

=====

3Com(R) Network Director Version 2.5 (Service Pack 3)
(Product #: 3C15500)

=====

This document provides the following information:

1. Legal
2. About This Software
3. System Requirements
4. Enhancements in this release
5. Enhancements included in this release from earlier service packs
6. Problems fixed in this release
7. Fixes included in this release from earlier service packs
8. Running 3Com Network Director on Windows XP Service Pack 2
9. Running 3Com Network Director as a Windows service
10. Active Directory and Internet Authentication Service (IAS) access
11. Security configuration limitations
12. Known Problems in 3Com Network Director Version 2.5
13. Integration with 3Com Wireless Switch Manager
14. The software upgrade process
15. World Wide Web Site

=====

1. Legal

=====

IMPORTANT: READ BEFORE USING THIS SOFTWARE

You should carefully read the terms and conditions of the Software License Agreement that is displayed when you install this software. Your legal rights are defined therein.

USE OF THIS SOFTWARE INDICATES THAT YOU ACCEPT SUCH TERMS AND CONDITIONS.
If you do not agree with such terms and conditions, do not use this software.

=====

2. About This Software

=====

3Com Network Director is a standalone application that allows you to carry out key management and administrative tasks on mid-sized enterprise networks.

By using 3Com Network Director you can:

- discover, map and monitor all the devices on the network
- backup and restore 3Com device configurations
- configure 3Com devices across the network in a single operation (including - VLANs and Traffic Prioritization)
- gather historical performance information for your network and generate flexible reports

3Com Network Director also provides:

- fault finding and event generating capabilities
- element management for 3Com switches and routers

=====

3. System Requirements

=====

The following Windows operating systems support the application:

- Windows 2000 Professional Service Pack 4
- Windows XP Professional Service Pack 2
- Windows Server 2003
- Windows Vista may be used, but this is not a supported operating system. In particular, running 3ND as a service will not work under Windows Vista. The following information is provided as guidance when using Vista:
 - As the application uses privileged operations, it should be installed and run by a user with administrator privileges.
 - The initial 3ND v2.5 installation should be run in "Windows XP+SP2" compatibility mode (set via properties on the install .exe file).
 - After installation, 3ND should not be run in "compatibility mode". (Do not launch 3ND at the end of the installation process).
 - Always run 3ND by using the "Run as Administrator" option from the right-click menu.

Adobe Acrobat Reader is required to view the PDF files installed with 3Com Network Director.

A web browser is required to access the Help system and the HTML-based reports. The following web browsers have been successfully tested against 3Com Network Director:

- Netscape 7.72
- Netscape 8.1
- Internet Explorer 6
- Internet Explorer 7
- Mozilla Firefox 1.5
- Mozilla Firefox 2.0
- Opera 7.22
- Opera 9
- Mozilla 1.5

Netscape 6 is not recommended because of interoperability issues. There may also be restrictions on the web browsers supported by WebHelp.

3Com Network Director has the following platform requirements:

	Minimum	Recommended
IBM PC or compatible	500MHz Pentium III	1GHz Pentium 4 or better
RAM	512MB	1GB or more
Free hard disk space	500MB	1GB or more
Graphics capabilities	1024x768 / 256 colors	1024x768 / 64K colors
CD-ROM drive	Yes	Yes
Network adapter card	Yes	Yes

Multiple network interfaces are not supported.

Allow an additional 2MB of disk space per network device for historical data logging.

=====

4. Enhancements in this release

1. Support is included, or enhanced, for the following devices or agent versions:
- 3Com Switch 8800 (family) V5 agent code.
 - 3Com Switch 4200G
 - 3Com Switch 4210
 - 3Com Switch 4500G 10Gig module
 - 3Com Baseline Switch 2948-SFP Plus
 - 3Com OfficeConnect Managed Gigabit PoE Switch
 - 3Com 24 port Unified Switch
 - 3Com Wireless LAN Controllers WX4400, WX2200, WX1200, WXR100
 - 3Com Wireless Access Point 3150
 - 3Com Wireless Access Point 3850
 - 3Com OfficeConnect 54/108Mb Wireless Firewall Router (recognition only)
 - 3Com AirProtect Wireless Intrusion Protection System Engine 6100 (trap decode only)
2. A warning is now issued if 3ND cannot connect to the SNMP Trap port when it starts up. The Trap port is UDP port 162. This warning includes advice on what actions may be taken to rectify the problem.
3. Integration with version 4 of Device Manager.

