



Release Notes for Cisco iSCSI Driver Version 4.2.1 for Microsoft Windows

June 1, 2005

These release notes support Cisco iSCSI Driver version 4.2.1 for Microsoft Windows. For a list of software caveats that apply to version 4.2.1, see the “[Caveats](#)” section. The caveats are updated for every maintenance version and are located on [Cisco.com](#).

Contents

These release notes describe the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New and Changed Information, page 3](#)
- [Installation Notes, page 4](#)
- [Caveats, page 5](#)
- [Troubleshooting, page 7](#)
- [Related Documentation, page 7](#)
- [Service and Support, page 8](#)
- [Obtaining Documentation, page 8](#)
- [Documentation Feedback, page 9](#)
- [Cisco Product Security Overview, page 9](#)
- [Obtaining Technical Assistance, page 10](#)
- [Obtaining Additional Publications and Information, page 12](#)



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

© 2005 Cisco Systems, Inc. All rights reserved.

Introduction

The iSCSI Driver for Microsoft Windows provides an IP host with the ability to access storage through an IP network. The iSCSI driver uses the iSCSI protocol to transport SCSI requests and responses over an IP network between the IP host and a Cisco SN 5400 or MDS 9000 Series system.

Architecturally, the iSCSI driver combines with the IP host's TCP/IP stack, network drivers, and network interface cards (NICs) to provide the same functions as a SCSI or a Fibre Channel adapter driver with a host bus adapter (HBA).

The iSCSI driver provides a transport for SCSI requests and responses for storage devices; however, instead of providing a transport for directly attached devices, the driver transports the SCSI requests and responses between the IP host and a Cisco SN 5400 or MDS 9000 Series system via an IP network. The SN 5400 or MDS 9000 Series system, in turn, transports SCSI requests and responses between it and the storage devices attached to it.

Once the iSCSI driver is installed and started, the host proceeds with a discovery process for storage devices.

A more technical description of the driver's design and its features can be found in the readme file that accompanies the iSCSI driver in the downloaded driver archive file.

**Note**

The iSCSI protocol is an IETF-defined protocol for IP storage (ips). For more information about the iSCSI protocol, refer to the IETF standards for IP storage at <http://www.ietf.org>.

System Requirements

This section describes the system requirements for version 4.2.1 and includes the following information:

- [Operating System Requirements, page 2](#)
- [SN 5400 Series System Software Requirements, page 3](#)
- [MDS 9000 Series System Software Requirements, page 3](#)

Operating System Requirements

- The driver requires either Microsoft Windows XP Professional with service pack 2 or later, Microsoft Windows Server 2003 with service pack 1 or later, or Microsoft Windows 2000 Professional, Advanced Server or Datacenter Server with service pack 3 or later.

If the iSCSI driver is running on a Microsoft Windows 2000 Professional, Advanced Server or Datacenter Server, hotfix Q839635 is also required.

If the iSCSI driver is running on a Microsoft Windows 2000 Advanced Server Cluster node, Microsoft Hotfix Q307939 is also required.

These hotfixes do not appear on the Microsoft Hotfix website; you must specifically request them.

Contact Microsoft Product Support Services to obtain the hotfixes. For a complete list of Microsoft Product Support Services phone numbers and information about support costs, visit the following Microsoft website: <http://support.microsoft.com/default.aspx?scid=fn;EN-US;CNTACTMS>.

**Note**

In special cases, charges that are ordinarily incurred for support calls may be canceled if a Microsoft Support Professional determines that a specific update will resolve your problem. The typical support costs will apply to additional support questions and issues that do not qualify for the specific update in question.

Request the hotfixes for the specific Knowledge Base (KB) article (307939 and 839635). You will be asked to supply an e-mail address. You will receive an e-mail message with a link to an FTP site where you can download the hotfixes. The e-mail message will also contain a password that you will be prompted to enter when you open the hotfix files.

For additional information about these hotfixes, access the Microsoft website at <http://www.microsoft.com> and follow the support link to view KB article 307939 and 839635.

- The driver supports single-processor and multiprocessor machines.
- To ensure the best performance for iSCSI drivers, the extended windowing feature of TCP should be enabled on all IP hosts connecting to the SN 5400 Series system. In general, a larger window size enhances SN 5400 Series system performance.
- The receive and transmit flow control feature of the Gigabit Ethernet driver should be enabled on all IP hosts connecting to the SN 5400 Series system.

SN 5400 Series System Software Requirements

The iSCSI driver version 4.2.1 for Microsoft Windows is interoperable with a Cisco SN 5400 Series system running software release 3.2 or later. This version of the driver is not interoperable with a Cisco SN 5400 Series system running software release 2.5 or earlier.

