



# CHAPTER 13

## Configuring High Availability (HA)

---

This chapter describes how to set up two Clean Access Servers in high availability (HA) mode. By deploying Clean Access Servers in high-availability mode, you can ensure that important user authentication and connection tasks continue in the event of an unexpected shutdown. Topics include:

- [Overview, page 13-1](#)
- [CAS High Availability Requirements, page 13-5](#)
- [Before Starting, page 13-8](#)
- [Configure High Availability, page 13-9](#)
- [Failing Over an HA-CAS Pair, page 13-22](#)
- [Configure DHCP Failover, page 13-22](#)
- [Modifying High Availability Settings, page 13-26](#)
- [Upgrading an Existing Failover Pair, page 13-28](#)
- [Useful CLI Commands for HA, page 13-28](#)
- [Accessing High Availability Pair Web Consoles, page 13-30](#)
- [Adding High Availability Cisco NAC Appliance To Your Network, page 13-31](#)



### Note

---

You must use identical appliances (e.g. NAC-3350 and NAC-3350) in order to configure High Availability (HA) pairs of Clean Access Managers (CAMs) or Clean Access Servers (CASs).

---

## Overview



### Note

---

Cisco NAC network modules installed in Cisco Integrated Services Routers (ISRs) do not support high availability.

---

The following key points provide a high-level overview of HA-CAS operation:

- The Clean Access Server high-availability mode is an Active/Passive two-server configuration in which a standby CAS machine acts as a backup to an active CAS machine.
- The active CAS performs all tasks for the system. Since most of the CAS configuration is stored on the CAM, when CAS failover occurs, the CAM pushes the configuration to the newly-active CAS.




---

**Note** If you use the Authorization feature in a CAS HA-pair, follow the guidelines in “Backing Up and Restoring CAM/CAS Authorization Settings” in the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)* to ensure you are able to exactly duplicate your Authorization settings from one CAS to its high availability counterpart.

---

- The standby CAS does not forward any packets between its interfaces.
- The standby CAS monitors the health of the active CAS via heartbeat interface (serial and one or more UDP interfaces). Heartbeat packets can be sent on the serial interface, dedicated eth2 interface, dedicated eth3 interface, or eth0/eth1 interface (if no eth2 or eth3 interface is available).
- The primary and secondary CAS machines exchange UDP heartbeat packets every 2 seconds. If the heartbeat timer expires, stateful failover occurs.
- In addition to heartbeat-based failover, the CAS also provides link-based failover based on eth0 or eth1 link failure. The CAS sends ICMP ping packets to an external IP address via the eth0 and/or eth1 interface. Failover will occur if only one CAS can ping the external addresses.




---

**Note** The standby CAS may still receive heartbeat packets from the active CAS via other available heartbeat interfaces (serial or eth2, for example) even though its eth0 and/or eth1 interface goes down. If the standby CAS relies only on heartbeat timers for stateful failover, the standby CAS would never assume the active role even though the active CAS becomes unable to perform its primary function. With link-based failover configured, the active and standby CAS exchange eth0 and eth1 status via the heartbeat interface, so if one of those two interfaces go down, the standby CAS can still assume the active role even if the heartbeat from the active CAS does not trigger a failover event.

---

- Both Clean Access Servers share a virtual Service IP for the eth0 trusted interface and eth1 untrusted interface. The Service IP should be used for SSL certificates.
- Starting from release 4.5(1), when a standby CAS assumes the role of an active CAS that is performing DHCP address management and has gone into Fallback state, the new active CAS also assumes DHCP functions in addition to user login.

**Caution**


---

The connection between HA pairs must be extremely reliable, with communication between HA pairs unimpeded. The best practice is to use a dedicated Ethernet cable. Breaking communication between HA pairs will result in two active nodes, which can have serious negative operational consequences. A key aspect of the link between HA pairs is the ability to restore that link should it go down; restoration may be fundamental to network stability, depending on your design.

---

Figure 13-1 illustrates the basic connections in an example HA-CAS configuration.



Figure 13-2 Active CAS in an HA-Pair

| IP Address                     | Type            | Location | Status    | Manage | Disconnect | Reboot | Delete |
|--------------------------------|-----------------|----------|-----------|--------|------------|--------|--------|
| 10.201.200.200 [10.201.200.16] | Real-IP Gateway |          | Connected |        |            |        |        |

**Note**

If a CAS was previously configured and added to the CAM as a standalone CAS, it must be deleted prior to configuring it for HA. After HA configuration is complete on both CASs, the Service IP is then entered in the **New Server** form to add the HA-CAS pair to the CAM.

**Note**

To ensure heartbeat redundancy, Cisco recommends connecting the serial ports of each Clean Access Server (using “null modem cable”) and enabling the Heartbeat Serial Interface option on each CAS for heartbeat exchange.

**Failover Events**

- If both UDP and serial heartbeat interfaces are configured, then both must fail for the standby system to take over. See [Physical Connection, page 13-5](#) for additional details.
- If the CAS is unable to communicate with the CAM:
  - Users that are already connected will not be affected.
  - New users will not be able to log in.
- You can configure link-based failover. Two IP addresses that are external to the CAS are configured for Link-detect: one on the trusted network, the other on the untrusted network.
  - The active and standby CAS will send ICMP ping packets via eth0 to the IP address on the trusted network.
  - The active and standby CAS will send ICMP ping packets via eth1 to the IP address on the untrusted network.

**Note**

If your network topology restricts Link-detect functionality between your CAS HA pair appliances, you can also use the `/etc/ha.d/linkdetect.conf` file to enforce Link-detect behavior on your eth0 and/or eth1 interfaces. See [Link-Detect Interfaces, page 13-29](#) for more details.

The status of these ping packets is communicated between the CASs via the heartbeat signal:

- If the active and standby CAS can ping both external IPs, no failover occurs
- If the active and standby CAS cannot ping either of the external IPs, no failover occurs
- If the active CAS cannot ping either of the external IPs, but the standby CAS can ping them, failover occurs

- Both the Clean Access Manager and Clean Access Server are designed to automatically reboot in the event of a hard-drive failure, thus automatically initiating failover to the standby CAM/CAS.

