



# Release Notes for the Catalyst Express 500 Switches, Cisco IOS Release 12.2(25)FY

---

**September 13, 2005**

The Cisco IOS Release 12.2(25)FY runs on all Catalyst Express 500 switches.

These release notes include important information about this Cisco IOS release and any limitations, restrictions, and caveats that apply to it. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the device manager, and check the **Switch Information** area on the dashboard.

The key features are described in the *User Guide for the Catalyst Express 500 Switches*. For the complete list of Catalyst Express 500 switch documentation, see the [“Related Documentation” section on page 5](#).

## Contents

This information is in the release notes:

- [“System Requirements” section on page 2](#)
- [“Upgrading the Switch Software” section on page 3](#)
- [“Limitations and Restrictions” section on page 3](#)
- [“Open Caveats” section on page 3](#)
- [“Documentation Updates” section on page 4](#)
- [“Related Documentation” section on page 5](#)
- [“Obtaining Documentation” section on page 5](#)
- [“Documentation Feedback” section on page 6](#)
- [“Obtaining Technical Assistance” section on page 8](#)
- [“Obtaining Additional Publications and Information” section on page 9](#)



---

**Corporate Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2005 Cisco Systems, Inc. All rights reserved.

# System Requirements

The system requirements are described in these sections:

- “Hardware Supported” section on page 2
- “Device Manager System Requirements” section on page 2

## Hardware Supported

Table 1 lists the hardware supported on Cisco IOS Release 12.2(25)FY.

**Table 1** Supported Hardware

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst Express 500-24TT	24 10/100BASE-T Ethernet ports and 2 10/100/1000BASE-T Ethernet ports	Cisco IOS Release 12.2(25)FY
Catalyst Express 500-24LC	20 10/100BASE-T Ethernet ports, 4 10/100 PoE <sup>1</sup> ports, and 2 dual-purpose uplinks <sup>2</sup> (two 10/100/1000BASE-T copper ports and two SFP <sup>3</sup> module slots)	Cisco IOS Release 12.2(25)FY
Catalyst Express 500-24PC	24 10/100 PoE ports, and 2 dual-purpose uplinks (two 10/100/1000BASE-T copper ports and two SFP module slots)	Cisco IOS Release 12.2(25)FY
Catalyst Express 500G-12TC	8 10/100/1000BASE-T Ethernet ports and 4 dual-purpose uplinks (four 10/100/1000BASE-T copper ports and four SFP module slots)	Cisco IOS Release 12.2(25)FY
SFP <sup>4</sup> modules	100BASE-BX, -FX, -LX 1000BASE-LX, -SX	Cisco IOS Release 12.2(25)FY
Redundant power system	Cisco RPS 675 redundant power system <sup>5</sup>	Supported on all software releases

1. PoE = Power over Ethernet
2. Each uplink port is considered a single interface with dual front ends (RJ-45 connector and SFP module slot). The dual front ends are not redundant interfaces, and only one port of the pair is active.
3. SFP = small form-factor pluggable
4. Only Cisco SFP modules supported.
5. Only on the Catalyst Express 500-24PC switch.

## Device Manager System Requirements

The device manager hardware and software requirements are described in the *User Guide for the Catalyst Express 500 Switches*.

# Upgrading the Switch Software

The software upgrade procedure is described in the *User Guide for the Catalyst Express 500 Switches*.

## Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

### Device Manager Limitations

This is the device manager limitation:

- When a PC is connected directly to a switch port, the username password dialog appears twice before the device manager page appears.

The workaround is to enter the username and password in both dialog windows. (CSCei30778)

### Open Caveats

These are the open caveats with possibly unexpected activity:

- CSCei77157

When a copper RJ-45 connector is connected to a dual-purpose uplink port, you change the port speed to a nondefault setting, and then insert an SFP module into the fiber port, the port might be error disabled.

The workaround is to unplug the SFP module, change the speed setting to **auto**, and then reenabling the port.

- CSCei77607

When a 100BASE-FX-FE module inserted in the switch is connected to a link partner 100BASE-FX-GE module, sometimes there is a duplex mismatch.

The workaround is to configure the full duplex setting on the link partner.

- CSCei77817

When the switch time is set at least 60 minutes faster than the connected PC time, the device manager responds slowly, and the refresh function takes longer than normal to complete.

The workaround is to use the device manager to correct the switch time so that it is same as the PC time.

- CSCsb53732

The redundant power system (RPS) status LED on the switch does not match the description given in the device manager online help legend.

The workaround is to use the status LED on the RPS device, which correctly matches the device manager online help legend.

- CSCsb63132

When you access the device manager through a secured session and change the switch software image from a cryptographic to a noncryptographic image, the device manager cannot detect if the switch is fully reloaded. It displays this message:

```
Switch is not yet reloaded, device manager is waiting for a response from the device.
```

The workaround is to close the device manager and the browser. Open a new browser session, and enter **http://** before the switch IP address.

