



Doc. No. 78-2707-02

## CiscoView 3.0(3) on AIX Release Note

---

This document discusses the CiscoView 3.0(3) on AIX release. It contains the following sections:

- CiscoView 3.0(3) CD Installation Instructions, page 1
- CiscoView 3.0(3) on AIX Features, page 2
- Documentation Information, page 2
- Troubleshooting, page 2
- CiscoView 3.0(3) on AIX Caveats, page 3
- Cisco Information Online, page 11

---

**Note** CiscoView 3.0(3) runs on AIX 4.1 *in addition* to AIX 3.2.5, and optionally with either NetView for AIX 4.1 *or* 3.1. These additional compatibilities are not mentioned in the CD-ROM installation instructions shipped with CiscoView 3.0(3).

---

### CiscoView 3.0(3) CD Installation Instructions

The CD-ROM installation instructions shipped with CiscoView 3.0(3) are identical to those shipped with the previous release, CiscoView 3.0(2). The older instructions are valid for CiscoView 3.0(3) with the following clarifications.

- References to the *CiscoView 3.0(2) Release Note* on pages 2 and 5 should be *CiscoView 3.0(3) on AIX Release Note*.
- The Software Requirements Checklist on page 5 should note that:
  - CiscoView 3.0(3) runs on AIX 4.1 *in addition* to AIX 3.2.5, and optionally with either NetView for AIX 4.1 *or* 3.1.
  - CiscoView 3.0(3) requires 40 MB or more in the */usr* directory, not 25 MB.

## CiscoView 3.0(3) on AIX Features

CiscoView is a graphical user interface or GUI-based device management software application that provides dynamic status, statistics, and comprehensive configuration information for Cisco Systems' switched internetworking products. CiscoView allows you to display a graphical representation of each network device, display configuration and performance information, and perform minor troubleshooting tasks.

CiscoView allows you to manage the following Cisco devices:

- Cisco 4000 series running Cisco Internetwork Operating System (Cisco IOS™) Software Release 9.21 through 10.3, inclusive
- Cisco 2505 and 2507 running Cisco IOS Software Release 10.0(6) through 10.3, inclusive
- Cisco 2501, 2502, 2503, 2504, 2509, 2510, 2511, 2512, 2513, 2514, 2515, and 2516 running Cisco IOS Software Release 10.2(1.3) through 10.3, inclusive
- Cisco 7000 series (includes 7000 and 7010) and Cisco 7500 series (includes 7505, 7507, and 7513) running Cisco IOS Software Release 9.21 through 11.0(2), inclusive
- Catalyst 5000, 1600, and 1200 series running Catalyst software version 1.0 or later; Catalyst 3000 and Kalpana EPS 2015 switches (any firmware)
- CiscoPro CPW16, CPW 2115, and CPW500 switches (any firmware)
- WS-C1400 series and WS-C1100 series workgroup concentrators (any firmware)
- Cisco LightStream 100 (formerly called the Cisco HyperSwitch A100) running RTOS version 1.2(0) or later

---

**Note** CiscoView supports the Qualified Logical Link Control (QLLC) feature in Cisco IOS Software Release 10.3(7) or later, and in Cisco IOS Software Release 11.0(2) or later.

---

## Documentation Information

The documentation for CiscoView 3.0 includes this document, CD-ROM installation instructions (except when CiscoView is bundled with CiscoWorks), and online help. The primary documentation for CiscoView is the online help. If you have documentation feedback, please send your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

For more information on online help caveats, refer to the section, "Online Help Caveats," later in this document.

## Troubleshooting

If you cannot open a device in CiscoView, you will receive a message indicating that the device is unmanageable. This message indicates one of the following conditions:

- The Simple Network Management Protocol (SNMP) server is not set in the device. You can still ping the device from the management station.
- You have entered an incorrect community string in the **File>Open Device** window.
- The management station cannot reach or successfully ping the device.

- CiscoView will fail to come up after an Interface Processor card is removed from the router because the ifTable still contains information on the card. Reinsert the card or reload the routing image after removing the card to allow CiscoView to work. [CSCdi42488]

## CiscoView 3.0(3) on AIX Caveats

This section lists notes and restrictions that apply to the CiscoView 3.0(3) release.

