



Software Management Operations

This chapter provides information about software management operations on the system.

- [Understanding the Local File System, on page 1](#)
- [Maintaining the Local File System, on page 2](#)
- [Configuring the Boot Stack, on page 7](#)
- [Upgrading the Operating System Software, on page 11](#)
- [Performing Dynamic Software Updates, on page 35](#)
- [Managing License Keys, on page 36](#)
- [Managing Local-User Administrative Accounts, on page 39](#)

Understanding the Local File System

The Management Input/Output (MIO/UMIO/MIO2) card provides control and management for the system.

The local file system is made up of files that are stored on one or more of the following:

- **/flash** - Flash memory located on the circuit board of the MIO/UMIO/MIO2, is the default storage media for the operating system software image, CLI configuration, and crash log files used by the system.
- **/usb1** - This device is available when a USB memory stick is inserted on the front panel of the active MIO/UMIO/MIO2.
- **/hd-raid** - This is the solid state hard disk array supported by the Fabric and Storage Cards (FSCs) and accessed via the active MIO/UMIO/MIO2.

File Types Used by the Local File System

The following file types can be located in the local file system:

- **Operating System Software Image File:** This binary file type is identified by its **.bin** extension. The file is the operating system that is loaded by the system upon startup or reloading. This is an executable, read-only file that cannot be modified by end users.
- **CLI Configuration File:** This file type is identified by its **.cfg** extension. These are text files that contain CLI commands that work in conjunction with the operating system software image. These files determine services to be provided, hardware and software configurations, and other functions performed by the

system. The files are typically created by the end user. You can modify the files both on and off-line and use descriptive long filenames.

- **System File:** Only one file identified by a `.sys` extension is used by the system. The `boot.sys` file contains system-specific information, which describes how the system locates, and in what priority it loads, file groups (paired `.bin` and `.cfg` files) from its boot stack.
- **Abridged Crash Log:** The abridged crash log, identified by its `crashlog` filename, contains summary information about software or hardware failures that occur on the system. This file is located in the `/flash/crsh2/` directory on the device. You can view the contents of this file through the CLI, but you cannot modify the file.

Understanding the boot.sys File

The system uses the `boot.sys` file to store the prioritized boot stack parameters and file groups the system uses during startup. Modify this file only through system CLI commands and not through external means. Boot parameters contain information the system needs to locate the operating system image file, including:

- **bootmode:** This setting is typically configured to normal, and identifies how the system starts.
- **network interface configuration:** Use these optional boot method settings when you configure the system to obtain its operating system image from an external network server that is using one of the management LAN interfaces on the MIO/UMIO/MIO2 card.
- **boot stack information:** The boot stack is made up of prioritized file group entries that designate the operating system image file and the CLI configuration file to load.

When a system is started for the first time, the `boot.sys` file is configured to use the normal boot mode and load the operating system software image from the `/flash` directory.

There is no CLI configuration file contained on the local file system. This causes the system to automatically start its CLI-based Quick Setup Wizard upon the first successful boot. Refer to *Getting Started* for more information on using the Quick Setup Wizard.

Maintaining the Local File System

Use CLI commands to manage and maintain the devices that make up the local file system. Execute all the commands described in this section in the Exec Mode. Unless otherwise specified, you must have security administrator or administrator privileges to execute these commands.

File System Management Commands

Use the commands in this section to manage and organize the local file system.



Important

For complete information on the commands listed below, see the *Exec Mode Commands* chapter of the *Command Line Interface Reference*.

Synchronizing the File System

Commands are supported for mirroring the local file systems from the active MIO/UMIO/MIO2 to the standby MIO/UMIO/MIO2 in systems containing two cards. Use these commands to synchronize any or all of the local devices.



Important

Crash log files are not synchronized when these commands are executed.

The following Exec mode command synchronizes the file systems between two MIO/UMIO/MIO2s:

```
[local]host_name# filesystem synchronize [ /flash | /usb1 | all ] [ checkonly ] [ from card_num | to card_num ] [ -noconfirm ]
```

Only filesystems on matching local devices are synchronized. For example, if the active MIO/UMIO/MIO2 contains two local devices (/flash and /usb1) and the standby MIO/UMIO/MIO2 contains only one local device (/flash), then synchronization only occurs on the matching local device (/flash).

The following command synchronizes the file systems on two MIO/UMIO/MIO2 flash devices.

```
[local]host_name# filesystem synchronize /flash
```

Creating Directories

Use the **mkdir** command to create a new directory on the specific local device. This directory can then be incorporated as part of the path name for any file located in the local file system.

```
[local]host_name# mkdir { /flash | /usb1 | /hd-raid } /dir_name
```

Use the following command to create a directory named *configs*:

```
[local]host_name# mkdir /flash/configs
```

Renaming Files and Directories

Use the **rename** command to change the name of a file from its original name to a different name. Remember to use the same file extension, if applicable, to ensure that the file type remains unchanged.

```
[local]host_name# rename { /flash | /usb1 | /hd-raid } /src_filename { /flash | /usb1 | /hd-raid } /dst_filename [ -noconfirm ]
```

Use the following command to rename a file named *iot_test.cfg* to *iot_accept.cfg* on the *flash* local device.

```
[local]host_name# rename /flash/iot_test.cfg /flash/iot_accept.cfg -noconfirm
```



Important

Use the **rename** command only within the same local device. You cannot rename a file and place it onto another local device at the same time. To move a renamed file, you must use the **copy** command.

Copying Files

These instructions assume that you are at the root prompt for the Exec mode. To save your current configuration, enter the following command:

```
[local]host_name# copy from_url to_url [-noconfirm]
```

To copy a configuration file called *system.cfg* from a directory that was called *cfgfiles* to a directory named *configs_old*, enter the following command:

```
[local]host_name# copy /flash/cfgfiles/system.cfg
/flash/configs_old/system_2011.cfg
```

To copy a configuration file called *init_config.cfg* to the root directory of a TFTP server with a hostname of *config_server*, enter the following command:

```
[local]host_name# copy /flash/cfgfiles/init_config.cfg
tftp://config_server/init_config.cfg
```

Deleting Files

The **delete** command removes a designated file from its specified location on the local file system.



Important

This command does not support wildcard entries; each filename must be specified in its entirety.



Caution

Do not delete the *boot.sys* file. If deleted, the system will not reboot on command and will be rendered inoperable.

```
[local]host_name# delete { /flash | /usb1 | /hd-raid }/filename [ -noconfirm
]
```

The following command deletes a file named *test.cfg* from the */flash* directory.

```
[local]host_name# delete /flash/test.cfg
```

Removing Directories

The **rmdir** command deletes a current directory on the specific local device. This directory can then be incorporated as part of the path name for any file located in the local file system.



Important

The directory you want to remove (delete) must be empty before executing the **rmdir** command. If the directory is not empty, the CLI displays a "Directory not empty" message and will not execute.

```
[local]host_name# rmdir url /dir_name
```

The following command deletes an empty directory named *configs* in the */flash* directory.

```
[local]host_name# rmdir /flash/configs
```

Formatting Local Devices

The **format** command performs a low-level format of a local device. This operation formats the device to use the FAT16 formatting method, which is required for proper read/write functionality with the operating system.

**Important**

Local devices that have been formatted using other methods such as NTFS or FAT32 may be used to store various operating system, CLI configuration, and crash log files. However, when placing a new local device into the MIO/UMIO/MIO2 for regular use, you should format the device via the system prior to use. This ensures that the proper file allocation table format is used, preventing any possible discrepancies between other formats used with other operating systems.

**Caution**

The **filesystem format** command removes all files and information stored on the device.

To format a local device for use by the local file system, enter the following command:

```
[local]host_name# filesystem format { /flash | /usb1 | /hd-raid }
```

Applying Pre-existing CLI Configuration Files

A pre-existing CLI configuration file is any .cfg file created to provide utility functions (such as clearing all statistics during testing) or created off-line using a text editor. There may be pre-existing configuration files stored on the local file system that can be applied to a running system at any time.

**Caution**

If a configuration file is applied to a system currently running another CLI configuration, any like contexts, services, logical interfaces, physical ports, IP address pools, or other configured items will be overwritten if the same command exists in the configuration file being applied. Take caution to ensure that you are knowledgeable of the contents of the file being applied and understand what the service ramifications are if a currently running command is overwritten. Also note that changes will not be saved automatically.

A CLI configuration file, or script containing CLI commands, can be applied to a running system by entering the following command at the Exec mode prompt:

```
[local]host_name# configure url [ verbose ]
```

url specifies the location of the CLI configuration file to be applied. It may refer to a local or a remote file.

The following command applies a pre-existing CLI configuration file named *clearcmds.cfg* in the */flash* directory.

```
[local]host_name# configure /flash/clearcmds.cfg
```

Viewing Files on the Local File System

This section describes how to view a variety of files.

Viewing the Contents of a Local Device

The contents, usage information, and file system directory structure of any local device can be viewed by entering the following command at the Exec mode prompt:

```
directory { /flash | /usb1 | /hd-raid }
```

Viewing CLI Configuration and boot.sys Files

The contents of CLI configuration and boot.sys files, contained on the local file system, can be viewed off-line (without loading them into the OS) by entering the following command at the Exec mode prompt:

```
[local]host_name# show file url { /flash | /usb1 | /hd-raid } filename
```

Where: *url* is the path name for the location of the file and *filename* is the name of the file, including any extension.



Important

Operator and inspector-level users can execute the **show file** command but cannot execute the **directory** command.

Validating an Operating System File

The operating system software image file, identified by its .bin extension, is a non-readable, non-editable file that executes on the system, creating its runtime operating system (OS).

It is important to verify a new operating system image file before attempting to load it. To accomplish this, a proprietary checksum algorithm is used to create checksum values for each portion of the application stored within the .bin file during program compilation.

