

Release Notes for the Cisco NSS4000 and NSS6000 Series Network Storage System, Version 1.21.0

February 2011

These release notes contain important information about the Version 1.21.0 release of the NSS4000/NSS4100 and NSS6000/NSS6100 Network Storage Systems and any limitations, restrictions, and caveats that apply to these products.

Contents

The following information is included in the release notes:

- **Compatibility**
- **Downloading and Upgrading the Firmware**
- **Open Caveats**
- **Closed Caveats**
- **Related Information**

Compatibility

When the NSS is joined to the Windows Server 2008 domain and multiple users are sharing the same file, these are the compatibility issues that can occur:

- When accessing a database file (such as a Microsoft Access file), files opened by the user automatically obtain an exclusive lock, blocking other users from opening the files, even in read-only mode.

- In other applications, when multiple users access the same file, each user has read-write access privileges. This can cause the file to be overwritten and can lead to data loss. If this occurs, no user warning message appears.

Although this feature is working, Cisco does not fully support joining the NSS to the Windows Active Directory Server (ADS) in a Windows Server 2008 environment. This workaround only applies to a single user. (CSCsw93385)

NOTE NSS does not support downgrading the firmware. Upgrading to a wrong or earlier version of the firmware might cause undesirable effects, including loss of data, corrupted data, or system outage.

Downloading and Upgrading the Firmware

This procedure describes how to upgrade the firmware on the NSS by using the NSS Configuration graphical user interface (GUI).

NOTE Back up the system configuration file to a USB flash device and/or a RAID volume by using the Configuration GUI before you upgrade the firmware. From the **Manager Menu**, click **Admin > Configuration** to backup the file.

To download and upgrade the NSS firmware:

STEP 1 Download the latest image from the Cisco support website to your local computer. See <http://www.cisco.com/support/index.shtml> for further details. After downloading, **do not unzip the file**.

STEP 2 Log into the Configuration GUI.

STEP 3 From the **Manager Menu**, click **Admin > Maintenance**.

STEP 4 Click the **Browse** button and navigate to the specific firmware upgrade image:

The firmware filename for the NSS4000 is *NSS4000_FW_1.21.0.tar.gz*.

The firmware filename for the NSS6000 is *NSS6000_FW_1.21.0.tar.gz*.

STEP 5 Click the **Upgrade Firmware** button.

STEP 6 Run this procedure again by repeating Steps 2 through 5.

Performing the upgrade twice allows the system to continue to operate properly (when running the latest firmware), if a system failure occurs.

NOTE If you are moving drives between two NSS systems, make sure that both of the systems are using the latest firmware and that the system configurations are saved on USB memory sticks and/or a RAID volume.

- When upgrading the firmware from v1.12 to v1.14, v1.12 to v1.20.1, or v1.12 to v1.21.0 the Configuration GUI displays a "Programming images.." message for more than 12 minutes (the time it takes to upgrade the firmware is usually 5 to 10 minutes).

The workaround is to wait at least 15 minutes to complete the upgrade and then power cycle the NSS by removing the power cord. Do not try and access the Configuration GUI during this time. (CSCsx17923)

Base Model Firmware

The firmware filename for the NSS4000 is *NSS4000_FW_1.21.0.tar.gz*.

The firmware filename for the NSS6000 is *NSS6000_FW_1.21.0.tar.gz*.

For more information about upgrading the firmware, see the *NSS4000/NSS6000 Administration Guide* available on Cisco.com.

Open Caveats

These are the open caveats for this release. These caveats apply to both the NSS4000 and NSS6000 unless otherwise specified.

- CSCsw86726

When the NSS sends out a broadcast message to discover an NIS server, the broadcast is only sent to the physical interfaces, not over any VLANs that are defined in the system.

The workaround is to not use the NSS in networks where NIS servers are only accessible over VLANs.

- CSCsw86844

If you delete and then recreate a user account from an ADS domain, the user cannot log in to the NSS by using the CIFS, FTP, or NFS protocols.

The workaround is to create another ADS user account with a different name.