### Choosing External IPs for Link-Based Failover

- Keep in mind that when the CAS initiates traffic, it will always send packets out of its untrusted (eth1) interface except for packets destined to its default gateway. Therefore, when choosing an external IP on trusted network for CAS to ping via the eth0 interface, choose any IP belonging to a subnet other than the CAS subnet.
- When choosing an external IP on the untrusted network for CAS to ping via the eth1 interface:
  - This IP has to exist on the CAS management subnet
  - It cannot be the default gateway of the CAS
  - The CAS will send these ping packets out of the eth1 interface
  - Verify whether **Set Management VLAN ID** is enabled for the eth1 interface. If this option is not enabled, CAS will send traffic out untagged on the eth1 interface. The switch will determine whether these packets should be received on its native VLAN. Therefore, on the untrusted interface, ensure that the native VLAN is being forwarded.
  - The external IP address will be in the CAS management subnet, but on the untrusted side, the traffic will be going out from the CAS in the native VLAN; hence ensure the native VLAN is being forwarded towards the external IP device.

Refer to [c. Configure HA-Primary Mode and Update, page 13-11](#) and [c. Configure HA-Secondary Mode and Update, page 13-17](#) for additional configuration details.

## CAS High Availability Requirements

This section describes additional planning considerations when implementing high availability.



### Note

In a CAS HA deployment using NAT on the trusted (eth0) side, you must ensure that the `-Dperfigo.nat.serviceip=<NAT'ed service IP or CAS service hostname>` property is set for the `starttomcat` and `restartweb` files on both the Primary and Secondary CAS.

For example, `-Dperfigo.nat.serviceip=172.10.20.100`.

### Physical Connection

Cisco recommends using a **dedicated** connection for failover heartbeat on Clean Access Server high-availability pairs. You can use:

- A serial null-modem cable

Heartbeat Serial Interface connection generally requires the server machine to have at least two serial ports: one port (ttyS0) is used for the serial heartbeat connection and the other is used to access to the server for configuration tasks. For details, see [Serial Port High-Availability Connection, page 13-9](#).

**Note**

Do not connect the serial cable before starting HA (failover) configuration. The serial cable must be connected after the configuration is complete. See [Connect the Clean Access Servers and Complete the Configuration, page 13-21](#).

**Note**

For serial cable connection for HA (either HA-CAM or HA-CAS), the serial cable must be a “null modem” cable. For details, refer to <http://www.nullmodem.com/NullModem.htm>.

**Warning**

**When connecting high availability (failover) pairs via serial cable, BIOS redirection to the serial port must be disabled for NAC-3300 series appliances and any other server hardware platform that supports the BIOS redirection to serial port functionality. See [Supported Hardware and System Requirements for Cisco NAC Appliance \(Cisco Clean Access\)](#) for more information.**

- A dedicated Ethernet NIC card, configured as the eth2 or eth3 interface of the CAS

**Note**

If a dedicated Ethernet interface (e.g. eth2 or eth3) is not available on the server machine, eth0 and eth1 are supported for the Heartbeat UDP interface in conjunction with the Heartbeat Serial Interface. (This function does not apply, however, if you have deployed your CASs in Virtual Gateway mode *and* the eth0 and eth1 interfaces have the *same* IP address.) See [Selecting and Configuring the Heartbeat UDP Interface, page 13-8](#).

If additional network interfaces (e.g. eth2 or eth3) are available, you can use them for UDP heartbeat instead of eth0. In this case, the eth2 or eth3 interfaces on the two machines are connected using a crossover cable. If installing an additional Ethernet interface, configure the IP address for the interface. For instructions, see [Configuring Additional NIC Cards, page 4-25](#).

## Switch Interfaces for OOB Deployment

For Out-of-Band deployments, ensure that Port Security is not enabled on the switch interfaces to which the CAS and CAM are connected. This can interfere with CAS HA and DHCP delivery.

## Service IP Addresses

In addition to the IP addresses for the trusted and untrusted interfaces for each individual CAS, you will need to provide two Service IP addresses for the trusted and untrusted interfaces of the CAS pair (see [Figure 13-1 on page 13-3](#) for an example configuration). A **Service IP address** is the common IP address that the external network uses to address the pair.

In addition, either the trusted or untrusted interface Service IP address should be used to generate the SSL certificate. If a CAS was previously configured and added to the CAM as a standalone CAS, it must be deleted prior to configuring it for HA.

After HA configuration is complete on both CASs, use the Service IP in the **New Server** form to add the HA-CAS pair to the CAM. Note that the HA-CAS pair is automatically added as the same Server Type (for example, Out-of-Band Virtual Gateway).

## Host Names

For heartbeat, each CAS needs to have a unique hostname (or node name). For HA CAS pairs, this host name will be provided to the peer, and must be resolved via DNS or added to the peer's `/etc/hosts` file.

## DHCP Synchronization

If the Clean Access Servers operate as DHCP Servers (not in DHCP Relay or DHCP Passthrough mode) additional configuration steps must be taken to enable the Clean Access Servers to keep their DHCP-related information synchronized. DHCP information, such as information regarding active leases and lease times, is exchanged by SSH tunnel, which you configure as described in [Configure DHCP Failover, page 13-22](#).

## SSL Certificates

As in standalone mode, in HA mode the Clean Access Servers can use either a temporary, self-signed certificate or a CA (Certificate Authority)-signed certificate. A temporary certificate is useful for testing or development. A production deployment should have a CA-signed certificate. Considerations in either case are:

1. Both the temporary or CA-signed certificates can use either the Service IP address (for either the trusted interface or untrusted interface) or a domain name as the certificate domain name.
2. If creating a certificate using a domain name, then the domain name must map to the Service IP in DNS. If you are not using a domain name in the certificate, then the DNS mapping is not necessary.
3. For a temporary certificate, generate the temporary certificate on one of the Clean Access Servers, and transfer it from that CAS to the other CAS.
4. For a CA-signed certificate, you will need to import the CA-signed certificate into each of the Clean Access Servers in the pair.



---

**Note** The CA-signed certificate must be either based on the Service IP or a hostname/domain name resolvable to the Service IP through DNS.

---



---

**Note** The Clean Access Server retrieves session information from the CAM during failover. For example, if user A is logged into the system in role B, when failover occurs, user A will still be logged in and have access specified by role B.

If the CAS is the DHCP server and failover occurs, user A also retains his/her assigned IP address because to HA CASs *do* directly exchange DHCP failover information. See [Configure DHCP Failover, page 13-22](#).