This information can be used to validate the actual file against the checksum values stored within the file during its compilation. If any portion of the image file has become corrupted (for example, the file was truncated or was transferred using ASCII mode instead of binary mode), then this information is reported and the file is deemed unusable.

To validate an operating system software image file, enter the following command at the Exec mode prompt:

```
[local]host_name# show version { /flash | /usb1 | /hd-raid } /[directory]/filename
[all]
```

The output of this command displays the following information:

- Version number
- Description
- Date
- Boot Image
- Size
- Flags
- Platform

If an invalid file is found, the system displays a failure message similar to these:

```
Failure: Image /flash/image_version.bin CRC check failed!
Failure: /flash/image_version.bin, has a bad magic number
```

Configuring the Boot Stack

The boot stack consists of a prioritized listing of operating system software image-to-CLI configuration file associations. These associations determine the software image and configuration file that gets loaded during system startup or upon a reload/reboot. Though multiple associations can be configured, the system uses the association with the highest priority. In the event that there is an error processing this association (for example, one of the files cannot be located), the system attempts to use the association with the next highest priority. Priorities range from 1 to 100, with 1 being the highest priority. The maximum number of boot stack entries that may be configured in the `boot.sys` file is 10.

Boot stack information is contained in the `boot.sys` file, described in [Understanding the boot.sys File, on page 2](#). In addition to boot stack entries, the `boot.sys` file contains any configuration commands required to define the system boot method as explained in the section that follows.

System Boot Methods

The local-boot method uses software image and configuration files stored locally on the system. On system startup or reboot, the system looks on one of its local devices or **/hd-raid** for the specific software image and accompanying configuration text file. When using the local-booting method, you only need to configure boot stack parameters.

The system can also be configured to obtain its software image from a specific external network server while it is paired with a configuration text file that resides on the system. When using network booting, you need to configure the following:

- Boot stack parameters, which define the files to use and in what priority to use them
- Boot interface and network parameters defining the remote management LAN interface and the methods to use to reach the external network server
- Network booting delay time and optional name server parameters defining the delay period (in seconds) to allow for network communications to be established, and the IP address of any Domain Name Service (DNS) name server that may be used

Detailed information on how to configure the system to use the network booting method appears in [Network Booting Configuration Requirements, on page 9](#)

Viewing the Current Boot Stack

To view the boot stack entries contained in the `boot.sys` file run the Exec mode **show boot** command.



Important

Operator and inspector-level users can execute the **show boot** command.

The examples below shows the command output for a local booting configuration. Notice that in these examples both the image file (operating system software) and configuration file (CLI commands) are located on the **/flash** device.

**Important**

The StarOS image filename scheme changed with release 16.1. Pre-16.1, format = "production.image.bin". For 16.1 onwards, format = "asr5500-image_number.bin". This change is reflected in the examples provided below.

Example 1 – StarOS releases prior to 16.1:

```
boot system priority 18 \
  image /flash/15-0-builds/production.45666.bin \
  config /flash/general_config.cfg

boot system priority 19 \
  image /flash/15-0-builds/production.45717.bin \
  config /flash/general_config_3819.cfg

boot system priority 20 \
  image /flash/15-0-builds/production.45069.bin \
  config /flash/general_config_3665.cfg
```

Example 2 – StarOS release 16.1 onwards:

```
boot system priority 18 \
  image /flash/16-1-builds/asr5500-16.1.3.bin \
  config /flash/general_config.cfg

boot system priority 19 \
  image /flash/16-1-builds/asr5500-16.1.1.bin \
  config /flash/general_config_3819.cfg

boot system priority 20 \
  image /flash/16-1-builds/asr5500-16.1.0.bin \
  config /flash/general_config_3665.cfg
```

The example below shows the output for a combination network booting and local booting configuration. Notice in this example that the first two boot stack entries (Priorities 18 and 19) load the image file (operating system software) from an external network server using the Trivial File Transfer Protocol (TFTP), while all configuration files are located on the **/flash** device.

Also notice the boot network interface and boot network configuration commands located at the top of the boot stack. These commands define what remote management LAN interface(s) to use and information about communicating with the external network server that hosts the operating system software image file.

```
boot networkconfig static ip address mio1 192.168.1.150 netmask 255.255.255.0
boot delay 15
boot system priority 18 image tftp://192.168.1.161/tftpboot/image_version.bin \config
/flash/general_config.cfg
boot system priority 19 image tftp://192.168.1.161/tftpboot/image_version.bin \config
/flash/general_config.cfg
boot system priority 20 image /flash/image_version.bin \config /flash/general_config.cfg
```

To identify the boot image priority that was loaded at the initial boot time enter:

show boot initial-config

The example below displays the output:

```
[local]host_name# show boot initial-config
Initial (boot time) configuration:
  image tftp://192.168.1.161/tftpboot/image_version.bin \
  config /flash/config_name.cfg
  priority 1
```


Adding a New Boot Stack Entry

**Important**

Before performing this procedure, verify that there are less than 10 entries in the `boot.sys` file and that a higher priority entry is available (i.e. that minimally there is no priority 1 entry in the boot stack). Refer to *Viewing the Current Boot Stack* for more information.

If priority 1 is in use, then you must renumber the existing entry(ies) to ensure that at least that priority is available. The maximum number of boot stack entries that can be contained in the `boot.sys` file is 10. If there are already 10 entries in the boot stack, you must delete at least one of these entries (typically, the lowest priority) and, if necessary, renumber some or all of the other entries before proceeding. Refer to [Deleting a Boot Stack Entry, on page 9](#) for more information.

This procedure details how to add new boot stack entries to the `boot.sys` file. Make sure you are at the Exec mode prompt and enter the following commands:

```
configure
boot system priority number image image_url config cfg_url
```

The following command creates a new boot stack entry, using a boot priority of 3.

```
boot system priority 3 image /flash/image_filename.bin config
/flash/config_name.cfg
```

**Important**

Boot stack changes saved to the `boot.sys` file are not executed until the system is rebooted.

Synchronize the local file systems on the MIO/UMIO/MIO2s with the following command:

```
filesystem synchronize all
```

Deleting a Boot Stack Entry

This procedure details how to remove an individual boot stack entry from the `boot.sys` file. Make sure you are at the Exec mode prompt and enter the following commands:

```
configure
no boot system priority number
```

Where *number* specifies the boot priority used for the boot stack entry. This command removes that specific entry from the boot stack, causing the `boot.sys` file to be overwritten.

Network Booting Configuration Requirements

Configuring the Boot Interface

Boot interface parameters define the MIO/UMIO/MIO2 management LAN interface that the system will use to communicate with the management network when using the network booting method.

This procedure details how to configure the boot interface for reliable communications with your network server. Make sure you are at the Exec mode prompt.

Step 1 Enter the Global Configuration mode by entering the following command:

```
[local]host_name# configure
```

The following prompt appears:

```
[local]host_name(config)#
```

Step 2 Enter the following command:

```
[local]host_name(config)#boot interface { local-eth1 | local-eth2 } medium { auto |
speed { 10 | 100 | 1000 } duplex { full | half } } media { rj45 | sfp }
```

For complete information about the above command, see the *Global Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Use port 1 for network booting.

If the speed is manually configured, you must also configure the duplex mode. In addition, you must ensure that the network server configuration supports the speed and duplex configuration.

Network speed for MIO/UMIO/MIO2 is fixed at **1000**.

Ethernet networking rules dictate that if a device's interface is configured for auto-negotiation is communicating with a device that is manually configured to support full duplex, the first device will negotiate to the manually configured speed of the second device, but will only communicate in half duplex mode.

The media for MIO/UMIO/MIO2 port 1 is fixed at **rj45**.

Step 3 Save the configuration as described in the *Verifying and Saving Your Configuration* chapter.

Configuring the Boot Network

Boot network parameters define the protocols and IP address information for MIO/UMIO/MIO2 interfaces used to reach the external network server that hosts the operating system software image file. To configure boot network parameters, make sure you are at the Exec mode prompt.

Step 1 Enter the Global Configuration mode by entering the following command:

```
[local]host_name(config)#configure
```

The following prompt appears:

```
[local]host_name(config)#
```

Step 2 Enter the following command:

```
[local]host_name(config)# boot networkconfig { dhcp | { { dhcp-static-fallback | static
} ip address mio5 ip_address5 [ mio6 ip_address6 ] netmask subnet_mask [ gateway
gw_ip_address ] } }
```

For complete information about the above command, see the *Global Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

The following command configures the boot network to communicate using DHCP, with a static-fallback IP address for MIO/UMIO/MIO2 in slot 5 of 192.168.206.101 and a Class C netmask.

```
[local]host_name(config)# boot networkconfig dhcp-static-fallback ip address mio5  
192.168.206.101 netmask 255.255.255.0
```

The next example uses static IP addresses for MIO/UMIO/MIO2 in slot 5, which can access the external network server through a gateway whose IP address is 135.212.10.2.

```
[local]host_name(config)# boot networkconfig static ip address mio5 192.168.206.101  
netmask 255.255.255.0 gateway 135.212.10.2
```

Step 3 Save the configuration as described in the *Verifying and Saving Your Configuration* chapter.

Configuring Boot Network Delay Time

An optional delay period, in seconds, can be configured for systems booting from a network. The purpose of this parameter is to allow time for external devices, such as switches, that use the Spanning Tree Protocol (STP) to determine the network route to a specified IP address.

To configure a boot network delay, enter the following command from the Global Configuration mode prompt.

```
[local]host_name(config)# boot delay time
```

Where *time* is an integer from 1 to 300 seconds before attempting to contact the external network server. If your network uses STP, a typical delay time of 30 seconds should suffice.