Release Notes

- CSCta87135

When using filenames with Chinese characters, characters are lost when transferring the files to the NSS by using the FTP protocol.

The workaround is to use the CIFS protocol.

- CSCtl45049

If a volume is locked (encrypted) and used for a home location, you might not be able to unlock the volume or access the corresponding share. This issue does not apply to locking or unlocking a volume that is not dedicated for “home location.”

The workaround is to reboot the device and unlock the volume again. The share should then be accessible.

Closed Caveats

Resolved in Firmware Version 1.21.0

Closed in Version 1.21.0 Due to Working As Designed

- CSCtf79245

When user quota limit is exceeded, the NSS will prompt a warning from the log, in addition to sending trap messages to the SNMP manager. This can be slow and the NSS can take (20 to 30 minutes) to send the trap message.

The workaround is to wait for the system SNMP process periodic audit (30 minutes interval) and the SNMP trap will be sent to the SNMP manager.

- CSCtg85937

Offline files issue with Windows Vista and Windows 7 using Microsoft Office 2007. When using offline files with Windows Vista, the owner of a file will see his own files just fine but non-owner users will see the file as a xxxxxxxx.TMP instead of (x=1hex value). This is affecting the Microsoft Office files only. Text (.txt) and other files not modified using Microsoft Office are correctly synchronized. This issue does not affect Windows XP offline files.

This is a known bug for Microsoft Window OS. Please check <http://support.microsoft.com/kb/935663/en-us> for more details about the Windows fix.

Fixed in Version 1.21.0

- CSCsv34612

Web access log for successful or failed login are recorded as the same. An administrator could not track a failed attempt or unauthorized access.

- CSCsv34612

Backup job is stalled if a file is added into a different folder in the share after the backup of that particular share has started. The backup job hangs and the backup process from the GUI is not completed. Also, the logs in the "/tmp" folder are not cleared.

- CSCsv47104

When FTP login is attempted, both successful login and failure to login trigger the message that the user is not known, since the login process is sent to Samba for validation. However, with a successful login, the connection is established. This applies to both a local user and NIS user. ADS user successful login and failure to login attempts are reported correctly.

- CSCsw85367

Network Access Policy/Filter does not work for some protocols, such as SmartFTP and CuteFTP. For example, setting a drop or reject filter would still allow traffic to flow.

- CSCsw86562

When the default network filtering policy is set to Drop, there is not an automatic allow filter created for the default gateway. This results in all traffic from the default gateway being dropped, which causes access to the NFS share to fail.

- CSCsw86787

Using Windows Vista, soft quotas specified in the NAS interface appear to be treated as hard quotas. A Windows Vista client cannot write files to the NAS beyond the point where the soft quota limit will be exceeded. This also applies to Windows 2003.

- CSCtg89974, CSCtg89979

DMM does not stop the array with the following cases; FTP IO, NFS IO, IO on encrypted volumes and home directories located on the array.

NFS shares are not exported when shutting down an array. This also applies to FTP shares. Access to FTP shares continue even after degradation of the array. DMM erroneously prints log messages that a RAID array has been stopped although it is still active. DMM does not stop IO on encrypted volumes and home directories located on the array.

- CSCth22472

Encrypted volumes and shares disappear after a firmware upgrade. When home directories are set up on an encrypted volume, it can trigger this issue whereas the shares disappears after a system upgrade. The share that disappears is specific to Samba configuration files and the share was set as not available.

Related Information

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Cisco Small Business Firmware Downloads	<p>www.cisco.com/go/smallbizfirmware</p> <p>Select a link to download firmware for Cisco Small Business Products. No login is required.</p> <p>Downloads for all other Cisco Small Business products, including Network Storage Systems, are available in the Download area on Cisco.com at www.cisco.com/go/software (registration/login required).</p>
Product Documentation	
NSS4000 and NSS6000	www.cisco.com/en/US/products/ps9957/tsd_products_support_series_home.html
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

© 2011 Cisco Systems, Inc. All rights reserved.

OL-24526-01