### Installation Caveats

The installation caveats follow.

### Changing the X Authority of CiscoView Binaries

The following caveat is important if you are running or want to run the switch configuration applications (CiscoPro, Catalyst 3000, and Kalpana EPS 2015 products).

Two versions of CiscoView software are provided with this installation: one requires X authentication to be in place, and one does not. The version of CiscoView software that is installed on your system does not require X authentication for full operation. Read this section if you would like to use or are currently using X authentication.

For more information about X authentication, refer to the next section, “X Access on Your System.” If you are already using or understand X authentication, skip to the section “CiscoView and X Authority.”

### X Access on Your System

The X windowing system supports several forms of access security. The most common are “*xhost*” and “*Xauthority*.”

The *xhost* mechanism controls display access on a per host basis; that is, once enabled for a specific host, any X application from that host can access the display on the machine where the access was granted. Once granted, access is open to all logins.

The *Xauthority* mechanism controls display access on a per process basis; that is, each process is validated before display access is granted. Validation occurs by matching a *token* known to both the client process and the X server. Tokens are created using a script described in the section “Creating Xauthority Tokens.” The list of valid tokens is usually maintained in a file (the default is *.Xauthority* in the user’s home directory). Access is controlled by knowledge of the value of these valid tokens which in turn is controlled by access to the file’s contents. For *Xauthority* to function, the X server process running on a given machine must be started with knowledge or access to the file with the tokens.

---

**Note** The mechanisms *xhost* and *Xauthority* interact. Specifically, once you use *Xauthority*, any use of the **xhost** command, for example, **xhost +machine**, suspends further token validations. Applications can run and display, but functions keyed to *Xauthority* validation (*Xauth* binaries of *Ciscoview* and the Switch *applets*) will not operate correctly. An applet is an application that runs on CiscoView. For proper *Xauthority* operation, the **xhost** command should report that NO hosts are authorized.

---

### CiscoView and Xauthority

CiscoView is a Tcl/Tk application. Tcl/Tk applications can be built with versions of the TK library that enforce or ignore the Xauthority mechanism. This issue is important only when two or more application processes wish to communicate using the Tk *send* function. The Switch applets (domain and channel) are examples of Tcl/Tk applications that are designed to communicate with CiscoView processes using this *send* function.

CiscoView is installed by default with binaries that do not enforce X authentication. If you are running an X server with the Xauthority feature enabled, you will need to install the alternate binaries.

### Changing the CiscoView Binaries

If you choose to install the Xauthority versions of the applications and do not provide the X server support for Xauthority, the applications (such as the Switch applets) will not function properly and will be unable to communicate with CiscoView.

After installation, you can change the binaries in use (or reinstall them) by running the following script:

```
$NMSROOT/bin/chgxauth.sh (-t)
```

The *-t* parameter switches to alternate binaries; the command without the parameter reinstalls the current binaries.

For additional information see the following manual pages: **xauth(1)**, **Xserver(1)**, **xinit(1)**, and **Xsecurity(1)**.

### Creating Xauthority Tokens

Create the following shell script to add authorization tokens to the *.Xauthority* file and start the X server. The following line must be the first line when used as a standalone script:

```
#!/bin/sh
# Get hostname
HOST=`hostname`
# Create new magic cookie key
randomkey=`perl -e 'srand;
    for (1..4) {
        printf("%08x", int(rand(1024*1024*1024*4)));
    }'`
# Add new magic cookie key into .Xauthority
xauth add ${HOST}-alf/unix:0 . $randomkey
xauth add ${HOST}/unix:0 . $randomkey
xauth add ${HOST}:0 . $randomkey
# ***** The following command line will start the
#           X server using the .Xauthority file created.
#
# Start the X server with authorization turned on
exec X -auth $HOME/.Xauthority :0
#End
```

### Creating the .Xauthority File

Before you start the X server, create an *.Xauthority* file. You must create a new *.Xauthority* file when you switch machines because the name of the machine that the server is on is part of the authority mechanism. This is how the X server knows which token to send to the server to which it is connecting.