Important Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Configuring a Boot Nameserver

To configure a boot nameserver address, enter the following command from the Global Configuration mode prompt.

```
[local]host_name(config)# boot nameserver ip_address
```

Where *ip_address* is the IP address of the DNS server entered in IPv4 dotted-decimal notation.



Important Save the configuration as described in the *Verifying and Saving Your Configuration* chapter.

Upgrading the Operating System Software

This section describes how to manually perform the StarOS binary image upgrade procedure.

Prior to initiating the StarOS software upgrade procedure, make sure the conditions described in the [Prerequisites](#), on page 12 section are met.



Caution Undeploying/redeploying VPC is not supported after the bin upgrade. Deactivating VPC removes the upgraded StarOS bin image.

To upgrade the StarOS software manually:

1. [Obtain VIP Addresses for AutoVNF, CF, ESC and UEM, on page 12](#)
2. [Identify OS Release Version and Build Number, on page 14](#)
3. [Download the Software Image from the Support Site, on page 15](#)
4. [Verify Zookeeper Database, on page 15](#)
5. [Verify ESC Database, on page 16](#)
6. [Verify Free Space on the /flash Device, on page 17](#)
7. [Transfer StarOS Image to /flash, on page 17](#)
8. [Save the Running Configuration, on page 22](#)
9. [Synchronize File Systems, on page 30](#)
10. [Reboot the System, on page 24](#)

Prerequisites

Prior to performing an upgrade of StarOS software containing CF and SF VNFCs, check if the following prerequisites are met:

- You'll need the login credentials and IP address of AutoDeploy, AutoVNF, ESC, UEM, and CF VMs. You should have administrative rights to the OpenStack setup.
- Verify the OpenStack status. The Ansible output should all pass.

```
cd /home/stack/
source stackrc
cd /home/stack/ansible/
ansible-playbook -i inventory openstack_verify.yml
```

- Check if the health of AutoVNF/ESC/EM/VNF VM is normal through the UltraM health logs on AutoIT. If any of the VM(s) are not normal, then take necessary actions to recover the health of the corresponding VM(s).
- You should have the new StarOS binary image file (for manual upgrade).
- Ensure that there are no pending transactions between ESC, UEM and CF.
- Be sure to take a backup of the original StarOS bin file.

Obtain VIP Addresses for AutoVNF, CF, ESC and UEM

This section provides instructions that are applicable only to the upgrade of CF and SF VNFCs.

To collect the VIP addresses for AutoVNF, CF, ESC and UEM VMs:

1. Log on to the AutoDeploy VM as the default user, *ubuntu*.


```
ssh ubuntu@<ad_vm_address>
```
2. Switch to the *root* user.

```
sudo -i
```

3. Enter the ConfD CLI.

```
confd_cli -u admin -C
```

4. Enter the *admin* user credentials when prompted.

5. Collect the VIP address of AutoVNF, ESC, UEM and CF VMs.

```
show vnfr
```

Example output:

```
vnfr autoit-f-autovnf
vnfd      f-autovnf
vnf-type  usp-uas
state     deployed
external-connection-point avf
virtual-link-ref  management
ip-address      192.168.100.26
floating-ip-address 10.225.202.94

vnfr sj-autovnf-esc
vnfd      esc
vnf-type  esc
state     deployed
external-connection-point esc
virtual-link-ref  management
ip-address      192.168.100.22

vnfr sj-autovnf-vpc
vnfd      vpc
vnf-type  ugp
state     alive
external-connection-point cf
virtual-link-ref  management
ip-address      192.168.100.38
external-connection-point em
virtual-link-ref  management
```

```
ip-address      192.168.100.21
```

Identify OS Release Version and Build Number

The operating system can be configured to provide services and perform pre-defined functions through commands issued from the CLI.

The operating system software is delivered as a single binary file (**.bin** file extension) and is loaded as a single instance for the entire system.

- For StarOS releases prior to 16.1, the image filename is identified by its release type, build number and platform type. For example: **production.build_number.asr5500.bin**. For example, **production.54029.asr5500.bin**.
- For StarOS release 16.1 onwards, the image filename is identified by a suffix specifying its platform type and release number. For example, **asr5500-release_number. bin**. For example, **asr5500-16.1.0.bin**.

For StarOS releases 20.0 and higher, a starfile image must be signed with an REL key before being released. A deployable image will be signed with an REL key having a ".bin.SPA" extension, where "A" identifies the revision level of the signing key. For example, **asr5500-20.0.0.bin.SPA**. If a signing key becomes compromised, a new key is created and the revision level increments to "B".

For StarOS releases 20.0 and higher Trusted images have been introduced. The difference between a Trusted build and a Normal build is the absence of unsecure programs ftpd, telnet and tcpdump, as well as the addition of a staros.conf file for security options. Trusted images are identifiable by the presence of "_T" in the platform name. For example, **asr5500_T-20.0.0.bin.SPA**.

To identify the StarOS software version and build information:

1. Log on to the VNF to be upgraded.
2. Enter the following Exec mode command in the StarOS command line interface:

```
show version
```

Example output:

```
Active Software:
```

```
Image Version:          21.9.0.69918
Image Build Number:    69918
Image Description:     Deployment_Build
Image Date:            Sun Jul 22 12:08:55 EDT 2018
Boot Image:           /flash/staros.bin
Source Commit ID:     94797337b6c1691541ea0dd86f2f29b0f2c3630c
```

3. Execute the following Exec mode command to display additional information about the StarOS build release.

```
show build
```

Download the Software Image from the Support Site

This section provides instructions that are applicable only to the upgrade of CF and SF VNFs.

Access to the Cisco support site and download facility is username and password controlled. You must have an active customer account to access the site and download the StarOS image.

Download the software image to a network location or physical device (USB stick) from which it can be uploaded to the *flash* device. Contact your Cisco representative or Cisco TAC for additional information.

For UGP-based VNF, perform the following steps to download the new bin file to AutoVNF or OSPD VM.

1. Log on to the AutoVNF of the corresponding VNF.

```
ssh ubuntu@<ad_vm_address>
```

Command example:

```
ssh ubuntu@10.225.202.94
```

2. Create a directory to download the new StarOS qvpc-di binary file to AutoVNF/OSPD.

```
cd /home/ubuntu/
```

```
mkdir StarOSBinUpgrade
```

3. Download the new StarOS qvpc-di binary file from the Cisco support site and copy the file to the *StarOSBinUpgrade* directory.

```
cd StarOSBinUpgrade
```

Then, use the following command to verify if the directory contains the new bin file.

```
ls -lrt /home/ubuntu/StarOSBinUpgrade
```

Example output:

```
total 172560
```

```
-r--r--r-- 1 ubuntu ubuntu 176698880 Jul 24 23:29 qvpc-di-21.9.0.69932.bin
```

Verify Zookeeper Database

This section provides instructions that are applicable only to the upgrade of CF and SF VNFs.

To verify the zookeeper database:

1. Log on to the AutoVNF using the floating IP.

```
ssh ubuntu@<ad_vm_address>
```

Command example:

```
ssh ubuntu@10.225.202.94
```

2. Log on to the UEM VM using the VIP address fetched in the [Obtain VIP Addresses for AutoVNF, CF, ESC and UEM, on page 12](#).

```
ssh ubuntu@<vip-addr>
```

Command example:

```
ssh ubuntu@192.168.100.21
```

3. Become the *root* user.

```
sudo -i
```

4. Collect the UEM orchestration IP address for Zookeeper database connection.

```
#ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr fa:16:3e:71:1d:08
          inet addr:192.168.200.12  Bcast:192.168.200.255  Mask:255.255.255.0
```

5. Navigate to the `/opt/cisco/usp/packages/zookeeper/<current>/bin` directory.

6. Execute the following script from the command line to access the UEM Zookeeper database.

```
zkCli.sh -server ip_addr:port_num
```

For example:

```
zkCli.sh -server 192.168.200.12:2181
```

7. Check the zookeeper database and ensure that there are no pending requests between UEM and CF VMs.

```
ls /request
```

Example output:

```
[]
```

```
<Ctrl+D to exit Zookeeper shell>
```

Verify ESC Database

This section provides instructions that are applicable only to the upgrade of CF and SF VNFs.

To verify the ESC database:

1. Log on to the AutoVNF using the floating IP.

```
ssh ubuntu@<ad_vm_address>
```

Command example:

```
ssh ubuntu@10.225.202.94
```

2. Log on to the ESC VM using the VIP address fetched in the [Obtain VIP Addresses for AutoVNF, CF, ESC and UEM, on page 12](#).

```
ssh admin@<vip-addr>
```

Command example:

```
ssh admin@192.168.100.22
```

3. Check the ESC database to ensure there are no pending transactions.

```
sudo /opt/cisco/esc/pgsql/bin/psql -U esc -p 7878 -h localhost -c
'select * from esc_schema.workitem';
```

```
config_id | request_id | mo_type | config_action | config_state
```




Important Whenever transferring an operating system software image file using the file transfer protocol (FTP), the FTP client must be configured to transfer the file using binary mode. Failure to use binary transfer mode will make the transferred operating system image file unusable. In release 20.0 and higher Trusted StarOS builds, FTP is not supported.

- Transfer the file to the */flash* device using an SFTP client with access to the system.

For UGP-based VNF, copy the new StarOS bin to the active CF by following these steps.

