the IBM logo, and [ibm.com](http://ibm.com)<sup>®</sup> are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries,

or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (<sup>®</sup> or <sup>™</sup>), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe is either a registered trademark or trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX<sup>®</sup> is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.



---

# Index

## B

BladeCenter  
network devices 6, 9  
products, supported tasks 6, 9

## C

Configuration templates  
creating 27

## D

DCFM 29, 30, 35, 36  
configuration 44

## H

Health  
network 28, 39, 41, 44

## I

IBM Systems Director tasks 6, 9  
installation 16

## L

legal notices 52

licensing  
requirements 5

## M

Managing  
network devices 1  
network systems 1

## N

Network Control 1, 43  
network control, about 29, 30, 35, 36  
network device  
failure to discover 41, 47  
launch-in-context 48  
network devices 1, 6, 9, 29, 30, 35, 36  
supported 6, 9  
network management 41, 47, 48  
Network Management 6, 9  
network management, about 1  
new features  
V1.2 2

## P

planning 6  
plug-ins  
network control 29, 30, 35, 36  
network management 1

## R

requirements  
licensing 5

## S

Specified operating environment 6  
support 6, 9

## T

topology  
network 43  
trademarks 53  
troubleshooting  
DCFM 45, 46, 49, 50  
network 45, 46, 49, 50

## W

what's new  
Network Control 2  
V1.2 2