To create the *.Xauthority* file, you can do any of the following:

- copy part of the script under “Creating X Authority Tokens”
- copy part of the script under “.Xauthority Creation Script Example”
- create your own script

In the “.Xauthority Creation Script Example,” one of the following options is used to generate the random numbers used for the tokens:

- If you have a program that generates md5 signatures, you can use it to generate a strong random number by passing the **-md5** flag.
- If you have md4, edit the script below to use it instead of md5.
- If you do not have md4 or md5, the script assumes you have perl to generate random numbers.
- If you do not have perl, write a program to generate a long random number with an even number (maximum 32) of hexadecimal digits, and run **xauth add** as shown.

---

**Note** md4 and md5 generate values that have an even number of digits. An implementation of md5 can be found in Internet RFC 1321.

---

### **.Xauthority Creation Script Example**

An example of the *.Xauthority* creation script follows. The following line must be the first line when used as a standalone script:

```
#!/bin/sh
# create new .Xauthority file
PATH=/usr/local/X/bin:/usr/gnu/bin:$PATH
# try some security
auth=$HOME/.Xauthority
#cp /dev/null $auth
# generate a nice long random key
if [ "$1" = "-md5" ]; then
    # use a random noise source and get a strong checksum of it.
    # this is probably a stronger random number than the other method.
    key=`pstat -pfs | md5`
else
    # quick and dirty. can probably be recreated if time can be guessed.
    key=`perl -e 'srand; printf int(rand(1000000000000000))'`
    # use $key$key to make sure even length.
    key=$key$key
fi
# add to auth file.
xauth add ${HOST}/unix:0 . $key
xauth add ${HOST}:0 . $key
# Remember to start the X server with the -auth parameter
#End
```

### Starting the Xauthority Server

To start the X server with X authentication enabled, use one of the following commands:

- **exec X**
- **xinit**
- **startX**

The X server for each display (UNIX machine) must be started with the parameter *-auth* or *-auth filename*.

### HyperHelp Resource File

The CiscoView installation puts the X resource file for HyperHelp in the */usr/lib/X11/app-defaults* directory. As different systems have different types of X Windows installations, the CiscoView application does not always read this resource file. When the resource file is not read, the HyperHelp viewer text may be unreadable on your screen. Do one of the following tasks to make sure that this resource file is read:

- Run the following command each time you log in to your system:  
**xrdb -merge /usr/lib/X11/app-defaults/HyperHelp**
- Put the above command in your *.cshrc* or *.profile* file so that it is run automatically every time you log in to your system.
- Move the HyperHelp X resource file to another directory, such as each user's home directory.

[CSCdi41126] [CSCdi33830]

### Installing CiscoView and Workgroup Director on the Same Workstation

If you need to install Workgroup Director and CiscoView on the same workstation, Cisco recommends that you install Workgroup Director before installing CiscoView.

### Installing CiscoView on CiscoWorks 2.0.2 or 3.0.1

If you install CiscoView 3.0(3) on a machine where CiscoWorks 2.0.2 or CiscoWorks 3.0.1 is already loaded, you *must* install CiscoView in the same directory in which CiscoWorks is installed.

### Deinstallation Caveats

The deinstallation caveats follow.

### Deinstalling CiscoView and Retaining Map Icons

If you created map icons in SNM or HP OpenView and want to retain the map icons after deinstalling CiscoView, do not remove the *\$NMSROOT* directory. [CSCdi37187]

## General Caveats

The general caveats follow.

### NumLock Hinders Mouse Operation

Do not set NumLock on the keyboard while using CiscoView. The NumLock key disables certain mouse operations.

### Context-Sensitive Help

Context-sensitive help does not appear when you press F1. [CSCdi43445]

### Bogus Characters in Port Configuration Window

When you access the Configuration Window for a device port (whether by double-clicking the image of a port or by selecting **Configure> Port** on the CiscoView menu), and if a Local Description field appears that is user-settable, click the **Modify** button after typing a description but do not press the Return key. If you press Return before clicking Modify, an extraneous hexadecimal character appears in the Local Description field.