1. Log on to the AutoVNF or OSPD VM where the new bin file is downloaded.

```
ssh ubuntu@<ad_vm_address>
```

Command example:

```
ssh ubuntu@10.225.202.94
```

2. Navigate to the directory where the new bin file is downloaded from the Cisco support site.

```
cd /home/ubuntu/StarOSBinUpgrade/ && ls -lrt
```

Example output:

```
total 172560
```

```
-r--r--r-- 1 ubuntu ubuntu 176698880 Jul 24 23:29 qvpc-di-21.9.0.69932.bin
```

3. SFTP to the CF VM.

For example:

```
sftp ubuntu@192.168.100.38
```

4. Navigate to the *sftp* directory.

```
#sftp>pwd
```

```
Remote working directory: /
```

```
#sftp>ls
```

```
hd-raid sftp
```

```
#sftp>cd sftp
```

5. Upload the new binary file to the *sftp* directory.

```
#sftp>put image_filename.bin
```

Example output:

```
#sftp>put qvpc-di-21.9.0.69932.bin
```

```
Uploading qvpc-di-21.9.0.69932.bin to /.auto/onboard/flash/sftp/qvpc-di-21.9.0.69932.bin
qvpc-di-21.9.0.69932.bin 100% 169MB 168.5MB/s 00:01
```

6. Log on to the CF VM using the VIP address fetched in the [Obtain VIP Addresses for AutoVNF, CF, ESC and UEM, on page 12](#).

```
ssh ubuntu@<vip-addr>
```

Command example:

```
ssh ubuntu@192.168.100.38
```

7. Copy the new bin from *sftp* to *flash* directory.

```
copy /flash/sftp/image_filename.bin /flash/updated.bin
```

Example output:

```
#copy /flash/sftp/qvpc-di-21.9.0.69932.bin /flash/updated.bin
```

```
*****
```

```
Transferred 176698880 bytes in 2.718 seconds (63486.9 KB/sec)
```

8. Delete the new bin from *sftp* directory.

```
delete /flash/sftp/image_filename.bin
```

Example output:

```
delete /flash/sftp/qvpc-di-21.9.0.69932.bin
```

```
Are you sure? [Yes|No]: yes
```

```
File /flash/sftp/qvpc-di-21.9.0.69932.bin removed
```

9. Verify that the image file was successfully transferred to the *flash* device by running the following Exec mode command:

```
[local]host_name# directory /flash
```

The image filename should appear in the displayed output.

10. Execute the following command to verify the build information.

```
show version /flash/image_filename.bin
```

Saving a Copy of the Current Configuration File

Prior to upgrading to a new software release, you should copy and rename the current configuration file to the *flash* device and to an off-chassis location (external memory device or network URL). This renamed copy assures that you will have a fallback, loadable configuration file should a problem be encountered during the upgrade.

Downgrading from Release 15.0 to 14.0

Release 14 and Release 15 chassis IDs use different encryption formats. Release 15 will recognize a Release 14 chassis ID and consider it as valid. Upgrading from 14.x to 15.0 will not require changing the chassis ID or configuration file.

However, if the chassis key is reset in Release 15 through the setup wizard or **chassis-key** CLI command, a new chassis ID will be generated in Release 15 format (44 instead of 16 characters). Release 14 builds will not recognize the 44-character chassis ID. If the chassis is subsequently downgraded to Release 14, a new 16-character chassis ID will be generated. To accommodate the old key format, you must save the configuration file in pre-v12.2 format before the downgrade. If you attempt to load a v15 configuration file on the downgraded chassis, StarOS will not be able to decrypt the password/secrets stored in the configuration file.

Downgrading from Release 20.0

Prior to release 20.0, local-user passwords were hashed with the MD5 message digest-algorithm and saved in the database. In release 20.0, PBKDF2 (Password Based Key Derivation Function - Version 2) is now used to derive a key of given length, based on entered data, salt and number of iterations. Local-user account passwords are hashed using the PBKDF2 method with a randomly generated salt coupled with a large number of iterations to make password storage more secure.

Since hash functions are one-way, it is not possible to convert PBKDF2 hashed passwords to the MD5 format. The local-user database must be downgraded prior to reverting to StarOS releases prior to 20.0.

To downgrade the local-user database to use the MD5 hash algorithm, a Security Administrator must run the Exec mode **downgrade local-user database** command. StarOS prompts for confirmation and requests the Security Administrator to reenter a password. The entered password re-authenticates the user prior to executing the downgrade command. After verification, the password is hashed using the appropriate old/weak encryption algorithm and saved in the database to allow earlier versions of StarOS to authenticate the Security Administrator.

The downgrade process does not convert PBKDF2 hashed passwords to MD5 format. The downgrade process re-reads the database (from the /flash directory), reconstructs the database in the older format, and writes it back to the disk. Since the PBKDF2 hashed passwords cannot be converted to the MD5 hash algorithm, and earlier StarOS releases cannot parse the PBKDF2 encryption algorithm, StarOS suspends all those users encrypted via the PBKDF2 algorithm. Users encrypted via the MD5 algorithm ("Weak Hash" flag) can continue to login with their credentials. After the system comes up with the earlier StarOS release, suspended users can be identified in the output of the **show local-user [verbose]** command.

To reactivate suspended users a Security Administrator can:

- Set temporary passwords for suspended users, using the Exec mode **password change local-user *username*** command.
- Reset the suspend flag for users, using the Configuration mode **no suspend local-user *username*** command.

Off-line Software Upgrade

An off-line software upgrade can be performed for any system, upgrading from any version of operating system software to any version, regardless of version number. This process is considered off-line because while many of the steps can be performed while the system is currently supporting sessions, the last step of this process requires a reboot to actually apply the software upgrade.

This procedure assumes that you have a CLI session established and are placing the new operating system image file onto the local file system. To begin, make sure you are at the Exec mode prompt:

```
[local]host_name#
```

To perform offline software upgrade:

1. [Configure a Newcall Policy, on page 21](#)
2. [Configure a Message of the Day Banner, on page 21](#)
3. [Back up the Current CLI Configuration File , on page 21](#)
4. [Save the Running Configuration, on page 22](#)
5. [Create a New Boot Stack Entry, on page 23](#)

6. [Synchronize File Systems, on page 30](#)
7. [Reboot the System, on page 24](#)

Configure a Newcall Policy

Configure a newcall policy from the Exec mode to meet your service requirements. When enabled the policy redirects or rejects new calls in anticipation of the system reload that completes the upgrade process. This reduces the amount of service disruption to subscribers caused by the system reload that completes the upgrade.



Important

Newcall policies are created on a per-service basis. If you have multiple services running on the chassis, you can configure multiple newcall policies.

The syntax for newcall policies is described below:

```
[local]host_name# newcall policy { asngw-service | asnpc-service | sgsn-service
} { all | name service_name } reject
[local]host_name# newcall policy { fa-service | lns-service | mipv6ha-service
} { all | name service_name } reject
[local]host_name# newcall policy { ha-service | pdsn-service |
pdsnclosedrp-service } { all | name service_name } { redirect target_ip_address
[ weight weight_num ] [ target_ipaddress2 [ weight weight_num ] ...
target_ip_address16 [ weight weight_num ] | reject }
[local]host_name# newcall policy ggsn-service { apn name apn_name | all | name
service_name } reject
[local]host_name# newcall policy hnbgw-service { all | name service_name } reject
[local]host_name# newcall policy { pcc-af-service | pcc-policy-service } {
all | name service_name } reject
[local]host_name# newcall policy {pcc-af-service | pcc-policy-service } { all
| name service_name } reject
[local]host_name# newcall policy mme-service { all | name service_name } reject
```

For complete information about the above commands, see the *Exec Mode Commands* chapter of the *Command Line Interface Reference*.

Configure a Message of the Day Banner

Optional: Configure a "Message of the Day" banner informing other management users that the system will be rebooted by entering the following command from the Global Configuration mode prompt.

```
[local]host_name(config)# banner motd "banner_text"
```

banner_text is the message that you would like to be displayed and can be up to 2048 alphanumeric characters. Note that *banner_text* must begin with and end in quotation marks (" "). For more information in entering CLI banner information, see the *CLI Reference*. The banner is displayed when an administrative user logs onto the CLI.

Back up the Current CLI Configuration File

Back up the current CLI configuration file by entering the following command:

```
[local]host_name# copy from_url to_url [ -noconfirm ]
```

This creates a mirror-image of the CLI configuration file linked to the operating system defined in the current boot stack entry.

The following command example creates a backup copy of a file called *general.cfg* located on the */flash* device to a file called *general_3652.cfg*:

```
[local]host_name# copy /flash/general.cfg /flash/general_3652.cfg
```

Save the Running Configuration

Save the currently running, upgraded configuration prior to rebooting the chassis.

To save the boot configuration:

1. Log on to the VNF using the previously fetched VIP address in the [Obtain VIP Addresses for AutoVNF, CF, ESC and UEM, on page 12](#).

```
ssh ubuntu@<vip-addr>
```

Command example:

```
ssh ubuntu@192.168.100.38
```

2. *Optional.* Execute the following command in the Exec mode.

```
chassis key value 1234
```

Save config before reload chassis, EVEN IF the same old key value is used. Old config scripts will become invalid after reload.



Important

This step is optional, and needed only if the chassis key is not set.

3. Save the boot configuration in the flash directory.

```
save configuration /flash/system.cfg
```

```
Warning: About to overwrite boot configuration file
Are you sure? [Yes|No]: yes
```

This will update the boot configuration to use the new bin image.