This problem only happens when the device manager is accessed through a secured session. When the device is running a cryptographic image and device manager is accessed through a standard session (**http://**) the change to a noncryptographic image completes successfully.

- CSCsb66458

When a PC is connected directly to a switch port, the software upgrade procedure is not successful if you have not previously loaded the software image on the PC.

Make sure that you have downloaded the switch software image from Cisco.com to your PC or network drive before following the software upgrade procedure.

- CSCsb66596

When the Desktop Smartports role is applied to a port and you are using Cisco Network Assistant with a security level other than **High**, this error message appears:

```
Dot1x authentication is supported on "Desktop" Smartport only. Use "Smartports" window to change the role of this port or disconnect the connected device.
```

The workaround is to ignore this message when the security level is set to **High** to enforce IEEE 802.1X authentication on the Desktop Smartports port role.

- CSCsb71365

If you close your browser session during a software upgrade or you lose internet connectivity, there is no indication of a software upgrade failure. When you restart the switch, there might be unexpected behavior, or some device manager pages will not display.

The workaround is to follow the software recovery procedure described in the user guide. Select option 3 to delete the system configuration and boot with the factory default Cisco IOS image. Follow the software upgrade procedure.

- CSCsb80043

When you replace a 100BASE-FX-GE SFP module with a 1000BASE-LX, or 1000BASE-SX SFP module, the module port shows collisions.

The workaround is to restart the switch when you replace a 100BASE-FX-GE SFP module with a 1000BASE-LX, or 1000BASE-SX SFP module.

## Documentation Updates

These are the updates for the device manager online help:

- The device manager online help incorrectly states that the username that you enter is case sensitive. The username is *not* case sensitive.
- The device manager online help legend incorrectly states that the PoE LED solid amber color means that one or more ports have PoE administratively disabled.

## Related Documentation

These documents provide complete information about the Catalyst Express 500 switches and are available at Cisco.com:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/catex500/index.htm>

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the “[Obtaining Documentation](#)” section on page 5.

These documents provide complete information about the Catalyst Express 500 switches:

- *User Guide for the Catalyst Express 500 Switches* (not orderable but available on Cisco.com)
- *Getting Started Guide for the Catalyst Express 500 Switches* (order number DOC-7817084=)
- *Regulatory Compliance and Safety Information for the Catalyst Express 500 Switches* (order number DOC-7817085=)
- Device manager online help (available on the switch)

For other information about related products, see these documents:

- *Getting Started with Cisco Network Assistant* (not orderable but available on Cisco.com)
- *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com)
- *Cisco Small Form-Factor Pluggable Modules Installation Notes* (not orderable but available on Cisco.com)
- *Cisco RPS 675 Redundant Power System Hardware Installation Guide* (order number DOC-7815201=)

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

## Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:  
<http://www.cisco.com/en/US/partner/ordering/>
- Instructions for ordering documentation using the Ordering tool are at this URL:  
[http://www.cisco.com/univercd/cc/td/doc/es\\_inpck/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm)
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

## Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

# Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—[security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



### Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.htm](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.htm)

The link on this page has the current PGP key ID in use.

# Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco SMB Support Assistant provides service and support for the Catalyst Express 500 switches and other Cisco networking products. Cisco SMB Support Assistant offers simple-to-use Portal and Client applications, 8 hours a day, 5 days a week TAC support, and Advanced Replacement Next Business Day. If you do not hold a valid Cisco service contract, please contact your reseller.

## SMB Support Assistant Portal and Client

The Cisco SMB Support Assistant Portal and Client applications are management tools designed specifically for SMBs. This secure portfolio of tools helps you access information and inventory as well as providing device management and technical support tools for covered Cisco networking devices.

The Cisco SMB Support Assistant Portal (*Portal*) is the online tool, serving as the how-to arm and starting point for a particular task. It is specifically designed to offer self-help and support for products covered by Cisco SMB Support Assistant.

The Cisco SMB Support Assistant Client (*Client*) is the application stored locally on your computer hard drive and can be installed much like common Windows-based programs. It runs the tools for performing particular tasks and interacts with the Portal in launching the support functions.

The Portal and Client are available 24 hours a day, 365 days a year, at this URL:

<http://tools.cisco.com/Support/SMBSA/Login.do>

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

## Submitting a Service Request

If you cannot successfully resolve an issue through the self-help tools, click the Open Service Request option in the Portal and fill out the online form. This will immediately submit the request to the Cisco SMB Technical Assistance Center (Cisco SMB TAC). Requests can be submitted at any time, 24 hours a day, 365 days a year. A Cisco SMB TAC engineer will then respond to the request within 1 business day during normal business hours.

If your issue is not resolved by using the recommended resources, your service request is assigned to a Cisco TAC engineer. To open a service request by telephone, use one of these numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

# Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:  
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:  
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:  
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:  
<http://www.cisco.com/go/iqmagazine>  
or view the digital edition at this URL:  
<http://ciscoiq.texterity.com/ciscoiq/sample/>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:  
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:  
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:  
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:  
<http://www.cisco.com/en/US/learning/index.html>

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)