### Catalyst Counter Values

In monitor dialogs, MIB variables of type Counter32 do not display the values correctly. Some of the variables being monitored (graphed) are plotting using absolute values instead of delta values. [CSCdi40858]

### Device Physical View Displays Blank Spaces

When a device physical view displays in CiscoView, system information is displayed below the toolbar area by default. System information includes system description, system location, system uptime, and CPU utilization. If the system information exceeds the width of the physical view, blank spaces display on the sides of the physical view. To remove blank spaces, change the system information display option using the toggle control under the Options menu. [CSCdi44388]

### Port Status Functionality

On Cisco 2503I and Cisco 2504I routers the ports are grayed out. CiscoView scans the interface table for ports that are disabled on these routers and gets a “No such name” response back. When CiscoView receives this response from the agent, all the ports are then grayed out. This problem is related to the Cisco 2503I and Cisco 2504I and will be fixed in the next release of CiscoView. [CSCdi40999]

The CiscoView engine performs an SNMP query on different MIB variables to show the status of ports and LEDs. If the device fails to return a value on any one MIB variable, the status will not be shown on any ports or LEDs. All ports and LEDs will appear with no color and a failure message will display in the status bar. The message will not provide any indication of the problem MIB variable. Status failure may occur due to the following causes:

- The MIB variable that is used for status poll is not supported in a particular software version that is running on a device (noSuch).
  - The value that is returned for a device does not match the MIB definition (bad value).
- [CSCdi41636]

When a single port is monitored, CiscoView appropriately displays the informational message: “No available category for port <port number>.” When multiple ports are monitored, the same message should display. Currently, when multiple ports are being monitored, the error message “Error: bad window path name .mnport-tb.fcI” displays. [CSCdi43193]

CiscoView will not display any port status for Cisco 7500 routers running Cisco IOS images previous to Software Release 11.0 with two FDDI interface cards present. The snmpFddi table shows information for only one interface, even if two interfaces are present. [CSCdi42516]

If routers are not configured properly, you may not see all statuses on all ports. [CSCdi43460]

### Reconfiguring Asynchronous Ports after Reloading Image

If you load a new image, you need to re-enter configuration commands to configure the asynchronous ports as follows:

```
interface Async1
ip unnumbered TokenRing0 #(or Ethernet0)

interface Async8 #(8 asynchronous ports for Cisco 2509/2511; 16 asynchronous ports for
Cisco 2510/2512)
```

[CSCdi37062]

### Rewind Inconsistency on Monitoring Ports Window

The **Rewind** button will not rewind the same way for all CATEGORY selections on a given port type. In some cases the CATEGORY display will be invalid after rewinding. Select the default CATEGORY and rewind to work around the problem. [CSCdi39539]

### Running CiscoView with Little Swap Space

If the server or display workstation is running out of swap space, you will see a message such as “X error: Couldn’t allocate color cell,” and CiscoView will core dump. If you are running other applications, you might want to check your swap space occasionally.

To check swap space on an AIX system, enter the following:

```
hostname% lsps -a
```

If your system is running out of swap space (for example, only 200 KB of swap space remains), quit some of the other applications you are running, or increase your swap space if possible.

[CSCdi37063]

### Running Out of Colors

CiscoView can run out of colors. If this occurs, CiscoView will continue to run, but all the colors it cannot allocate will dither to black or white. You can avoid this by starting CiscoView before starting color-intensive applications, or by using a private color map for the color-intensive applications (such as **application\_name -install**).



## Device-Specific Caveats for CiscoPro 16, 2115, and 500, Catalyst 3000, and Kalpana EPS2015

The caveats for the above mentioned devices follow.

### CiscoView Times Out

In high traffic situations, you may experience timeouts. To increase the timeout period, select **Options>Properties** from the CiscoView menu and change the value for the Timeout field.

### CV\_BBAreaX1 Error Message

The error window “CV\_BBAreaX1 no such variable” may display when you click the mouse. Close the window and ignore it.

### Dragging Port Image Problem

In OpenWindows, when you drag a port across a device bitmap in order to set the EtherChannel/Domain information, the port image can get stuck on the border of the bitmap. To resolve this problem, move the pointer onto the port and click the middle mouse button.