Use the following command to check the boot configuration.

```
# show boot
```

```
Monday May 21 20:39:57 UTC 2018
```

```
boot system priority 8 \
  image /flash/sftp/production.YYYY.qvpc-di.bin \
  config /flash/sftp/tb5_vnf1_dayN.cfg
```

```
boot system priority 9 \
  image /flash/staros.bin \
  config /flash/sftp/tb5_vnf1_dayN.cfg
```

```
boot system priority 10 \
  image /flash/staros.bin \
  config /flash/system.cfg
```

4. Enter the configuration mode to change the boot priority of new StarOS bin file.

```
#config
#boot system priority 1 image /flash/updated.bin config
/flash/system.cfg
#end
```

5. Verify the new boot priority.

```
#show boot
```

```
boot system priority 1 \
    image /flash/updated.bin \
    config /flash/system.cfg
boot system priority 10 \
    image /flash/staros.bin \
    config /flash/system.cfg
```

6. Verify whether the flash directory contains the boot configuration and new bin.

```
dir /flash
```

```
total 320376
-rw-rw-r-- 1 root root 134 May 3 10:11 boot.sys
-rw-rw-r-- 1 root root 3920672 May 11 19:49 crashlog2
drwxrwxr-x 2 root root 4096 May 11 19:49 crsh2
-rw-rw-r-- 1 root root 156 May 11 19:49 module.sys
drwxrwxr-x 3 root root 4096 May 11 19:49 patch
drwxrwxr-x 2 root root 4096 May 11 19:49 persistdump
-rw-rw-r-- 1 root root 79 May 11 19:49 restart_file_cntr.txt
drwxrwxr-x 3 root root 4096 May 11 20:07 sftp
-rw-rw-r-- 1 root root 160871936 May 3 10:11 staros.bin
-rw-rw-r-- 1 root root 5199 May 11 19:57 system.cfg
-rw-rw-r-- 1 root root 163227136 May 11 20:07 updated.bin
320476 /flash
Filesystem 1K-blocks Used Available Use% Mounted on
/var/run/storage/boot1/part2
4112620 320476 3792144 8% /mnt/user/.auto/onboard/flash
```

Create a New Boot Stack Entry

Create a new boot stack entry for the new file group, consisting of the new operating system image file and the currently used CLI configuration file by entering the following Global Configuration command:

```
[local]host_name(config)# boot system priority number image image_url /flash filename
config cfg_url /flash/filename
```

Assign the next highest priority to this entry, by using the <N-1> method, wherein you assign a priority number that is one number less than your current highest priority.



Important

Run the Exec mode **show boot** command to verify that there are less than 10 entries in the boot.sys file and that a higher priority entry is available (minimally there is no priority 1 entry in the boot stack).

If priority 1 is in use, you must renumber the existing entries to ensure that at least that priority is available.

The maximum number of boot stack entries that can be contained in the `boot.sys` file is 10. If there are already 10 entries in the boot stack, you must delete at least one of these entries (typically, the lowest priority) and, if necessary, renumber some or all of the other entries before proceeding. Use the `no boot system priority` command to delete a boot stack entry.

```
[local]host_name# configure
[local]host_name(config)# no boot system priority number
```

To add new boot stack entries to the `boot.sys` file enter the following commands:

```
[local]host_name# configure
[local]host_name(config)# boot system priority number image image_url config cfg_url
```

For information on using the `boot system priority` command, refer to the [Adding a New Boot Stack Entry, on page 9](#).

Synchronize File Systems

Synchronize the local file systems on the management cards by entering the following command:

```
[local]host_name# filesystem synchronize all
```

Reboot the System

To reboot the system (VNF):

1. Log on to the VNF using the previously fetched VIP address in the [Obtain VIP Addresses for AutoVNF, CF, ESC and UEM, on page 12](#).

```
ssh ubuntu@<vip-addr>
```

Command example:

```
ssh ubuntu@192.168.100.38
```

2. Enter the following Exec mode command:

```
[local]host_name# reload [-noconfirm]
```

As the system reboots, it loads the new operating system software image and its corresponding CLI configuration file using the new boot stack entry configured earlier.

3. *Optional for PDSN:* If you are using the IP Pool Sharing Protocol during your upgrade, refer to *Configuring IPSP Before the Software Upgrade* in the *PDSN Administration Guide*.
4. After the reload is complete, log on to the VNF and make sure it is loaded with the intended StarOS version and all the cards have booted up and are in active or stand-by state as expected.

```
show version
```

Example output:

```
Active Software:
  Image Version:          21.9.0.69977
  Image Build Number:    69977
  Image Description:      Build
  Image Date:             Mon Jul 30 06:48:34 EDT 2018
  Boot Image:             /flash/updated.bin
  Source Commit ID:      abde005a31c93734c89444b8aec2b6bb2d2e794d
```

```
show card table
```


Example output:

Slot	Card Type	Oper State	SPOF	Attach
1: CFC	Control Function Virtual Card	Active	No	
2: CFC	Control Function Virtual Card	Standby	-	
3: FC	4-Port Service Function Virtual Card	Standby	-	
4: FC	4-Port Service Function Virtual Card	Standby	-	
5: FC	4-Port Service Function Virtual Card	Standby	-	
6: FC	4-Port Service Function Virtual Card	Standby	-	
7: FC	4-Port Service Function Virtual Card	Standby	-	
8: FC	4-Port Service Function Virtual Card	Standby	-	
9: FC	4-Port Service Function Virtual Card	Standby	-	
10: FC	4-Port Service Function Virtual Card	Standby	-	

- Run the following Exec mode command to display additional information about the running StarOS build release.

```
show build
```

- Optional.* Verify the operational state of CF and SF VNFCs.



Note This step is relevant only for the upgrade of CF and SF VNFCs.

- Repeat the steps in [Verify Zookeeper Database, on page 15](#) and [Verify ESC Database, on page 16](#) sections.

- Log on to the UEM using either the floating IP or from the AutoVNF using the UEM VIP.

```
ssh ubuntu@<vip-addr>
```

Command example:

```
ssh ubuntu@192.168.100.21
```

- Become the *root* user.

```
sudo -i
```

- Collect the UEM orchestration IP address for Zookeeper database connection.

```
#ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr fa:16:3e:71:1d:08
```

```
          inet addr:192.168.200.12  Bcast:192.168.200.255  Mask:255.255.255.0
```

- Navigate to the `/opt/cisco/usp/packages/zookeeper/<current>/bin` directory.

- Run Zookeeper tool to access the UEM Zookeeper database.

```
zkCli.sh -server <vip-addr>:port_num
```

Command example:

```
zkCli.sh -server 192.168.200.12:2181
```

Make sure there are no outstanding requests between UEM and CF.

- Verify the “state”: “alive” for each of the CFs and SFs using the following commands:

```
get /oper/vnfs/vnf_name/vdus/vdu_name/cf1
get /oper/vnfs/vnf_name/vdus/vdu_name/cf2
get /oper/vnfs/vnf_name/vdus/vdu_name/sf1
get /oper/vnfs/vnf_name/vdus/vdu_name/sf2
```

Command examples:

```
get /oper/vnfs/tb1-autovnf1_vpc-vpc-core/vdus/vdu-cf1/cf1
get /oper/vnfs/tb1-autovnf1_vpc-vpc-core/vdus/vdu-cf1/cf2
get /oper/vnfs/tb1-autovnf1_vpc-vpc-core/vdus/vdu-sf1/sf1
get /oper/vnfs/tb1-autovnf1_vpc-vpc-core/vdus/vdu-sf1/sf2
```

- h. Look for the state Alive in the console output.

```
zk: localhost:2181(CONNECTED) 2] get
/oper/vdus/control-function/BOOT_generic_di-chassis_CF1_1
{"id":"BOOT_generic_di-chassis_CF1_1","state":"alive","vnfcId":"cf-vnfc-di-chassis","uuid":"c4",
"host":"tb5-ultram-osd-compute-2.localdomain","vimId":"523b921c-7266-4fd5-90bb-5157cffc6951",
"cppts":[{"cpid":"di_intf1","state":"alive","subnet":"6102e9b5-8555-41f5-8cdc-0b47d30a6f7a",
"netmask":"255.255.255.0","dhcp":true,"vl":"vl-vnf1-DI-INTERNAL1-CAT","vnfc":"cf-vnfc-di-chassis",
"port_id":"19539aea-edbf-4acf-a57c-af5627d859ea","ip_address":"192.168.10.3",
"mac_address":"fa:16:3e:19:80:ed","network":"0d72f553-5a9c-4904-b3ea-83371a806e23"},
{"cpid":"di_intf2","state":"alive","nicid":1,"subnet":"30002d02-761d-4ccb-8a9e-d6188cdf54a3",
"netmask":"255.255.255.0","dhcp":true,"vl":"vl-vnf1-DI-INTERNAL2-CAT","vnfc":"cf-vnfc-di-chassis",
"port_id":"ff1dale1-ecf3-477d-98b7-398c3c77fc8d","ip_address":"192.168.11.13",
"mac_address":"fa:16:3e:89:88:23","network":"9f109c0a-b1e7-4d90-a746-5de4ab8ef536"},
{"cpid":"orch","state":"alive","nicid":2,"subnet":"729e9dd2-3c75-43eb-988a-769016f2f44c",
"netmask":"255.255.255.0","dhcp":true,"vl":"vl-vnf1-UAS-ORCH-CAT","vnfc":"cf-vnfc-di-chassis",
"port_id":"81370948-f686-4812-820c-20ec5d3d3cdd","ip_address":"172.168.11.17","mac_address":"fa:16:3e:1d:0b:56",
"network":"9a286170-e393-4ba5-abce-147a45fb337a"}, {"cpid":"mgmt","state":"alive","nicid":3,
"subnet":"9778a11b-1714-4e84-4bc2-86c84b111e8e","netmask":"255.255.255.0","dhcp":true,"vl":"vl-vnf1-UAS-MGMT-CAT",
"vnfc":"cf-vnfc-di-chassis","port_id":"6130cbb4-3dd8-4822-af90-50dac98f2f0d",
"ip_address":"172.168.10.17","mac_address":"fa:16:3e:42:92:47","network":"e278b524-e9a9-48c1-a45b-956a8c3ea583"}],
"monitor":true,"vduId":"control-function"}
cZxid = 0x100000051
ctime = Fri May 18 19:04:40 UTC 2018
mZxid = 0x10000024a
mtime = Mon May 21 17:48:19 UTC 2018
pZxid = 0x100000051
cversion = 0
dataVersion = 12
aclVersion = 0
ephemeralOwner = 0x0
dataLength = 1625
numChildren = 0
```



Note You can use **CTRL+D** to exit the zookeeper CLI.