MDS 9000 Series System Software Requirements

The iSCSI driver version 4.2.1 for Microsoft Windows is interoperable with a Cisco MDS 9000 Series system running SAN-OS Release 1.1(1) or later.

New and Changed Information

- iSCSI redirect feature support—Allows all iSCSI login requests to be redirected to a different target or portal. This feature is used by some disk arrays for load balancing. The behavior of this feature follows the requirements outlined in the iSCSI RFC and is transparent to the user.
- Asynchronous event notification support—Allow configuration changes that occur at the target to be communicated to the initiator as asynchronous messages. Async event notification must be enabled by the initiator negotiating the key SendAsyncText. The following events are notified by asynchronous messages:
 - Portal Online
 - Portal Offline
 - Target Online
 - Target Offline
 - LunChange

- Enhanced support for multi-path I/O software—Allows you to modify the configuration of the iSCSI driver to facilitate more efficient operation of the multi-pathing software.
- Silent installation feature
- Installation and use without reboot—The iSCSI driver can now be installed and started without rebooting the server.
- LUN information display—Allows you to view LUN details, including LUN ID, disk number and path.
- Enhanced support for initiator names—Allows you to change the Initiator name via the Global Settings tab.

See the readme file for additional information about all new features.

Installation Notes

This section describes how to obtain iSCSI driver software and upgrade an existing iSCSI driver installation. It also describes important information about using the iSCSI driver with Cisco Network Boot. It includes the following information:

- [Downloading the iSCSI Driver, page 4](#)
- [Installing, Upgrading and Uninstalling iSCSI Driver Software, page 5](#)
- [Using the iSCSI Driver with Cisco Network Boot, page 5](#)

Downloading the iSCSI Driver

Registered Cisco.com users can download the most current Cisco iSCSI drivers, readme files and release notes from Cisco.com. In addition, information about driver compatibility and other relevant driver information is available on Cisco.com. You can access software and related information by following these instructions:

-
- Step 1** At <http://www.cisco.com>, log in to Cisco.com. Click **Technical Support & Documentation** and **Downloads**.
 - Step 2** At the Downloads web page, under Software Products & Downloads, click **Storage Networking Software**.
 - Step 3** At the Storage Networking Software web page, click **Cisco iSCSI Drivers**.
 - Step 4** At the Software Download web page, click the file that you want to download. Another software download web page will be displayed with detailed information about the download file and Cisco's Software License Agreement. Follow the instructions on that and any subsequent web pages to download the software.
 - Step 5** To install and configure an iSCSI driver, see the readme file that accompanies the iSCSI driver (in the downloaded driver archive file) and the appropriate release notes.
-

Installing, Upgrading and Uninstalling iSCSI Driver Software

For complete procedures to install and configure, upgrade, or uninstall iSCSI driver software, refer to the readme file that accompanies the iSCSI driver (in the downloaded driver archive file).

Using the iSCSI Driver with Cisco Network Boot

The iSCSI driver version 4.2.1 supports Cisco Network Boot, a product that allows you to initiate a boot of a computer without an attached disk drive. Cisco Network Boot supports a boot of the following Microsoft Windows operating systems:

- Microsoft Windows 2000 (Server or Advanced Server) with service pack 3 or higher
- Microsoft Windows XP (Professional Edition) with service pack 2 or higher
- Microsoft Windows Server 2003 (Enterprise, Standard or Web Edition) with service pack 1 or higher

With Cisco Network Boot, a computer without a directly attached disk drive uses iSCSI protocol via an iSCSI driver to boot from an iSCSI disk through an IP network and a Cisco SN 5400 or MDS 9000 Series system.

For more information on Cisco Network Boot, refer to the *Cisco Network Boot Installation and Configuration Guide* and the associated release notes document. These documents are available as electronic document on Cisco.com and the Documentation CD-ROM.

Caveats

Caveats describe unexpected behavior or defects in the specified version of the driver. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

This document describes open and resolved severity 1 and 2 caveats and selected caveats of other severities, for the iSCSI driver version 4.2.1 for Microsoft Windows.

- The “[Open Caveats](#)” section lists caveats that are open in the current release and may be open in previous releases.
- The “[Resolved Caveats](#)” section lists caveats that are resolved in this release, but open in previous releases.



Note

If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any version. You can reach Bug Navigator II on Cisco.com at Service & Support: http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Open Caveats

There are no open severity 1 or 2 caveats for the iSCSI driver version 4.2.1 for Microsoft Windows.