### Exiting CiscoView Causes Applications to Close

If you are using the CiscoPro CPW16 or Catalyst 3000 and close the CiscoView window, any application window that was launched from it will automatically close. Remember to close the EtherChannel and Domain Configuration application windows before you open another CiscoView application or exit from the CiscoView application. There is no limitation on the number of CiscoView applications that you can run.

### False Error Reported after Setting Parameters

On the CiscoPro CPW16 and Catalyst 3000, when you try to set parameters for the EtherChannel/Domain application under moderate to high traffic conditions, CiscoView incorrectly displays an error window indicating that the operation was not successful. In reality, the command was successful. Dismiss the error dialog and CiscoView will continue to function properly.

### HP OpenView Discovery Issue

When a switch is configured as two or more domains, NetView discovery may not work properly and may discover only one of the domains. If this occurs, use CiscoView to manage the domain directly rather than launching it from the map.

### Kalpana ProStack Power Supply Link Problem

The rear view of the Kalpana Prostack Matrix power supply does not indicate whether the connector link is up or down (for example, the connector does not come up green if there is a link).

### Shadows on Bitmaps

On SunOS using OpenWindows, when you open menu boxes shadows display on the bitmaps. To remove the shadows, use the **Refresh** option in OpenWindows or the CiscoView **View** menu.

## Device-Specific Caveats for WS-C1100 and WS-C1400 Series Workgroup Concentrators

The caveats for the above mentioned devices follow.

### Community String Mismatching

A mismatch between the user-entered community strings “read-only,” “read-write,” and “read-writeld” entered through the Command Line Interface (CLI) leads to ambiguous error conditions such as “noSuchName” or “timeout.” To avoid these errors, use identical community strings in CiscoView and the corresponding agents.

### Online Help Caveats

This section lists the online help links that are currently missing or broken.

- The **Help>Contents** and **Help>Using CiscoView** display the same window.
- The help for the Configure Card window shows help for the device.
- Help is not displayed when you click Help in the **File>Communities** window.
- Help is not displayed in the Monitor port window for X.25 circuits. [CSCdi36557]

## Cisco Information Online

Cisco Information Online (CIO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CIO to obtain additional content and services.

Available 24 hours a day, 7 days a week, CIO provides a wealth of standard and value-added services to Cisco's customers and business partners. CIO services include product information, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CIO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously—a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CIO (called "CIO Classic") supports Zmodem, Kermit, Xmodem, FTP, Internet e-mail, and fax download options, and is excellent for quick access to information over lower bandwidths. The WWW version of CIO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CIO in the following ways:

- WWW: <http://www.cisco.com>.
- Telnet: [cio.cisco.com](telnet://cio.cisco.com).
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and baud rates up to 14.4 kbps.

For a copy of CIO's Frequently Asked Questions (FAQ), contact [cio-help@cisco.com](mailto:cio-help@cisco.com). For additional information, contact [cio-team@cisco.com](mailto:cio-team@cisco.com).

---

**Note** If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or [tac@cisco.com](mailto:tac@cisco.com). To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or [cs-rep@cisco.com](mailto:cs-rep@cisco.com).

---

---

AtmDirector, Catalyst, CD-PAC, CiscoFusion, Cisco IOS, the Cisco IOS logo, CiscoPro, Cisco Systems, CiscoView, CiscoVision, CiscoWorks, ClickStart, ControlStream, EtherChannel, HubSwitch, LAN<sup>2</sup>LAN Enterprise, LAN<sup>2</sup>LAN Remote Office, LightSwitch, Newport Systems Solutions, *Packet*, Point and Click Internetworking, RouteStream, SMARTnet, StreamView, SwitchBank, SwitchProbe, SwitchVision, SynchroniCD, *The Cell*, TokenSwitch, TrafficDirector, VirtualStream, VlanDirector, WNIC, Workgroup Director, Workgroup Stack, and XCI are trademarks, Access by Cisco and Bringing the power of internetworking to everyone are service marks, and Cisco, the Cisco Systems logo, EtherSwitch, IGRP, Kalpana, the Kalpana logo, LightStream, and UniverCD are registered trademarks of Cisco Systems, Inc. All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective owners.

Copyright © 1996, Cisco Systems, Inc.  
All rights reserved. Printed in USA.  
9511R