- i. From the UEM VM as a root user, log on to the `ncs_cli` and check for devices live status.

```
~$ sudo -i
ncs_cli -C -u admin
# show devices device device_name live-status
```

Verify that the command output reflects the correct 'state' and 'card-state' of each card.

Example output:

```
# show devices device tb1-autovnf1_vpc-vpc-core-cf-nc live-status
```

```
<snip>
```

VNFC REF	STATE	VNFC ID	VDU REF	CARD TYPE	CARD ID	NUMBER OF CORES	CPU UTILIZATION	DISK SPACE	START TIME	UPTIME	NOVA LAUNCH CMD	ID	DATE AND TIME	FROM STATE	TO STATE
----------	-------	---------	---------	-----------	---------	-----------------	-----------------	------------	------------	--------	-----------------	----	---------------	------------	----------

cf1	-	cf1	cf	cf1	1	-	-	-	-	-	-				
-----	---	-----	----	-----	---	---	---	---	---	---	---	--	--	--	--

cf2	-	cf2	cf	cf2	2	-	-	-	-	-	-				
-----	---	-----	----	-----	---	---	---	---	---	---	---	--	--	--	--

sf1	-	sf1	sf	sf1	3	-	-	-	-	-	-				
-----	---	-----	----	-----	---	---	---	---	---	---	---	--	--	--	--

sf2	-	sf2	sf	sf2	4	-	-	-	-	-	-				
-----	---	-----	----	-----	---	---	---	---	---	---	---	--	--	--	--

```
live-status vnfd sj-autovnf-vpc-abc
```

```
version 6.0
```

```
vnfm vim-tenant-name abc
```

```
vnfm tenant-name abc
```

```
vnfm ipaddr 192.168.100.22
```

```
vnfm port 830
```

```
vnfm username ubuntu
```

```
vnfm password "$4$+HLzhFFzHq66nqtTsc00CfiODYHq1USVmkn1tRelf84byNakWEa9sJ8sY/cwfFME3aG0UaBC\nvvNNAMkuXQI9Ksfu5IiQQ9ViWbbHw16IEFQ="
```

```
virtual-link vl-di-internal1
```

```
auto-vnf-connection-ref di-internal1
```

```
virtual-link vl-management
```

```
auto-vnf-connection-ref management
```

```
virtual-link vl-orchestration
```

```
auto-vnf-connection-ref orchestration
```

```
virtual-link vl-abc-vpc-svc
```

```
auto-vnf-connection-ref sj-autovnf-abc-vpc-svc
```

```
vdu cf
```

```
ssh-keygen false
```

```
vm-image 076c887a-a12c-4a0b-b4d6-b2d213f64b9e
```

```
lifecycle-event-initialization staros_config.txt
```

```
source-url http://192.168.100.9:5000/config/sj-autovnf-vpc-abc/cf/staros_config.txt
```

```

lifecycle-event-initialization staros_param.cfg

source-url http://192.168.100.9:5000/config/sj-autovnf-vpc-abc/cf/staros_param.cfg

ned cisco-staros-nc

user "$4$+HLzsE1kLJOeufWY0smBWY2LHjOi2WtJdKy/OIux7YHhsNY/
08hnA9/WwWuFD5trHrW3ZHs\nLo4TfiAKqYwxdNKqFYyoTxH2hrLJV5DgwmE="

password "$4$+HLzsXtCHJ2vsYZD5s0RGtBRY/dHDU1mgHJX7wCt3o1DMtQZqpBLDcNSJumC7n5rnkVxwI1s\
ncJYeCOFLrqpLHXm3xtXyMdtT7WVzvRMtdao="

netconf

port-number 830

card-type control-function

usp-auto-vnf-id sj-autovnf-vpc-abc-cf

vnfc cf-vnfc-ugp

<snip>

```

Save the Running Configuration

Save the currently running, upgraded configuration prior to rebooting the chassis.

To save the boot configuration:

1. Log on to the VNF using the previously fetched VIP address in the [Obtain VIP Addresses for AutoVNF, CF, ESC and UEM, on page 12](#).

```
ssh ubuntu@<vip-addr>
```

Command example:

```
ssh ubuntu@192.168.100.38
```

2. *Optional.* Execute the following command in the Exec mode.

```
chassis key value 1234
```

Save config before reload chassis, EVEN IF the same old key value is used.
Old config scripts will become invalid after reload.



Important

This step is optional, and needed only if the chassis key is not set.

3. Save the boot configuration in the flash directory.

```
save configuration /flash/system.cfg
```

```
Warning: About to overwrite boot configuration file
Are you sure? [Yes|No]: yes
```

This will update the boot configuration to use the new bin image.

Use the following command to check the boot configuration.

```
# show boot
```

```
Monday May 21 20:39:57 UTC 2018

boot system priority 8 \
  image /flash/sftp/production.YYYYY.qvpc-di.bin \
  config /flash/sftp/tb5_vnfl_dayN.cfg

boot system priority 9 \
  image /flash/staros.bin \
  config /flash/sftp/tb5_vnfl_dayN.cfg

boot system priority 10 \
  image /flash/staros.bin \
  config /flash/system.cfg
```

4. Enter the configuration mode to change the boot priority of new StarOS bin file.

```
#config
```

```
#boot system priority 1 image /flash/updated.bin config  
/flash/system.cfg
```

```
#end
```

5. Verify the new boot priority.

```
#show boot
```

```
boot system priority 1 \
  image /flash/updated.bin \
  config /flash/system.cfg

boot system priority 10 \
  image /flash/staros.bin \
  config /flash/system.cfg
```

6. Verify whether the flash directory contains the boot configuration and new bin.

```
dir /flash
```

```
total 320376
-rw-rw-r-- 1 root root 134 May 3 10:11 boot.sys
-rw-rw-r-- 1 root root 3920672 May 11 19:49 crashlog2
drwxrwxr-x 2 root root 4096 May 11 19:49 crsh2
-rw-rw-r-- 1 root root 156 May 11 19:49 module.sys
drwxrwxr-x 3 root root 4096 May 11 19:49 patch
drwxrwxr-x 2 root root 4096 May 11 19:49 persistdump
-rw-rw-r-- 1 root root 79 May 11 19:49 restart_file_cntr.txt
drwxrwxr-x 3 root root 4096 May 11 20:07 sftp
-rw-rw-r-- 1 root root 160871936 May 3 10:11 staros.bin
-rw-rw-r-- 1 root root 5199 May 11 19:57 system.cfg
-rw-rw-r-- 1 root root 163227136 May 11 20:07 updated.bin
320476 /flash
Filesystem 1K-blocks Used Available Use% Mounted on
```

```
/var/run/storage/boot1/part2
4112620 320476 3792144 8% /mnt/user/.auto/onboard/flash
```

Synchronize File Systems

To synchronize the file systems:

1. Log on to the VNF using the previously fetched VIP address in the [Obtain VIP Addresses for AutoVNF, CF, ESC and UEM, on page 12](#).
2. Synchronize the local file systems on the management cards by entering the following command:

```
[local]host_name# filesystem synchronize all
```

Example output:

```
Updating /flash/system.cfg
*****
Updating /flash/updated.bin
*****
Updating /flash/sftp/yang/cisco-staros-bulkstats-config.yang
*****
Updating /flash/sftp/yang/cisco-staros-bulkstats-schema-types.yang
*****
Updating /flash/sftp/yang/cisco-staros-bulkstats.yang
*****
Updating /flash/sftp/yang/cisco-staros-cli-config.yang
*****
Updating /flash/sftp/yang/cisco-staros-confd-config.yang
*****
Updating /flash/sftp/yang/cisco-staros-config.yang
*****
Updating /flash/sftp/yang/cisco-staros-exec.yang
*****
Updating /flash/sftp/yang/cisco-staros-kpi.yang
*****
Updating /flash/sftp/yang/cisco-staros-notif.yang
*****
Updating /flash/boot.sys
```

```

*****
12 updated on card 2

    /flash/system.cfg
    /flash/updated.bin
    /flash/sftp/yang/cisco-staros-bulkstats-config.yang
    /flash/sftp/yang/cisco-staros-bulkstats-schema-types.yang
    /flash/sftp/yang/cisco-staros-bulkstats.yang
    /flash/sftp/yang/cisco-staros-cli-config.yang
    /flash/sftp/yang/cisco-staros-confd-config.yang
    /flash/sftp/yang/cisco-staros-config.yang
    /flash/sftp/yang/cisco-staros-exec.yang
    /flash/sftp/yang/cisco-staros-kpi.yang
    /flash/sftp/yang/cisco-staros-notif.yang
    /flash/boot.sys

```

Reboot the System

To reboot the system (VNF):

1. Log on to the VNF using the previously fetched VIP address in the [Obtain VIP Addresses for AutoVNF, CF, ESC and UEM, on page 12](#).

```
ssh ubuntu@<vip-addr>
```

Command example:

```
ssh ubuntu@192.168.100.38
```

2. Enter the following Exec mode command:

```
[local]host_name# reload [-noconfirm]
```

As the system reboots, it loads the new operating system software image and its corresponding CLI configuration file using the new boot stack entry configured earlier.