---



---

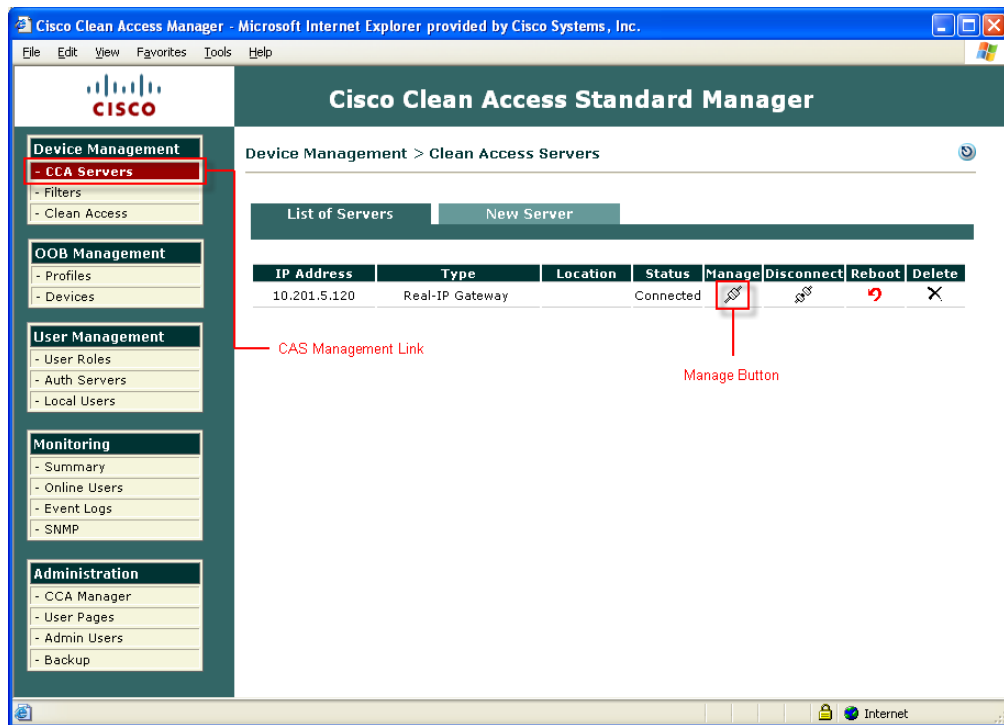
**Note** For HA CAS pairs, any CAS network setting changes performed on an HA-Primary CAS through the CAS management pages or CAS direct access web console must also be repeated on the HA-Secondary CAS unit through its direct access web console. These settings include updating the SSL certificate, system time, time zone, DNS, or Service IP. See [Clean Access Server Direct Access Web Console, page 12-2](#) and [Modifying High Availability Settings, page 13-26](#) for details.

---

## Before Starting

1. Before starting, make sure that both Clean Access Servers are installed and accessible over the network. See [Perform the Initial Configuration, page 4-11](#).
2. The two Clean Access Servers in the HA pair must remain Layer 2 adjacent to support heartbeat and sync functions.
3. If the Clean Access Servers have already been added to the management domain of a CAM, they should be removed. Use the **Delete** button in the **List of Servers** tab to remove the CASs.

**Figure 13-3** List of Servers



**Note**

Cisco NAC Appliance web consoles support Internet Explorer 6.0 and 7.0 browsers.

## Selecting and Configuring the Heartbeat UDP Interface

The Heartbeat UDP interface, if specified, is used to send UDP heartbeat traffic related to high availability. The interface used depends on the interfaces available on the server machine and the load level expected. This interface can use either a dedicated Ethernet interface (such as eth2 or eth3) or the trusted interface eth0, if a dedicated interface is not available.

When using an additional Ethernet interface, you must manually configure the interface using the CAS CLI. There are no eth2 or eth3 configuration settings (IP address, netmask, etc.) available via the CAS web console. For instructions, see [Configuring Additional NIC Cards, page 4-25](#). When a dedicated interface is used, the dedicated interfaces on both machines should be connected using a crossover cable.

Servers running a CAS typically use both available interfaces (eth0 and eth1), with eth0 configured as the trusted network interface. Cisco recommends using the eth2 and eth3 interfaces in addition to the serial interface for heartbeat redundancy, thus freeing up the eth0 and eth1 interfaces to handle Cisco NAC Appliance traffic.

**Note**

If using eth0 as the UDP heartbeat interface, make sure that the management interfaces on the CAS are in their own VLAN, not on a VLAN with other user traffic. This is a general best practice that allows you to segment and protect management traffic when running the failover heartbeat over the same physical interface.

## Serial Port High-Availability Connection

If each machine running the CAS software has two serial ports, use one of the ports for the serial cable connection.

By default, the first serial connector detected on the server is configured for console input/output (to facilitate installation and other types of administrative access).

**Warning**

**When connecting high availability (failover) pairs via serial cable, BIOS redirection to the serial port must be disabled for NAC-3300 series appliances and any other server hardware platform that supports the BIOS redirection to serial port functionality. See [Supported Hardware and System Requirements for Cisco NAC Appliance \(Cisco Clean Access\)](#) for more information.**

When high-availability mode is selected, the serial console login (ttyS0) is automatically disabled to free the serial port for HA mode. To re-enable ttyS0 as the console login, deselect the **Disable Serial Login** checkbox on the **Failover > General** tab after clicking **Update** and before clicking **Reboot**. For details, see steps [c. Configure HA-Primary Mode and Update, page 13-11](#) and [c. Configure HA-Secondary Mode and Update, page 13-17](#).

**Note**

The serial console login and HA serial heartbeat cannot be located on the same serial port.

## Configure High Availability

**Note**

Cisco NAC network modules installed in Cisco Integrated Services Routers (ISRs) do not support high availability.

The following sections describe how to set up high availability in four general procedures:

- Step 1: [Configure the HA-Primary Clean Access Server, page 13-10](#)
- Step 2: [Configure the HA-Secondary Clean Access Server, page 13-16](#)
- Step 3: [Connect the Clean Access Servers and Complete the Configuration, page 13-21](#)
- Step 4: [Failing Over an HA-CAS Pair, page 13-22](#)
- Step 5: [Configure DHCP Failover, page 13-22](#)

If configuring high availability for Clean Access Servers that operate as DHCP servers (not in DHCP relay or passthrough mode), you also need to configure the SSH tunnel between them.

**Note**

“Primary/Secondary” denotes the server mode when it is configured for HA.  
“Active/Standby” denotes the runtime status of the server.

## Configure the HA-Primary Clean Access Server

The general sequence to configure the HA-Primary CAS is as follows:

- a. [Access the HA-Primary CAS Directly, page 13-10](#)
- b. [Configure the Host Information for the HA-Primary CAS, page 13-10](#)
- c. [Configure HA-Primary Mode and Update, page 13-11](#)
- d. [Configure the SSL Certificate, page 13-15](#)
- e. [Reboot the HA-Primary CAS, page 13-16](#)
- f. [Add the CAS to the CAM Using the Service IP, page 13-16](#)

When done, continue to [Configure the HA-Secondary Clean Access Server, page 13-16](#).

