

Release Notes for the Cisco NSS4000 and NSS6000 Series, Version 1.16

November, 2009

These release notes contain important information about the Version 1.16 release of the NSS4000/NSS4100 and NSS6000/NSS6100 Network Storage Systems and any limitations, restrictions, and caveats that apply to these products.

Contents

This information is in the release notes:

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

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)

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.

Base Model	Firmware
NSS4000	NSS4000_fwupgrade_0116.tar.gz
NSS6000	NSS6000_fwupgrade_0116.tar.gz

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 *NSSxxxx_fwupgrade_0116.tar.gz* firmware upgrade image.

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 or v1.12 to v1.16, 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)

- When the NSS is joined to an ADS domain and you upgrade the firmware, the ADS is unable to access a share.

The workaround is to rejoin the NSS to the ADS domain. (CSCsw94409)

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.

- CSCsw86058

When the NSS is running over a network that is on a different subnet, a user cannot mount a CIFS connection by using a hostname.

The workaround is to mount the CIFS connection by using an IP address.

- CSCsw86138

When an unexpected power cycle occurs on the NSS, the time might be corrupted on the NSS. This only applies if the time is set manually, not by using NTP.

When this occurs, a pop-up alert window appears when you access Configuration GUI after the unexpected shutdown.

The workaround is to manually check the time in the GUI. From the **Manager Menu**, click **Admin** → **Time** and correct the time if necessary.

- CSCsw86187

If a data write operation is in progress, and the system power is interrupted, data stored in a degraded RAID1 or RAID5 array might become inaccessible. This is common to all NSS systems using software RAID implementations.

These are the workarounds:

- Replace the failed drives in the degraded arrays as soon as possible, as failed RAID arrays can result in complete loss of all user data.

- Use the degraded mode management feature to limit the amount of time that a RAID array will run in the degraded state.
- Implement a backup power strategy by using a UPS or RPSU backup power system.

- CSCsw86195

When a RAID0 array failure occurs, an alert (SNMP trap, email or system alert) is not triggered.

When this occurs, the Drive Error LED (on the disk that caused the array failure) does not light up.

There is no workaround.

- CSCsw86202

When rebuilding a RAID1 spare device, the rebuilding does not resume after the NSS reboots. After reboot, the array might be falsely marked as clean and the drive falsely marked as synced. This does not affect the initial rebuild of an array following a RAID creation.

The workaround is to not reboot the NSS during the RAID rebuild.

- CSCsw86224

If power is interrupted when rebuilding a RAID array (RAID1, RAID5 or RAID10), the rebuild does not restart automatically after the system is powered up again.

When this occurs, the array remains in the degraded state and the rebuilt drive is ejected from the array.

The workaround is to manually restart the rebuild by adding the ejected drive back to the array by using the Configuration GUI.

- CSC86417

When the RAID global spares option is enabled in the Configuration GUI, the RAID spares are not shared during the RAID array rebuild.

For example: If RAIDA has a hot spare and RAIDB does not, if RAIDB is degraded while RAIDA is rebuilding, the spare will not transfer to RAIDB until after RAIDA completes the rebuild.

There is no workaround.

- CSCsw86562

When the Default Network Policy filter is set to Drop Traffic, no automatic Allow Filter is created for the default gateway.

When this occurs, all traffic from the default gateway is dropped and all traffic sent from other subnets through a router is not forwarded to the NSS.

The workaround is to manually create an AllowAll Network Access Filter for the default gateway IP address by using the Configuration GUI.

- CSCsw86687

When writing simultaneously to the same file by using NFS and FTP or by using NFS and CIFS, the NSS file locking mechanism does not work properly.

There is no workaround.

- CSCsw86701

When you create a share by using the Initial Setup wizard and enable NFS, users are assigned root privilege access.

The workaround is to not enable NFS in the Initial Setup wizard. If NFS is required, you can enable it at a later time by using the Configuration GUI.

- 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.

- CSCsw86695

If a user was granted write access to a share and the write access was revoked, the user can still write to subfolders by using FTP or NFS.

This problem only occurs under these conditions:

- The user has write privileges to the subfolder (either because the user is the owner, or was granted access by the owner).
- The user has read privileges to the share (by having explicit share read-only access).
- The workaround is to not enable FTP or NFS (which is disabled by default), if these protocols are not being used.

- 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.

Closed Caveats

Resolved in Firmware Version 1.16

- CSCsw86113

When the Network Access Filter is set to Policy=Drop Traffic and Filter=AllowAll or Policy=Drop and Filter=AllowCIFS, the CIFS mount now works.

- CSCsw86116

When the Network Access Filter is set to Filter=AllowHTTPS and Filter=DropFTPS, you can now add Network Access from the Configuration GUI

- CSCsw86481

When a Seagate 1 terabyte (TB) hard drive (model ST31000340AS) is installed in the NSS, it is not detected by the system on bootup or when hotplugging the drive.

There is no workaround. This drive is not compatible with the NSS4000 and NSS6000.

For a current list of compatible disk drives, see the Cisco Approved Vendor List for Network Storage Systems at: http://www.cisco.com/en/US/products/ps9957/prod_technical_reference_list.html

- CSCsw86488

When Seagate hard drives are installed in the NSS, they can take about 30 seconds to be detected on bootup.

There is no workaround. Some drives are not compatible with the NSS4000 and NSS6000.

For a current list of compatible disk drives, see the Cisco Approved Vendor List for Network Storage Systems at: http://www.cisco.com/en/US/products/ps9957/prod_technical_reference_list.html

- CSCsw86593

The maximum transmission unit (MTU) size of the NSS is now supported.

- CSCsw86676

If a user was granted write access to a share and the write access was revoked, the user can no longer write to subfolders by using FTP.

- CSCsw86721

The **Network** ➔ **Identification** page in the Configuration GUI now accepts domain controller hostnames that begin with a digit.

- CSCta87119

When running firmware V1.14.20 on the NSS4000 and NSS6000, you cannot configure a share folder to work with the Symantec BackupExec application.

This problem was fixed in firmware version 1.16.

Resolved in Firmware Version 1.14

- The NSS now supports ADS domains of up to 8,000 objects (domain users and groups) for the NSS4000 and 16,000 objects (domain users and groups) for the NSS6000.
- Microsoft Vista interoperability issues no longer exist.
- Extraneous “Shutdown was not clean” messages no longer appear.

Release Notes

- CIFS idle disconnect is now working for Windows clients.
- Virtualized RAIDs no longer fail to start at bootup.
- System alerts are now generated for all conditions that generate SNMP traps.
- Changes to the system time no longer results in a system slowdown.
- Microsoft Access databases stored on the NSS can now be opened from more than one client at a time.
- Problems no longer exist when using passive mode FTP through a NAT router.
- Users can no longer be created with invalid usernames, prohibiting login.
- Linksys One NMS authentication can no longer be circumvented.
- Security issues no longer exist with the Linksys One window-in-window view, the Configuration GUI input validation, and Samba and Apache servers.
- The Configuration GUI is now accessible at all times.
- Domain joins are now operating properly.
- The network filter default drop policy no longer locks out access to the Configuration GUI if HTTP is running on a non-default port.
- The System Status page in the Configuration GUI no longer shows two connected users when no users are connected.
- FTP write performance is no longer abnormally slow. (only applies to the NSS6000).

Cisco, Cisco Systems, the Cisco logo, and the Cisco Systems logo are registered trademarks or 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. (0705R)

© 2009 Cisco Systems, Inc. All rights reserved.

OL-20074-01