3. *Optional for PDSN:* If you are using the IP Pool Sharing Protocol during your upgrade, refer to *Configuring IPSP Before the Software Upgrade* in the *PDSN Administration Guide*.
4. After the reload is complete, log on to the VNF and make sure it is loaded with the intended StarOS version and all the cards have booted up and are in active or stand-by state as expected.

```
show version
```

Example output:

```
Active Software:
  Image Version:          21.9.0.69977
  Image Build Number:     69977
  Image Description:      Build
```

```
Image Date:           Mon Jul 30 06:48:34 EDT 2018
Boot Image:           /flash/updated.bin
Source Commit ID:     abde005a31c93734c89444b8aec2b6bb2d2e794d
```

show card table

Example output:

Slot	Card Type	Oper State	SPOF	Attach
1: CFC	Control Function Virtual Card	Active	No	
2: CFC	Control Function Virtual Card	Standby	-	
3: FC	4-Port Service Function Virtual Card	Standby	-	
4: FC	4-Port Service Function Virtual Card	Standby	-	
5: FC	4-Port Service Function Virtual Card	Standby	-	
6: FC	4-Port Service Function Virtual Card	Standby	-	
7: FC	4-Port Service Function Virtual Card	Standby	-	
8: FC	4-Port Service Function Virtual Card	Standby	-	
9: FC	4-Port Service Function Virtual Card	Standby	-	
10: FC	4-Port Service Function Virtual Card	Standby	-	

- Run the following Exec mode command to display additional information about the running StarOS build release.

show build

- Optional.* Verify the operational state of CF and SF VNFCs.



Note This step is relevant only for the upgrade of CF and SF VNFCs.

- Repeat the steps in [Verify Zookeeper Database, on page 15](#) and [Verify ESC Database, on page 16](#) sections.

- Log on to the UEM using either the floating IP or from the AutoVNF using the UEM VIP.

```
ssh ubuntu@<vip-addr>
```

Command example:

```
ssh ubuntu@192.168.100.21
```

- Become the *root* user.

```
sudo -i
```

- Collect the UEM orchestration IP address for Zookeeper database connection.

```
#ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr fa:16:3e:71:1d:08
```

```
          inet addr:192.168.200.12  Bcast:192.168.200.255  Mask:255.255.255.0
```

- Navigate to the `/opt/cisco/usp/packages/zookeeper/<current>/bin` directory.

- Run Zookeeper tool to access the UEM Zookeeper database.

```
zkCli.sh -server <vip-addr>:port_num
```

Command example:


```
zkCli.sh -server 192.168.200.12:2181
```

Make sure there are no outstanding requests between UEM and CF.

- g. Verify the “state”: “alive” for each of the CFs and SFs using the following commands:

```
get /oper/vnfs/vnf_name/vdus/vdu_name/cf1
```

```
get /oper/vnfs/vnf_name/vdus/vdu_name/cf2
```

```
get /oper/vnfs/vnf_name/vdus/vdu_name/sf1
```

```
get /oper/vnfs/vnf_name/vdus/vdu_name/sf2
```

Command examples:

```
get /oper/vnfs/tb1-autovnf1_vpc-vpc-core/vdus/vdu-cf1/cf1
```

```
get /oper/vnfs/tb1-autovnf1_vpc-vpc-core/vdus/vdu-cf1/cf2
```

```
get /oper/vnfs/tb1-autovnf1_vpc-vpc-core/vdus/vdu-sf1/sf1
```

```
get /oper/vnfs/tb1-autovnf1_vpc-vpc-core/vdus/vdu-sf1/sf2
```

- h. Look for the state Alive in the console output.

```
zk: localhost:2181 (CONNECTED) 2] get
/oper/vdus/control-function/BOOT_generic_di-chassis_CF1_1
{"id":"BOOT_generic_di-chassis_CF1_1","state":"alive","vnfcId":"cf-vnfc-di-chassis","uuid":"c4",
"host":"tb5-ultram-osd-compute-2.localdomain","vimId":"523b921c-7266-4fd5-90bb-5157cffc6951",
"cpnts":[{"cpid":"di_intf1","state":"alive","subnet":"6102e9b5-8555-41f5-8cdc-0b47d30a6f7a",
"netmask":"255.255.255.0","dhcp":true,"vl":"vl-vnf1-DI-INTERNAL1-CAT","vnfc":"cf-vnfc-di-chassis",
"port_id":"19539aea-edbf-4acf-a57c-af5627d859ea","ip_address":"192.168.10.3",
"mac_address":"fa:16:3e:19:80:ed","network":"0d72f553-5a9c-4904-b3ea-83371a806e23"},
{"cpid":"di_intf2","state":"alive","nicid":1,"subnet":"30002d02-761d-4ccb-8a9e-d6188cdf54a3",
"netmask":"255.255.255.0","dhcp":true,"vl":"vl-vnf1-DI-INTERNAL2-CAT","vnfc":"cf-vnfc-di-chassis",
"port_id":"ff1dale1-ecf3-477d-98b7-398c3c77fc8d","ip_address":"192.168.11.13",
"mac_address":"fa:16:3e:89:88:23","network":"9f109c0a-b1e7-4d90-a746-5de4ab8ef536"},
{"cpid":"orch","state":"alive","nicid":2,"subnet":"729e9dd2-3c75-43eb-988a-769016f2f44c",
"netmask":"255.255.255.0","dhcp":true,"vl":"vl-vnf1-UAS-ORCH-CAT","vnfc":"cf-vnfc-di-chassis",
"port_id":"81370948-f686-4812-820c-20ec5d3d3cdd","ip_address":"172.168.11.17","mac_address":"fa:16:3e:1d:0b:56",
"network":"9a286170-e393-4ba5-abce-147a45fb337a"}, {"cpid":"mgmt","state":"alive","nicid":3,
"subnet":"9778a11b-1714-4e84-bbc2-86c84b11e8e","netmask":"255.255.255.0","dhcp":true,"vl":"vl-vnf1-UAS-MGMT-CAT",
"vnfc":"cf-vnfc-di-chassis","port_id":"6130cbb4-3dd8-4822-af90-50dac98f2f0d",
"ip_address":"172.168.10.17","mac_address":"fa:16:3e:42:92:47","network":"e278b524-e9a9-48c1-a45b-956a8c3ea583"}],
"monitor":true,"vduId":"Control-function"}
cZxid = 0x100000051
ctime = Fri May 18 19:04:40 UTC 2018
mZxid = 0x10000024a
mtime = Mon May 21 17:48:19 UTC 2018
pZxid = 0x100000051
cversion = 0
dataVersion = 12
aclVersion = 0
ephemeralOwner = 0x0
dataLength = 1625
numChildren = 0
```



Note You can use use **CTRL+D** to exit the zookeeper CLI.

- i. From the UEM VM as a root user, log on to the *ncs_cli* and check for devices live status.

```
~$ sudo -i
ncs_cli -C -u admin
# show devices device device_name live-status
```

Verify that the command output reflects the correct 'state' and 'card-state' of each card.

Example output:

```
# show devices device tb1-autovnf1_vpc-vpc-core-cf-nc live-status
<snip>
VNFC  STATE  VNFC  VDU  CARD  CARD  NUMBER  CPU  DISK  START  UPTIME  NOVA  ID  DATE  FROM  TO
REF  STATE  NAME  REF  TYPE  SLOT  OF  UTIL  SPACE  TIME  TIME  LAUNCH  AND  STATE
ID  ID  ID  ID  ID  CORES  CPU  %  %  TIME  TIME  CMD  TIME

cf1  -  cf1  cf  cf1  1  -  -  -  -  -  -
cf2  -  cf2  cf  cf1  2  -  -  -  -  -  -
sf1  -  sf1  sf  sf1  3  -  -  -  -  -  -
sf2  -  sf2  sf  sf1  4  -  -  -  -  -  -

live-status vnf sj-autovnf-vpc-abc

version 6.0

vnfm vim-tenant-name abc

vnfm tenant-name abc

vnfm ipaddr 192.168.100.22

vnfm port 830

vnfm username ubuntu

vnfm password "$4$+HLzhFFzHq66nqtTsc00CfiODYHq1USVmknltRelf84byNakWEa9sJ8sY/cwFME3aG0UaBC\nvvNNAMkuXQI9Ksfu5IiQQ9ViWbbHw16IEFQ="

virtual-link vl-di-internall

  auto-vnf-connection-ref di-internall

virtual-link vl-management

  auto-vnf-connection-ref management

virtual-link vl-orchestration

  auto-vnf-connection-ref orchestration

virtual-link vl-abc-vpc-svc

  auto-vnf-connection-ref sj-autovnf-abc-vpc-svc

vdu cf

ssh-keygen false
```

```

vm-image                076c887a-a12c-4a0b-b4d6-b2d213f64b9e

lifecycle-event-initialization staros_config.txt

source-url http://192.168.100.9:5000/config/sj-autovnf-vpc-abc/cf/staros_config.txt

lifecycle-event-initialization staros_param.cfg

source-url http://192.168.100.9:5000/config/sj-autovnf-vpc-abc/cf/staros_param.cfg

ned cisco-staros-nc

user                    "$4$+HLzsElkLJOeufWyoSmBwY2LHjOi2WtJdKy/OIux7YHhsNY/
O8hnA9/WwWuFD5trHrW3ZHs\nLo4TfiAKqYwxdNKqFYyoTxH2hrLJV5DgwmE="

password
"$4$+HLzsXtCHJ2vsYZD5s0RGtBRY/dHdu1mgHJX7wCt3o1DMtQZqpBLDCNSJumC7n5rnkVxwI1s\
ncJYeCOFLrqpLHXm3xtXyMdtT7WVzvRMtdao="

netconf

port-number 830

card-type            control-function

usp-auto-vnf-id     sj-autovnf-vpc-abc-cf

vnfc cf-vnfc-ugp

<snip>

```

Restoring the Previous Software Image

If for some reason you need to undo the upgrade, perform the upgrade again except:

- Specify the locations of the upgrade software image and configuration files.

then

- Specify the locations of the original software image and configuration files.

Upgrading ICSR Chassis

The procedure for upgrading primary and backup ICSR chassis is described in *Interchassis Session Recovery*. Essentially the procedure requires upgrading the primary and standby chassis using the off-line method while each is in standby mode.

Performing Dynamic Software Updates

StarOS allows the runtime loading of plugins. All StarOS builds include a "default" baseline plugin.