### a. Access the HA-Primary CAS Directly

Each Clean Access Server has its own web admin console that allows configuration of certain limited Administration settings directly on the CAS. The CAS direct access web console must be used to configure CAS pairs for HA.

To access the HA-Primary Clean Access Server’s direct access web admin console:

1. Open a web browser and type the IP address of the trusted (eth0) interface of the CAS in the URL/address field, as follows: **https://<primary\_CAS\_eth0\_IP\_address>/admin** (for example, **https://172.16.1.2/admin**).
2. Accept the temporary certificate and log in as user **admin** with the web console password specified during initial configuration.

**Note**

- In order to copy and paste values to/from configuration forms, Cisco recommends keeping both web consoles open for each CAS (primary and secondary). See also [a. Access the HA-Secondary CAS Directly, page 13-17](#).
- To ensure security, Cisco recommends changing the default password of the CAS.

### b. Configure the Host Information for the HA-Primary CAS

3. Click the **Network Settings** link, then the **DNS** tab.
4. In the **Host Name** field, type the host name for the HA-Primary CAS. Make sure there is a domain in the **Host Domain** field, such as cisco.com. If necessary, add one and click **Update**.

**Note**

When configuring HA, it is mandatory to specify a Host Name for each machine in the HA-pair. The Host Name is case-sensitive and cannot be an IP address. Host Names are needed later for the **Local Host Name** and **Peer Host Name** fields of the HA Primary and HA Secondary configuration. The **Local Host Name** and **Peer Host Name** do not need to be resolvable via DNS; however, they are case-sensitive and need to match the Host Names you have specified for the machines.

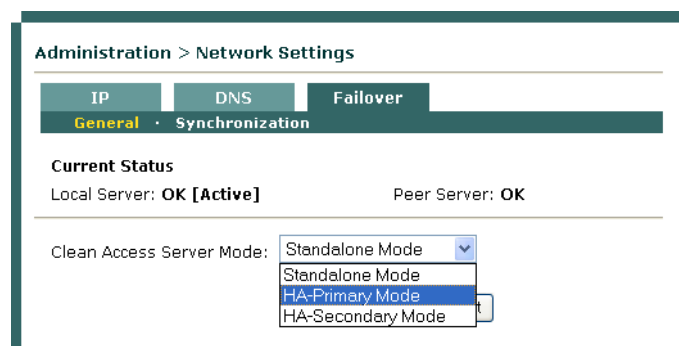
**Figure 13-4** DNS Tab



### c. Configure HA-Primary Mode and Update

- Click the **Failover > General** tab and choose **HA-Primary Mode** from the **Clean Access Server Mode** dropdown menu.

**Figure 13-5** Failover – Choose Mode



- In the **HA-Primary Mode** form that opens, type values for the following fields.

Figure 13-6 Failover — HA-Primary Mode

Administration > Network Settings

---

IP
DNS
Failover

General · Synchronization

**Current Status**

Local Server (rjcas\_1): **OK [ACTIVE]** Peer Server (rjcas\_2): **OK**

---

Clean Access Server Mode: HA-Primary Mode

|   |  |   |
|---|--|---|
| Trusted-side Service IP Address                 | <input style="width: 90%;" type="text" value="10.201.2.112"/>                        | *   |
| Untrusted-side Service IP Address               | <input style="width: 90%;" type="text" value="10.201.50.243"/>                       | *   |
| Trusted-side Link-detect IP Address             | <input style="width: 90%;" type="text" value="N/A"/>                                 |   |
| Untrusted-side Link-detect IP Address           | <input style="width: 90%;" type="text" value="N/A"/>                                 |   |
| Link-detect Timeout (seconds)                   | <input style="width: 90%;" type="text" value="30"/>                                  | **  |
|   | (10 seconds minimum; 25 seconds or longer recommended; 30 seconds default)           |   |
| [Primary] Local Host Name                       | <input style="width: 90%;" type="text" value="rjcas_1"/>                             |   |
| [Primary] Local Serial No.                      | <input style="width: 90%;" type="text" value="00_0C_29_84_1F_B2_00_0C_29_84_1F_BC"/> |   |
| [Primary] Local MAC Address                     | <input style="width: 90%;" type="text" value="00:0C:29:84:1F:B2"/>                   | (trusted-side interface)                  |
| [Primary] Local MAC Address                     | <input style="width: 90%;" type="text" value="00:0C:29:84:1F:BC"/>                   | (untrusted-side interface)                |
| [Secondary] Peer Host Name                      | <input style="width: 90%;" type="text" value="rjcas_2"/>                             | *   |
| [Secondary] Peer MAC Address                    | <input style="width: 90%;" type="text" value="00:0C:29:B2:0E:77"/>                   | (trusted-side interface)                  |
| [Secondary] Peer MAC Address                    | <input style="width: 90%;" type="text" value="00:0C:29:B2:0E:81"/>                   | (untrusted-side interface)                |
| Heartbeat UDP Interface 1                       | <input checked="" type="checkbox"/> eth0   |   |
| [Secondary] Heartbeat IP Address on eth0        | <input style="width: 90%;" type="text" value="10.201.2.111"/>                        | (peer ip on heartbeat udp interface eth0) |
| Heartbeat UDP Interface 2                       | <input type="checkbox"/> eth1  |   |
| [Secondary] Heartbeat IP Address on eth1        | <input style="width: 90%;" type="text"/>   | (peer ip on heartbeat udp interface eth1) |
| Heartbeat UDP Interface 3                       | <span style="border: 1px solid #ccc; padding: 2px;">N/A</span>                       |   |
| [Secondary] Heartbeat IP Address on interface 3 | <input style="width: 90%;" type="text"/>   | (peer ip on heartbeat udp interface 3)    |
| Heartbeat Serial Interface                      | <span style="border: 1px solid #ccc; padding: 2px;">N/A</span>                       |   |
| Heartbeat Timeout (seconds)                     | <input style="width: 90%;" type="text" value="15"/>                                  | *   |
|   | (5 seconds minimum; 15 seconds or longer recommended; 15 seconds default)            |   |

\* Mandatory. Note that at least one eth interface is required to be HA.  
 \*\* Mandatory if Link-detect IP is configured

Update
Reboot

185600

- **Trusted-side Service IP Address:** The common IP address by which the pair is addressed from the trusted network (10.201.2.112 in the example in [Figure 13-1](#) on page 13-3).
- **Untrusted-side Service IP Address:** The common address for the pair on the untrusted (managed) network (10.201.50.243 in the sample).
- **Trusted-side Link-detect IP Address:** When an IP address (e.g. for an upstream router) is optionally entered in this field, the CAS attempts to ping this external address. Typically, the same trusted-side link-detect address is entered on both the HA-Primary and HA-Secondary CAS, but you can specify different addresses for each CAS if your network topology is different.
- **Untrusted-side Link-detect IP Address:** When an IP address (e.g. for a downstream switch) is optionally entered in this field, the CAS will attempt to ping this external address. You can enter the same or different untrusted-side link-detect addresses on both the HA-Primary and HA-Secondary CAS.