Resolved Caveats

- CSCin70117
Deleting a portal and selecting the Status node immediately may cause the MMC application to crash.
Workaround: None. Synchronization was added to version 4.2.1 to protect the data buffer read/write.
- CSCin70120
After minimizing the MMC application, a high volume of traffic may make the application difficult to restore.
Workaround: The MMC application restores properly when the traffic volume is reduced. This problem is resolved in version 4.2.1.
- CSCin75490
Disabling all targets using global settings may result in a system hang if a Windows XP system is netbooted.
Workaround: Do not disable network boot targets in both the global and target settings. Version 4.2.1 disables this capability.
- CSCin77304
Disabling a target in the global settings may not actually drop the connection to the SCSI routing instance.
Workaround: None. This problem is resolved in version 4.2.1.
- CSCin78080
In certain circumstances, a login to a Netbooted image fails, and the local drive is corrupted.
Workaround: None. This problem is resolved in version 4.2.1.
- CSCin78349
After upgrading the driver, adding or removing an IP address may result in a WMI error.
Workaround: Be sure to follow the instructions in the readme file when upgrading an iSCSI driver. This problem is resolved in version 4.2.1.
- CSCin80263
Adding and deleting portals and rebooting the MDS system several times may result in a Windows system failure.
Workaround: None. This problem is resolved in version 4.2.1.
- CSCin80428
Deleting an IP address while running discovery to a large number of IP addresses during a time of heavy traffic to targets may result in a system reboot.
Workaround: None. This problem is resolved in version 4.2.1.

- CSCin81632

The “DisconnectTimeOutValue” configured in the MMC application may not be properly used by the iSCSI driver.

Workaround: None. The “DisconnectTimeOutValue” is reflected in the driver for timing out the packets when connection goes down. The default “DisconnectTimeOutValue” is 90 seconds. The Microsoft Windows SCSI PORT driver might time out commands on its own. So increasing the “DisconnectTimeOutValue” does not guarantee that all the commands are pending until the time out. It is seen that SCSI PORT driver starts timing out some commands normally after 90 seconds. If the DisconnectTimeOutValue is decreased, the commands start to fail immediately after the time out.

- CSCin88126

Microsoft Windows may reboot when running iSCSI sessions with the Microsoft Driver Verifier on.

Workaround: None. This problem is resolved in version 4.2.1.

Troubleshooting

Cisco iSCSI driver troubleshooting information is available on the Cisco.com web site.

You can access troubleshooting information by following these instructions:

-
- Step 1** At <http://www.cisco.com>, log in to Cisco.com. Click **Technical Support and Documentation**, and select **Technical Support and Documentation** from the menu.
 - Step 2** At the Technical Support and Documentation web page, under **Documentation and Tools**, click **Storage Networking**.
 - Step 3** At the Storage Networking Support Resources page, click **Cisco SN 5400 Series Storage Routers**.
 - Step 4** At the SN 5400 Series Storage Routers web page, click the **Troubleshooting TechNotes** link.
 - Step 5** At the Tech Notes page, click the appropriate link for your iSCSI driver.
-

You can access iSCSI driver FAQs by following these instructions:

-
- Step 1** At <http://www.cisco.com>, log in to Cisco.com. Click **Products & Solutions**, and select **Storage Networking** and **SN 5400 Series Storage Routers** from the menu.
 - Step 2** At the Cisco SN 5400 Series Storage Routers web page, click **Product Literature**.
 - Step 3** At the Product Literature web page, click the **Q&A** link.
 - Step 4** At the Q&A page, click the appropriate link for your iSCSI driver.
-

Related Documentation

The following sections describe the related documentation available for the iSCSI Driver version 4.2.1 for Microsoft Windows. These documents consist of the iSCSI driver release notes and readme file.

Release-Specific Documents

This Release Notes document and the readme file are the only documents specific to iSCSI Driver version 4.2.1 for Microsoft Windows. The release notes document is located on Cisco.com and the Documentation DVD. The iSCSI driver readme file is available in electronic format, as part of the software download package. See the “[Downloading the iSCSI Driver](#)” section on page 4 for details.

Service and Support

For service and support for a product purchased from a reseller, contact the reseller, who offers a wide variety of Cisco service and support programs described in “Service and Support” of Cisco Information Packet shipped with your product.

**Note**

If you purchased your product from a reseller, you can access Cisco.com as a guest. Cisco.com is Cisco Systems' primary real-time support channel. Your reseller offers programs that include direct access to Cisco.com services.

For service and support for a product purchased directly from Cisco, use Cisco.com.

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/univercd/home/home.htm>

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

Documentation DVD

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

Registered Cisco.com users (Cisco direct customers) can order a Cisco 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

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- 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 send comments about technical documentation to 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

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

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
- Nonemergencies—psirt@cisco.com



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 that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

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

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

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

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following 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>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

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, 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>

- *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>

- 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.



© 2005 Cisco Systems, Inc. All rights reserved.