5. Enhancements included in this release from earlier service packs

1. Support is included, or enhanced, for the following devices or agent versions:
- 3Com Office Connect ADSL Wireless 11g Firewall router (3CRWDR101A-75)
 - 3Com Baseline Switch 2250 Plus (3C16476CS)
 - 3Com Baseline Switch 2226 Plus (3C16475CS)
 - 3Com Baseline Switch 2426 PWR Plus (3C16491)
 - 3Com Switch 4200G family
 - 3Com Wireless Access Point 7760
 - 3Com Wireless Access Point 8760
 - 3Com Building to Building Bridge and AP (3CRWEASYA73)
 - 3Com 24 port Unified Switch
 - 3Com Wireless Switch family (V6 agent)
 - 3Com Switch 4500G family (V3.02.00)
 - 3Com Switch 8800 family (V3.01.30)
 - 3Com VCX Telephony systems (Basic Discovery and Trap Decodes)
 - 3Com NBX Telephony Systems (Trap decodes)
 - 3Com Switch 2916-SFP Plus/2924-SFP Plus/2924PWR-SFP Plus
 - 3Com 108 Mb Firewall Router (3CRWDR200A-75, 3CRWDR200B-75) - Discovery only
 - 3Com X506, X5 25-User and X5 Unlimited-User Secure Gateways (Discovery only)
 - Tipping Point X506 Secure Gateway (Discovery only)
2. The QoS ACL Editor
- This is used to create and edit ACL QoS Profiles which can then be used by other Network Management tools such as 3Com Network Director to configure devices. Currently this is only applicable to the Switch 5500 family.

6. Problems fixed in this release

1. Creating a VLAN, including an IP interface could cause a 3ND failure.
2. Editing a custom report could cause it to become corrupt.

3. Occasionally items on a network map would not indicate their correct health status. For example a device could stay red after all its outstanding events had been resolved.

=====

7. Fixes included in this release from earlier service packs

=====

1. Under some circumstances, for certain devices, it was possible for 3ND to reset its defined write community string to its default value (private).
2. Some additional traps are now decoded for the 3ND event log.
3. Some newer Switch 4200 devices are not fitted with fans. These devices are no longer monitored for hardware fan failure.
4. Occasionally, when RADIUS authentication was enabled on a port, the port could be left with security disabled.
5. For some products, manually configured link aggregations were reported as automatic (LACP configured).
6. "Inconsistent VLANs" could be incorrectly reported by 3ND in its "Misconfigurations AND Optimizations" report.
7. The network discovery process has been improved to reduce the number of clouds that can be included in the network map and make the mapping more accurate.
8. The agent upgrade process for the Switch 5500 family has been changed to delete old application files from the device if this would make space for the new agent to be installed.
9. In some situations, not all NBX phones were discovered.
10. Additional device configuration is now available for the Switch 7700 and Switch 7750.
11. The decoding of varbinds in SNMP v2 Traps is now correct.
12. Configuration Backup and Restore for the Switch 8800 family will now work correctly when a redundant fabric is installed.
13. The Live graphs and Historical reports for links now include the port information.
14. When backing up a Switch 8800 configuration, 3ND "saved" the current configuration before backing up the startup configuration file. This can inadvertently backup temporary configuration changes which may not be desirable. 3ND no longer issues the "save" command.
15. Occasionally, device "groups" unexpectedly became un-grouped.

=====

8. Running 3Com Network Director on Windows XP Service Pack 2

=====

1. When 3Com Network Director first runs, you may see a warning titled "Windows Security Alert", with the text:

To help protect your computer, Windows has blocked some features of this program.

Do you want to keep blocking this program?