**Note**

If your network topology restricts Link-detect functionality between your CAS HA pair appliances, you can also use the `/etc/ha.d/linkdetect.conf` file to enforce Link-detect behavior on your eth0 and/or eth1 interfaces. See [Link-Detect Interfaces, page 13-29](#) for more details.

- **Link-detect Timeout (seconds):** This configures the length of time the CAS attempts to ping the Trusted-side and/or Untrusted-side Link-detect IP address(es). Cisco recommends entering a time of at least 26 seconds. If the CAS cannot ping the node for the period of time specified, the node is not pingable.

**Note**

In addition to Heartbeat Serial Interface/UDP configuration, you can optionally configure the CAS to respond to link failures on the trusted and/or untrusted sides as failover events. The CAS attempts to ping the trusted and/or untrusted link-detect addresses specified, then counts the number of nodes it can reach:

0-for no addresses

1-for either trusted/untrusted

2-for both trusted/untrusted

If the Standby CAS can reach more nodes than the Active CAS, the Standby CAS will take over and become the Active CAS. If both CASs can ping the same number of addresses (all addresses or only one address), no failover event occurs, since neither CAS has the advantage. To enable link-detect, enter at least one link-detect IP address on each CAS and a link-detect timeout. See also [Choosing External IPs for Link-Based Failover, page 13-5](#) for further details.

**Note**

The standby CAS may still receive heartbeat packets from the active CAS via other available heartbeat interfaces (serial or eth2, for example) even though its eth0 and/or eth1 interface goes down. If the standby CAS relies only on heartbeat timers for stateful failover, the standby CAS would never assume the active role even though the active CAS becomes unable to perform its primary function. With link-based failover configured, the active and standby CAS exchange eth0 and eth1 status via the heartbeat interface, so if one of those two interfaces go down, the standby CAS can still assume the active role even if the heartbeat from the active CAS does not trigger a failover event.

The CAS performs Heartbeat connection and (optionally) Link-detect according to the same interval, approximately every 1-2 seconds.

- **[Primary] Local Host Name:** This is filled in by default for the HA-Primary CAS, as configured under **Administration > Network Settings > DNS | Host Name** (“rjcas\_1” in [Figure 13-4](#)).
- **[Primary] Local Serial No:** Filled in by default for the HA-Primary CAS. The local serial number identifies this CAS to the Clean Access Manager (and is composed of eth0/eth1 MAC addresses). In an HA-CAS pair, the serial number of the Primary CAS is the key used to associate all the configuration information specific to this CAS in the CAM database.
- **[Primary] Local MAC Address (trusted-side interface):** Filled in by default; the MAC address of the eth0 interface for the HA-Primary CAS.

- **[Primary] Local MAC Address (untrusted-side interface):** Filled in by default; the MAC address of the eth1 interface for the HA-Primary CAS.

**Note**

- You may want to copy and paste the **[Primary] Local Host Name**, **[Primary] Local Serial No.**, and **[Primary] Local MAC Address (trusted/untrusted)** values into a text file. These values are necessary later when configuring the HA-Secondary CAS.
- To enter the HA-Secondary CAS information into the form for the HA-Primary CAS, copy and paste the corresponding fields from the HA-Secondary CAS web console.

- **[Secondary] Peer Host Name:** Type the host name for the HA-Secondary CAS peer (“rjcas\_2” in this example). The Secondary Peer Host Name is case-sensitive and must exactly match the **Host Name** specified in the peer machine **DNS** tab (under **Administration > Network Settings > DNS | Host Name**).
- **[Secondary] Peer MAC Address (trusted-side interface):** This is the peer MAC address from the trusted (eth0) side of the HA-Secondary CAS.
- **[Secondary] Peer MAC Address (untrusted-side interface):** This is the peer MAC address from the untrusted (eth1) side of the HA-Secondary CAS.
- **Heartbeat UDP Interface 1:** This setting specifies eth0 as a failover IP interface on the CAS. If a dedicated Ethernet connection is not available, Cisco recommends using eth0 for the Heartbeat UDP interface in conjunction with Heartbeat Serial Interface when configuring a Clean Access Server in HA mode.
- **[Secondary] Heartbeat IP Address on eth0:** The IP address of the trusted interface (eth0) of the HA-Secondary CAS.
- **Heartbeat UDP Interface 2:** This setting specifies eth1 as a failover IP interface on the CAS. If you configure your CAS HA system to use eth0 as the primary failover heartbeat connection, you can also use the eth1 interface as a redundant heartbeat monitor.
- **[Secondary] Heartbeat IP Address on eth1:** The IP address of the untrusted interface (eth1) of the HA-Secondary CAS.
- **Heartbeat UDP Interface 3:** Options are N/A, eth2, or eth3. If a dedicated Ethernet connection is not available, Cisco recommends using eth0 or another Ethernet interface for the Heartbeat UDP interface in conjunction with the Heartbeat Serial Interface when configuring a Clean Access Server in HA mode.
- **[Secondary] Heartbeat IP Address on Interface 3:** The IP address of the tertiary failover heartbeat link configured on the HA-Secondary CAS.

**Note**

Before you can specify either the eth2 or eth3 interfaces to be **Heartbeat UDP Interface 3**, you must manually configure the interface using the CAS CLI. There are no eth2 or eth3 configuration settings (IP address, netmask, etc.) available via the CAS web console. For instructions, see [Configuring Additional NIC Cards, page 4-25](#).

- **Heartbeat Serial Interface:** Select the COM port for the serial connection. Cisco recommends using both serial and UDP connections for the Heartbeat interface. The CAS monitors its configured interfaces and only displays **Heartbeat Serial Interface** options that are available at the time you are configuring HA.