This feature is currently used to dynamically update the detection logic used to filter P2P applications via the Application Detection and Control (ADC) feature.

Patching is the process used to install a plugin as an incremental update to a StarOS release. One plugin can be provided to multiple, compatible, concurrent product releases. A plugin is distributed in the form of a compressed distribution kit via the internet or by other means (USB stick, CD, etc.).

A plugin is a functional software entity that provides incremental updates to a pre-existing StarOS software component. Plugins have the characteristic of being dynamically loadable at runtime and do not require a system restart. A plugin has a name and one or more versions. All plugin names are known to the system at product release.

For complete information on the Dynamic Software Update process, refer to the *ADC Administration Guide*.

Managing License Keys

License keys define capacity limits (number of allowed subscriber sessions) and available features on your system. Adding new license keys allows you to increase capacity and add new features as your subscriber base grows.

New System License Keys

New systems are delivered with no license keys installed. In most cases, you receive the license key in electronic format (usually through e-mail).

When a system boots with no license key installed a default set of restricted session use and feature licenses is installed. The following Exec Mode command lists the license information:

```
[local]host_name# show license information
```



Important

With no license key installed, the session use licenses for PDSN, HA, GGSN, and L2TP LNS are limited to 10,000 sessions.

The license keys on the ASR 5500 are stored in EEPROM on the chassis midplane. Both MIO/UMIO/MIO2s access this EEPROM when booting.

Session Use and Feature Use Licenses

Session use and feature use licenses are software mechanisms that provide session limit controls and enable special features within the system. These electronic licenses are stored in the system's configuration file that is loaded as part of the system software each time the system is powered on or restarted.

- Session use licenses limit the number of concurrent sessions that a system is capable of supporting per service type and are acquired on an as-needed basis. This allows carriers to pay only for what they are using and easily increase capacity as their subscriber base grows.
- Feature use licenses enable specific features/functionality within the system and are distributed based on the total number of sessions supported by the system.

Installing New License Keys

Use the instructions below to install a new license key.

Cutting and Pasting the Key

If you have a copy of the license, use the following configuration to cut and paste just the license key part:

Step 1 From the Exec mode, enter the following:

```
configure
 license key license
 exit
```

license is the license key string. The license can be an alphanumeric string of 1 through 1023 characters that is case sensitive. Copy the license key as shown in the example below, including the \" (double-quote slash). Please note: this is not a functional license.

```
"\
VER=1|C1M=000-0000-00|C1S=03290231803|C2M=11-1111-11-1|C2S=\
STCB21M82003R80411A4|DOI=0000000000|DOE=00000000|ISS=1|NUM=13459|00000000000000|
LSP=000000|LSH=000000|LSG=500000|LSL=500000|\|FIS=Y|FR4=Y|FPP=Y|FCS=Y|FTC=Y|FMG=Y|
FCR=Y|FSR=Y|FPM=Y|FID=Y|SIG=MCwCF\Esnq6Bs/
XdmyfLe7rHcD4sVP2bzAhQ3IeHDoyyd6388jHsHD99sg36SG267gshssja77
end
```

Step 2 Verify that the license key just entered was accepted by entering the following command at the Exec mode prompt:

```
[local]host_name# show license key
```

The new license key should be displayed. If it is not, return to the Global configuration mode and re-enter the key using the **license key** command.

Important An invalid license will not be accepted. A Failure error will appear in the output of the **license key** command when you attempt to configure an invalid license key. If you use the **-force** option to install an invalid license key, the license will be placed into a 30-day grace period. StarOS will generate daily syslog error messages and SNMP traps during the grace period. The output of the **show license information** command will indicate "License State" as "Not Valid".

Step 3 Verify that the license key enabled the correct functionality by entering the following command:

```
[local]host_name# show license information
```

All license keys and the new session capacity or functionality enabled should be listed. If the functionality or session capacity enabled by the new key is incorrect, please contact your service representative.

Step 4 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Caution Failure to save the new license key configuration in the current CLI configuration file will result in the loss of any of the new features enabled by the license key once the system is reloaded.

Adding License Keys to Configuration Files

License keys can be added to a new or existing configuration file.



Important License key information is maintained as part of the CLI configuration. Each time a key is installed or updated, you must re-save the configuration file.

- Step 1** Open the configuration file to which the new license key commands are to be copied.
- Step 2** Copy the license as shown in the example, including the "\" (double-quote slash). Please note: this is not a functional license.

```
"\
VER=1|C1M=000-0000-00|C1S=03290231803|C2M=11-1111-11-1|C2S=\STCB21M82003R80411A4|
DOI=0000000000|DOE=00000000|ISS=1|NUM=13459|0000000000000|LSP=000000|LSH=000000|
LSG=500000|LSL=500000\FIS=Y|FR4=Y|FPP=Y|FCS=Y|FTC=Y|FMG=Y|FCR=Y|FSR=Y|FPM=Y|FID=Y|
SIG=MCwCF\Esnq6Bs/XdmyfLe7rHcD4sVP2bzAhQ3IeHDoyyd6388jHsHD99sg36SG267gshssja77
end
```

- Step 3** Paste the license key into the configuration
- Important** Paste the license key information at the beginning of the configuration file to ensure the system has the expected capacity and features before it configures contexts.
- Step 4** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

License Expiration Behavior

When a license expires, there is a built-in grace period of 30 days that allows normal use of the licensed session use and feature use licenses. This allows you to obtain a new license without any interruption of service.

The following Exec mode command lists the license information including the date the grace period is set to expire:

```
show license information
```

Requesting License Keys

License keys for the system can be obtained through your Cisco account representative. Specific information is required before a license key may be generated:

- Sales Order or Purchase Order information
- Desired session capacity
- Desired functionality
- Midplane (chassis) serial number

To obtain the ASR 5500 chassis serial number, at the Exec mode prompt enter the **show card hardware 5** command. Look under the "MEC" heading for the "UDI Serial Number" as shown in the example below:

```
MEC:
Description           : MEC
Cisco Part Number     : 73-14501-01 A0
UDI Serial Number     : FLM154300D8
UDI Product ID        : ASR55-MEC
UDI Version ID        : V01
```

The ICSR license key for Active and Standby chassis are uniquely coded to each chassis. Two separate license keys are required.

Viewing License Information

To see the license detail, enter the following command from the Exec mode:

```
[local]host_name# show license information [ full | key [ full ] ]
```

Deleting a License Key

Use the procedure below to delete the session and feature use license key from a configuration. You must be a security administrator or administrator.

```
configure
  no license key
  exit
show license key
```

The output of this command should display: "No license key installed".

Management Card Replacement and License Keys

License keys are stored on a midplane EEPROM in the ASR 5500 chassis. The MIO/UMIO/MIO2s share these license keys. There is no need to swap memory cards into replacement MIO/UMIO/MIO2s.

Managing Local-User Administrative Accounts

Unlike context-level administrative accounts which are configured via a configuration file, information for local-user administrative accounts is maintained in a separate file in flash memory and managed through the software's Shared Configuration Task (SCT). Because local-user accounts were designed to be compliant with ANSI T1.276-2003, the system provides a number of mechanisms for managing these types of administrative user accounts.

For additional information, see [Disable AAA-based Authentication for Console](#) and [Limit local-user Login on Console/vty Lines](#).

Configuring Local-User Password Properties

Local-user account password properties are configured globally and apply to all local-user accounts. The system supports the configuration of the following password properties:

- **Complexity:** Password complexity can be forced to be compliant with ANSI T1.276-2003.
- **History length:** How many previous password versions should be tracked by the system.
- **Maximum age:** How long a user can use the same password.
- **Minimum number of characters to change:** How many characters must be changed in the password during a reset.
- **Minimum change interval:** How often a user can change their password.
- **Minimum length:** The minimum number of characters a valid password must contain.
- **Expiry warning:** Password expiry warning interval in days.

- **Auto-generate:** Automatically generates password with option to specify length of password.

Refer to the **local-user password** command in the *Global Configuration Mode Commands* chapter of the *Command Line Interface Reference* for details on each of the above parameters.

Configuring Local-User Account Management Properties

Local-user account management includes configuring account lockouts and user suspensions.

Local-User Account Lockouts

Local-user accounts can be administratively locked for the following reasons:

- **Login failures:** The configured maximum login failure threshold has been reached. Refer to the **local-user max-failed-logins** command in the *Global Configuration Mode Commands* chapter of the *Command Line Interface Reference* for details
- **Password Aging:** The configured maximum password age has been reached. Refer to the **local-user password** command in the *Global Configuration Mode Commands* chapter of the *Command Line Interface Reference* for details.

Accounts that are locked out are inaccessible to the user until either the configured lockout time is reached (refer to the **local-user lockout-time** command in the *Global Configuration Mode Commands* chapter of the *Command Line Interface Reference*) or a security administrator clears the lockout (refer to the **clear local-user** command in the *Exec Mode Commands* chapter of the *Command Line Interface Reference*).



Important

Local-user administrative user accounts could be configured to enforce or reject lockouts. Refer to the **local-user username** command in the *Global Configuration Mode Commands* chapter of the *Command Line Interface Reference* for details.

Local-User Account Suspensions

Local-user accounts can be suspended as follows:

```
configure
suspend local-user name
```

A suspension can be removed by entering:

```
configure
no suspend local-user name
```

Changing Local-User Passwords

Local-user administrative users can change their passwords using the **password change** command in the Exec mode. Users are prompted to enter their current and new passwords.

Security administrators can reset passwords for local-users by entering the following command from the root prompt in the Exec mode:

```
[local]host_name# password change username name
```


name is the name of the local-user account for which the password is to be changed. When a security administrator resets a local-user's password, the system prompts the user to change their password the next time they login.

All new passwords must adhere to the password properties configured for the system.