Name: javaw
Publisher: Unknown

This warning is generated by the Windows Firewall, which is enabled by default in Windows XP Service Pack 2.

You should select the "Unblock" option on this dialog, otherwise 3Com Network Director will not operate correctly.

2. When you first launch 3Com Network Director's HTML-based online help system, you may see a warning within Internet Explorer:

To help protect your security, Internet Explorer has

restricted this file from showing active content that could access your computer.

To allow 3Com Network Director's online help system to operate correctly, you should enable active content execution by doing the following:

- launch Control Panel
- select "Internet Options"
- select the "Advanced" tab
- check the option for "Allow active content to run in files on My Computer"

3. By default, Windows XP Service Pack 2 will not respond to discovery requests from 3Com Network Director. This will prevent any PC running Windows XP Service Pack 2 from being discovered and mapped by 3Com Network Director. If you want to include PCs running Windows XP Service Pack 2 in your 3Com Network Director map, follow the instructions below for each PC:

To allow the PC to respond to ICMP echo requests (used for basic discovery):

- launch Control Panel
- select "Windows Firewall"
- select the "Advanced" tab
- click the "Settings..." button in the "ICMP" frame
- check the option for "Allow incoming ICMP echo requests"
- click OK

To allow the PC to respond to NetBIOS requests (used for identification of type and capabilities):

- launch Control Panel
- select "Windows Firewall"
- select the "Exceptions" tab
- check the option for "File and Print Sharing"
- if you want to allow requests from subnets other than the local subnet:
 - click the "Edit..." button
 - change the access scope as required
- click OK

For more information on running 3Com Network Director on Windows XP Service Pack 2, please visit <http://www.3com.com/netman/winxpsp2>

=====

9. Running 3Com Network Director as a Windows service

=====

IMPORTANT NOTE:

3Com Network Director may not be run as a service under Windows Vista.

1. General

3Com Network Director is installed as a service with a startup type of 'disabled'. This mode is recommended for most customers. In this mode 3Com Network Director is a normal application that executes with the privileges assigned to the user logged on. The application will close when the user logs-off.

2. Automatic service

When run as an automatic service 3Com Network Director executes as 'local system user'. This user is a built in Windows user with pre-defined privileges that can not be changed. This causes issues when using Network drives and multiple users that save files to the desktop. It is advised that download files are copied to the local machine before being imported to 3Com Network Director and default locations are used when saving files. 'Local system user' has extensive privileges on the local machine, it is recommended not to use other business critical applications on the same machine e.g. domain controller.

To change 3Com Network Director to an automatic service:

- launch Control Panel
- launch Administrative Tools
- launch Services
- Double click 3Com Network Director
- Use the 'Startup type:' dropdown list to select the 'Automatic' mode.
- select the 'Apply' button
- select the 'Start' button

3Com Network Director will now automatically start should the system reboot or when windows detects the 3Com Network Director process is not executing.

When a user logs-off 3Com Network Director will restart using the Map loaded when the user logged-off. Support applications RMON Tool, Switch Manager, Router Manager, RMON Tool, Network Jack Configuration Tool, User Guide (Adobe Reader), Reports (Internet Explorer) and Network Access Manger may close depending on the windows OS being used. When a user logs-on the 3Com Network Director main window will be visible.

3. 3Com Network Access Manager shortcut

'Local system user' has restricted networking privileges which means when 3Com Network Access Manager is launched from 3Com Network Director it can only read Active Directory data, it can not write data. Using Start menu to launch 3Com Access Manager does not have this issue.

=====

10. Active Directory and Internet Authentication Service (IAS) access

=====

Additional privileges are required when 3Com Network Director service has a startup type of disabled (default install) to access or update the RADIUS Client information stored in IAS. The user details specified for Active Directory (see Tools->Options->Active Directory tab) should have the following privileges on the local machine:

- + "Act as part of the operating system"

- (Windows 2000 only)
- + "Adjust memory quotas for a process"
(Windows 2003 Server and Windows XP)
- + "Impersonate a client after authentication"
(All OS)
- + "Increase Quotes"
(Windows 2000 only)
- + "Replace a process level token"
(All OS)

To view or modify the privileges assigned to a user account on a computer:

- launch Control Panel
- launch Administrative Tools
- launch Local Security Policy
- select Local Policies
- select User Rights Assignment
- to add a user/group double click the appropriate policy setting
(see required privileges) and then add the user account or group using
the 'Add User or Group...' button

The changes become effective when the user next logs-on.