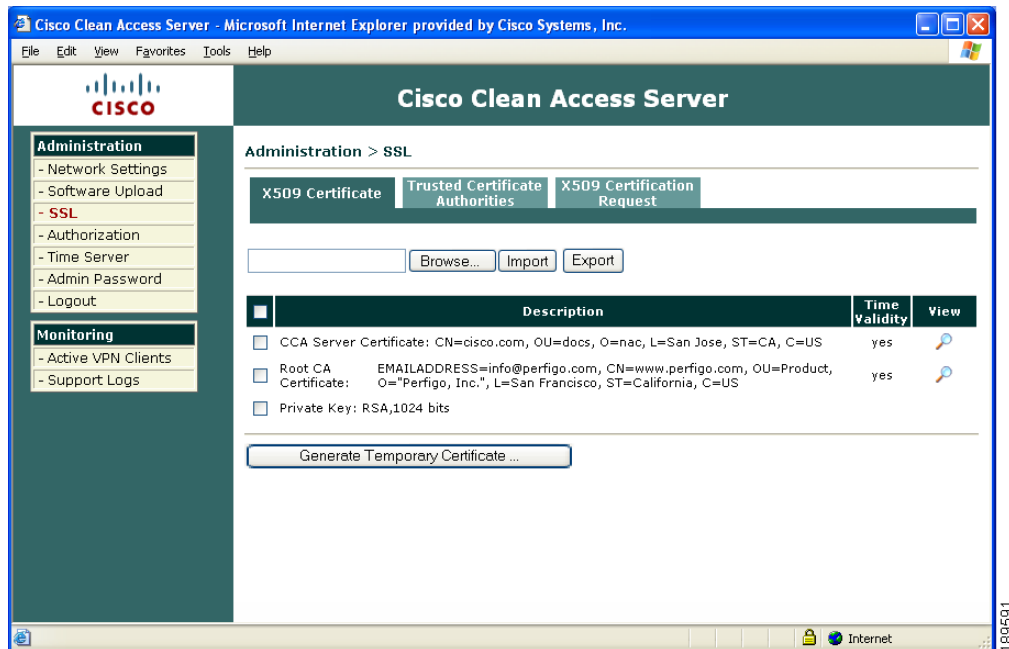
**Note** Do not connect the serial cable before starting HA (failover) configuration. The serial cable must be connected after the configuration is complete.

- **Heartbeat Timeout (seconds):** Choose a value greater than 15 seconds.
- **Update:** Click to update the HA configuration information for the CAS without rebooting it.
- **Reboot:** This is used to reboot the CAS at the end of HA-Primary CAS configuration. (Do **not** click Reboot at this point.)

## d. Configure the SSL Certificate

7. Now configure the SSL certificate for the HA-Primary CAS. Navigate to **Administration > SSL > X509 Certificate**.

**Figure 13-7 Administration > SSL > X509 Certificate**



8. Perform one of the following procedures, depending on whether you intend to use a temporary, self-signed certificate or a CA-signed certificate:

### If using a temporary certificate for the HA pair:

- a. Click **Generate Temporary Certificate**, enter information for all of the fields in the form, and click **Generate**. The certificate must be associated with the Service IP addresses of the HA pair.
- b. When finished generating the temporary certificate, click the checkboxes for the certificate and Private Key to highlight them in the table.
- c. Click **Export** to save the certificate and Private Key to your local machine. You must import the certificate and Private Key later when configuring the HA-Secondary CAS.

**If using a CA-signed certificate for the HA pair:****Note**

This process assumes you have already generated a Certificate Signing Request and accompanying Private Key, submitted the request to your Certificate Authority, and have received your CA-signed certificate. If you have not yet obtained a CA-signed certificate for the CAS, be sure to follow the instructions in [Manage CAS SSL Certificates, page 12-7](#).

- a. Click **Browse** and navigate to the directory on your local machine containing the CA-signed certificate and Private Key.
- b. Click **Import**. Note that you will need to import the same certificate later to the HA-Secondary CAS.

**Note**

The CA-signed certificate must either be based on the Service IP or a host name/domain name resolvable to the Service IP through DNS.

**e. Reboot the HA-Primary CAS**

9. **Reboot** the Clean Access Server from either the CAS direct access interface (**Network Settings > Failover > General > Reboot** button) or from the CAM web console (**Administration > CCA Manager > Network > Reboot** button).

**f. Add the CAS to the CAM Using the Service IP**

10. In the CAM web console, go to **Device Management > CCA Servers > New Server**, and add the CAS to the CAM using the Service IP for the pair (10.201.2.112) as the **Server IP** address.
11. Configure any other settings desired, such as DHCP settings, to control the runtime behavior of the CAS.
12. Test the configuration by trying to log into the untrusted (managed) network from a computer connected to the untrusted interface of the Clean Access Server. Proceed to the next step only if you can successfully access the network.

**Configure the HA-Secondary Clean Access Server****Note**

Cisco NAC network modules installed in Cisco Integrated Services Routers (ISRs) do not support high availability.

The general sequence to configure the HA-Secondary CAS is as follows:

- a. [Access the HA-Secondary CAS Directly](#)
- b. [Configure the Host Information for the HA-Secondary CAS](#)
- c. [Configure HA-Secondary Mode and Update](#)
- d. [Configure the SSL Certificate](#)
- e. [Reboot the HA-Secondary CAS](#)

## a. Access the HA-Secondary CAS Directly

1. Access the web console for the HA-Secondary CAS by opening a web browser and typing the IP address of the trusted (eth0) interface of the HA-Secondary CAS in the URL/address field, as follows: **https://<standby\_CAS\_eth0\_IP\_address>/admin** (for example, **https://172.16.1.3/admin**)
2. Log in as user **admin** and provide the correct password.

**Note**

- In order to copy and paste values to/from configuration forms, Cisco recommends keeping both web consoles open for each CAS (primary and secondary). See also [a. Access the HA-Primary CAS Directly](#), page 13-10.
- To ensure security, Cisco recommends changing the default password of the CAS.

## b. Configure the Host Information for the HA-Secondary CAS

3. In the **Network Settings** page, open the **DNS** tab.
4. Make sure the host name is a unique host name for the HA-Secondary CAS, such as “rjcas\_2.” You must have the same domain name specified in this tab as you did for the HA-Primary CAS (see [b. Configure the Host Information for the HA-Primary CAS](#), page 13-10).

**Note**

When configuring HA, it is mandatory to specify a Host Name for each machine in the HA-pair. The Host Name is case-sensitive and cannot be an IP address. Host Names are needed later for the **Local Host Name** and **Peer Host Name** fields of the HA Primary and HA Secondary configuration. The **Local Host Name** and **Peer Host Name** do not need to be resolvable via DNS; however, they are case-sensitive and need to match the Host Names you have specified for the machines.

## c. Configure HA-Secondary Mode and Update

5. Click the **Failover > General** tab and select **HA-Secondary Mode** from the **Clean Access Server Mode** dropdown menu.

Figure 13-8 Failover — HA-Secondary Mode

Administration > Network Settings

IP DNS Failover

General · Synchronization

**Current Status**  
 Local Server (rjcas\_2): OK [STANDBY] Peer Server (rjcas\_1): OK

Clean Access Server Mode: HA-Secondary Mode

Trusted-side Service IP Address: 10.201.2.112 \*

Untrusted-side Service IP Address: 10.201.50.243 \*

Trusted-side Link-detect IP Address: N/A

Untrusted-side Link-detect IP Address: N/A

Link-detect Timeout (seconds): 30 \*\*  
(10 seconds minimum; 25 seconds or longer recommended; 30 seconds default)

[Secondary] Local Host Name: rjcas\_2

[Secondary] Local Serial No.: 00\_0C\_29\_84\_1F\_B2\_00\_0C\_29\_84\_1F\_BC

[Secondary] Local MAC Address: 00:0C:29:B2:0E:77 (trusted-side interface)

[Secondary] Local MAC Address: 00:0C:29:B2:0E:81 (untrusted-side interface)

[Primary] Peer Host Name: rjcas\_1 \*

[Primary] Peer Serial No.: 00\_0C\_29\_84\_1F\_B2\_00\_0C\_29\_84\_1F\_BC \*

[Primary] Peer MAC Address: 00:0C:29:84:1F:B2 \* (trusted-side interface)

[Primary] Peer MAC Address: 00:0C:29:84:1F:BC \* (untrusted-side interface)

Heartbeat UDP Interface 1:  eth0

[Primary] Heartbeat IP Address on eth0: 10.201.2.110 (peer ip on heartbeat udp interface eth0)

Heartbeat UDP Interface 2:  eth1

[Primary] Heartbeat IP Address on eth1: (peer ip on heartbeat udp interface eth1)

Heartbeat UDP Interface 3: N/A

[Primary] Heartbeat IP Address on interface 3: (peer ip on heartbeat udp interface 3)

Heartbeat Serial Interface: N/A

Heartbeat Timeout (seconds): 15 \*  
(5 seconds minimum; 15 seconds or longer recommended; 15 seconds default)

\* Mandatory. Note that at least one eth interface is required to be HA.  
 \*\* Mandatory if Link-detect IP is configured

Update Reboot

185801

6. In the HA-Secondary form, complete the following fields:

- **Trusted-side Service IP Address:** The IP address by which the pair is addressed from the *trusted* network. Use the same value as for the primary CAS (10.201.2.112 in the example in Figure 13-1 on page 13-3).
- **Untrusted-side Service IP Address:** The IP address by which the pair is addressed from the *untrusted* (managed) network. Use the same value as for the primary CAS (10.201.50.243 in the example).
- **Trusted-side Link-detect IP Address (Optional):** When an IP address (e.g. for an upstream router) is optionally entered in this field, the CAS will attempt to ping this address. Typically, the same trusted-side link-detect address is entered on both the HA-Primary and HA-Secondary CAS, but you can specify different addresses for each CAS if your network topology is different.

- **Untrusted-side Link-detect IP Address (Optional):** When an IP address (e.g. for a downstream switch) is optionally entered in this field, the CAS will attempt to ping this address. You can enter the same or different untrusted-side link-detect addresses on both the HA-Primary and HA-Secondary CAS.



**Note** If your network topology restricts Link-detect functionality between your CAS HA pair appliances, you can also use the `/etc/ha.d/linkdetect.conf` file to enforce Link-detect behavior on your eth0 and/or eth1 interfaces. See [Link-Detect Interfaces, page 13-29](#) for more details.

- **Link-detect Timeout (seconds) (Optional):** This configures the length of time the CAS will attempt to ping the Trusted-side and/or Untrusted-side Link-detect IP address(es). Enter a time of at least 26 seconds. If the CAS cannot ping the node for the period of time specified, the node is not pingable.



**Note** The standby CAS may still receive heartbeat packets from the active CAS via other available heartbeat interfaces (serial or eth2, for example) even though its eth0 and/or eth1 interface goes down. If the standby CAS relies only on heartbeat timers for stateful failover, the standby CAS would never assume the active role even though the active CAS becomes unable to perform its primary function. With link-based failover configured, the active and standby CAS exchange eth0 and eth1 status via the heartbeat interface, so if one of those two interfaces go down, the standby CAS can still assume the active role even if the heartbeat from the active CAS does not trigger a failover event.

See [Choosing External IPs for Link-Based Failover, page 13-5](#) for additional details.

- **[Secondary] Local Host Name:** This is filled in by default for the HA-Secondary CAS, as configured under **Administration > Network Settings > DNS | Host Name** (“rjcas\_2” in this example).
- **[Secondary] Local Serial No:** Filled in by default for the HA-Secondary CAS.
- **[Secondary] Local MAC Address (trusted-side interface):** Filled in by default; the MAC address of the eth0 interface for the HA-Secondary CAS.
- **[Secondary] Local MAC Address (untrusted-side interface):** Filled in by default; the MAC address of the eth1 interface for the HA-Secondary CAS.



**Note**

- You may want to copy and paste the **[Secondary] Local Host Name**, **[Secondary] Local Serial No.** and **[Secondary] Local MAC Address (trusted/untrusted)** values into a text file. These values are needed to configure the HA-Primary CAS.
- To enter the HA-Primary CAS information into the form for the HA-Secondary CAS, copy and paste the corresponding fields from the web console of the HA-Primary CAS.

- **[Primary] Peer Host Name:** Type the host name of the HA-Primary CAS (“rjcas\_1” in [Figure 13-4](#)). The **[Primary] Peer Host Name** is case-sensitive and must exactly match the Host Name specified in the peer machine **DNS** tab (under **Administration > Network Settings > DNS | Host Name**).
- **[Primary] Peer Serial No:** The serial number of the HA-Primary CAS. When the HA-Secondary CAS becomes Active, it must use the serial number of the HA-Primary CAS to identify itself to the CAM in order to access the CAS configuration information.