It is important that the Account credentials configured to access Active Directory are appropriate, see Tools->Options Active Directory tab. The account should have read/write access rights to Users and Computers and RADIUS Client information stored in IAS. This will normally be a member of the "Administrators" group or the "Server Operators" group and must have logon rights on the computer running 3Com Network Director.

=====
11. Security configuration limitations
=====

1. The 5500, 5500G, 7750 use domain information contained in the dotlx requests to decide where to send the requests. Thus your network domains have to be configured in each switch for dotlx authentication to operate correctly. The default dotlx authentication mode on these switches is CHAP. If you have deployed a different authentication mode on your network, you must also configure it on every switch, using the CLI dotlx authentication-mode command. Additionally, if you are deploying eap-ttl, the device configuration must be modified by configuring a radius server domain and enabling this domain. Please check the device configuration guide.
2. The 5500, 5500G require the configuration of a Radius Authentication Server, even if you have not set up a Radius Accounting server on your network. In the Radius Settings Configuration dialog, copy the Radius Authentication Server details to the Radius Accounting details and set the Accounting Server unavailable action to 'Ignore'. If this is not done, authentication will fail.
3. After configuring the Radius Authentication Server via 3ND, console port logins will not be granted administrator rights. Also, if The RADIUS service fails it will become impossible to access the 5500, 5500G and 7750 via the console port.
4. It is not possible to modify the Radius Server details via 3ND while users are logged on via Telnet on the 5500, 5500G and 7750.
5. The 5500, 5500G and 7750 switches do not support continuous or automatic

learning port security modes.

6. On the 5500, 5500G and 7750 Secure Network Login operates as macAddressOrUserLoginSecure.
7. In order for 3ND to receive user authentication and security violation traps from the 5500, 5500G, 7750, the following CLI commands need to be applied to each device after enabling port security from 3ND:

```
port-security trap addresslearned
port-security trap intrusion
port-security trap dot1xlogon
port-security trap dot1xlogoff
port-security trap dot1xlogfailure
port-security trap ralmlogon
port-security trap ralmlogoff
port-security trap ralmlogfailure
```

8. The 7750 3C16859 module does not support port security.

=====
12. Known Problems in 3Com Network Director Version 2.5
=====

Installation:

1. On Windows XP and Windows 2000, you must log in with Administrator rights to install and run 3Com Network Director.
2. The 3Com Device View feature will not work properly if 3Com Network Director is launched at the end of the installation process. Please launch 3Com Network Director from the Start menu.
3. Uninstalling and reinstalling 3Com Device Manager may fail with the following error message:
"Resolve config file failed, exist..."

To resolve this issue, manually delete the following file:
<windows install directory>\DeviceMgr.ini

For example:
c:\Windows\DeviceMgr.ini

General:

1. Files generated using 3Com Network Director's Export To Visio feature are not compatible with the Microsoft Visio Viewer. Please use Microsoft Visio 2003 to view these files.
2. Use of 3Com Network Director via Remote desktop.
 - a. There are no known issues using Remote desktop when 3Com Network Director is running on Windows XP.
 - b. There are known issues with Windows server 2003 due to its implementation of multiple user support.
3. When a user logs-off all scheduled tasks are deleted

Device support:

1. 3Com Switch 5500 (if running agent versions prior to v3.1.7):

When upgrading or restoring Switch 5500 devices using 3Com Network Director's Agent Update and Restore features, please ensure that the unit number of standalone units is set to 1.

If the target device is using automatic unit numbering, you can do this by simply rebooting the device. If the target device is using manual unit numbering, you can do this by setting the unit number to 1 using the device's CLI.

If the unit number of standalone units is not set to 1 then Agent Update and Restore operations may fail, and further 3Com Network Director operations may also fail until the network is rediscovered.

This issue does not apply to Switch 5500 devices that form a stack of or more units.

2. 3Com Switch 7700 and 8800 Families

3ND does not attempt to upgrade the BootRoms on these devices. Suitable versions of BootRom must be loaded on these devices before upgrading with new application files. Using the incorrect BootRom/Application code combination can result in equipment failure.

3. 3Com Wireless Access Point 8760 (3CRWE876075A) and 3Com outdoor building to building bridge/Access Point (3cWEASYA73)

Occasionally, a configuration restore appears to work correctly, but the restore has failed. This problem has been fixed in the latest agent code.

There are a number of restrictions to the device configurations that may be applied to these devices. Please check the 3ND error reports carefully. These restrictions should be lifted in future AP agent releases. Please use the latest agent available from the 3Com web site.

4. 3Com Unified Gigabit Wireless PoE Switch 24 (3CRUS2475)

VLAN 1 (the default VLAN) is automatically assigned to ports by the unified switch. Therefore, attempting to configure this VLAN to ports using 3ND will normally result in errors being reported.

5. 3Com VCX - hosted by an IBM i-series

VCX servers contained within virtual (hosted) partitions on an IBM i-Series computer will not be topologized correctly in the network map.

Please refer to the Supported Device List installed with 3Com Network Director for information on support for 3Com devices, including known restrictions.

Please also ensure that you refer to the readme files supplied with your 3Com networking products, to check for possible compatibility issues with 3Com Network Director.

=====
3Com Network Director is fully compatible with 3Com Wireless Switch Manager. These applications can be installed and executed on the same PC, simultaneously.

By default only one of these applications can register for and receive traps on the standard UDP port that is reserved for trap reception. To prevent conflicts between these applications it is possible to configure 3Com Network Director to forward traps to another port and for 3Com Wireless Switch Manager to receive traps on another port.

Please follow these instructions to configure 3Com Network Director to forward traps to another UDP port on the same PC:

1. Open Windows Explorer, and navigate to the following directory where 3Com Network Director is installed:

`<install_dir>\data\com\coms\wsd\tns\server\network`

2. Using a text editor, such as Microsoft Notepad, open the following file:

`TrapForwarding.properties`

3. Enable trap forwarding by setting the status of the `trap_forwarding_enabled` parameter to "true":

`trap_forwarding_enabled = true`

Please use lower case letters, as 3Com Network Director is case-sensitive.

4. By default, traps will be forwarded to UDP port 1181. This port has been reserved specifically for this purpose by the Internet Assigned Numbers Authority (IANA). However, if you are running another application which is already using this port, then you can configure 3Com Network Director to forward to a different port by setting the `trap_forwarding_port` parameter to the desired UDP port. e.g.

`trap_forwarding_port = <port number>`

where `<port number>` is the number of an appropriate, unused UDP port.

5. Save the file, and restart 3Com Network Director. All traps received by 3Com Network Director will now be forwarded to the specified port.

Please refer to the documentation that comes with 3Com Wireless Switch Manager for instructions on how to configure it to receive traps on a specified UDP port.

=====
14. The Software Upgrade Process
=====

This 3ND Service Pack installs automatically over the initial release of Version 2.5 of 3Com Network Director and previous Service Packs.

The file "3com_network_director_v2_5_sp3.exe" should be run and the usual installer instructions followed.

This SP is available free of charge for all unregistered users running in the 60 day evaluation period by using the "LiveUpdate" function button on the main 3ND display.

Registered users of 3ND require a suitable 3Com Service Contract to obtain this Service Pack.

=====
15. World Wide Web Site
=====

Access the latest networking information on 3Com Corporation's World Wide Web site by entering our URL into your Internet browser:

<http://www.3com.com>

(R) means registered trademark.

(TM) means trademark.

3Com and SuperStack are registered trademarks of 3Com Corporation. Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

Other marks, brand and product names may be registered trademarks or trademarks of their respective holders.

Document Number: DRA15500-DAAA01

Revision: 15

Issued: August 2007

Copyright 2007 3Com Corporation.