- **[Primary] Peer MAC Address (trusted-side interface):** The peer MAC address from the trusted side (eth0) of the HA-Primary CAS.
- **[Primary] Peer MAC Address (untrusted-side interface):** The peer MAC address from the untrusted side (eth1) of the HA-Primary CAS.
- **Heartbeat UDP Interface 1:** This setting specifies eth0 as a failover IP interface on the CAS. If a dedicated Ethernet connection is not available, Cisco recommends using eth0 for the Heartbeat UDP interface in conjunction with the Heartbeat Serial Interface when configuring a Clean Access Server in HA mode.
- **[Primary] Heartbeat IP Address on eth0:** The IP address of the trusted interface (eth0) of the HA-Primary CAS.
- **Heartbeat UDP Interface 2:** This setting specifies eth1 as a failover IP interface on the CAS. If you configure your CAS HA system to use eth0 as the primary failover heartbeat connection, you can also use the eth1 interface as a redundant heartbeat monitor.
- **[Primary] Heartbeat IP Address on eth1:** The IP address of the untrusted interface (eth1) of the HA-Primary CAS.
- **Heartbeat UDP Interface 3:** Options are N/A, eth2, or eth3. If a dedicated Ethernet connection is not available, Cisco recommends using eth0 or another Ethernet interface for the Heartbeat UDP interface in conjunction with the Heartbeat Serial Interface when configuring a Clean Access Server in HA mode.
- **[Primary] Heartbeat IP Address on Interface 3:** The IP address of the tertiary failover heartbeat link configured on the HA-Primary CAS.



**Note** Before you can specify either the eth2 or eth3 interfaces to be **Heartbeat UDP Interface 3**, you must manually configure the interface using the CAS CLI. There are no eth2 or eth3 configuration settings (IP address, netmask, etc.) available via the CAS web console. For instructions, see [Configuring Additional NIC Cards, page 4-25](#).

- **Heartbeat Serial Interface:** Select the COM port for the serial connection. Cisco recommends using both serial and UDP connections for the Heartbeat interface. The CAS monitors its configured interfaces and only displays **Heartbeat Serial Interface** options that are available at the time you are configuring HA.
- **Heartbeat Timeout (seconds):** Choose a value greater than 15 seconds.
- **Update:** Click to update the HA configuration information for the CAS without rebooting it.
- **Reboot:** This is used to reboot the CAS at the end of HA-Primary CAS configuration. (Do **not** click Reboot at this point.)

## d. Configure the SSL Certificate

7. Now configure the SSL certificate for the HA-Secondary CAS. Navigate to **Administration > SSL > X509 Certificate** and perform one of the following procedures:

### If using a temporary certificate for the HA pair:

- a. Click **Browse** and navigate to the location on your local machine where you have saved the temporary certificate and Private Key you previously exported from the HA-Primary CAS.
- b. Select the certificate file and click **Import**.
- c. Repeat the process to import the Private Key.

**If using a CA-signed certificate for the HA pair:**

- a. Click **Browse** and navigate to the location on your local machine where you have saved the CA-signed certificate you received from your Certificate Authority and the associated Private Key you exported from the HA-Primary CAS and saved to your local machine.
- b. Select the CA-signed certificate file and click **Import**.
- c. Repeat the process to import the Private Key.

For more information, see [Manage CAS SSL Certificates, page 12-7](#).

**e. Reboot the HA-Secondary CAS**

8. From the CAS direct access interface (**Network Settings > Failover > General**), click the **Reboot** button to reboot the Clean Access Server.

**Connect the Clean Access Servers and Complete the Configuration**

1. Shut down the HA-Primary CAS machine and connect the `rjcas_1` and `rjcas_2` machines using a serial null modem cable (connecting available serial ports) and/or a crossover cable (connecting Ethernet ports if using a pair of Ethernet interfaces such as eth2 or eth3 for failover).
2. Open the Clean Access Manager administration console.
3. Go to **Device Management > CCA Servers > List of Servers**. The Active CAS of a high-availability pair is displayed in brackets next to the Service IP for the pair, as shown in [Figure 13-9](#). Since the HA-Primary CAS is turned off, the IP address of the HA-Secondary CAS should appear in brackets in the **List of Servers** with a status of Connected.

**Figure 13-9 Active CAS in an HA-Pair**



4. Click the **Manage** button for the pair. The management pages of the HA-Secondary CAS (now the Active CAS) should appear.
5. Configure the DHCP Server settings so that they match the DHCP settings of the HA-Primary CAS. If the HA-CAS pair operates as a DHCP server, follow the steps in [Configure DHCP Failover, page 13-22](#) to allow the peer Clean Access Servers to keep DHCP information in synchronization.
6. From a client computer connected to the Clean Access Server's untrusted interface, test the configuration by trying to log on to the untrusted (managed) network as an authorized user. If successful, remain logged on and proceed to the next step.

## Failing Over an HA-CAS Pair


**Note**

For a DHCP Server HA-CAS pair, perform the steps in [Configure DHCP Failover, page 13-22](#) first.

To test your HA system, use the following steps:

1. Turn on the HA-Primary CAS machine. Make sure that the CAS is fully started and functioning before proceeding.
2. From the client computer, log off the user's session and try to log onto the untrusted (managed) network again as the user.
3. The HA-Secondary CAS should still be active and providing services for the user.
4. Shut down the HA-Secondary CAS machine.


**Note**

Cisco recommends “shutdown” or “reboot” on the machine to test failover, or, if a CLI command is preferred, `service perfigo stop` and `service perfigo start`. For a Virtual Gateway CAS, use `service perfigo maintenance` instead to bring the CAS to maintenance mode and allow network connectivity to the management VLAN. See [CAS CLI Commands, page 4-20](#) for details.

5. After about 15 seconds, you should be able to continue browsing, with the HA-Primary CAS becoming the Active server and providing the service.
6. Turn on the HA-Secondary CAS machine (the standby server).
7. Check the event log on the Clean Access Manager. It should correctly indicate the status of the Clean Access Servers (e.g., “rjcas\_1 is dead. rjcas\_2 is up”).
8. Testing of the high availability configuration is now complete.

## Configure DHCP Failover


**Note**

Because Cisco NAC network modules installed in Cisco Integrated Services Routers (ISRs) do not support high availability, you cannot configure DHCP failover on Cisco NAC network modules.

High-availability peer Clean Access Servers (CASs) that operate in DHCP server mode exchange information regarding their DHCP activities, such as active leases and lease times, by secure SSH connection (tunnel). If configuring high availability for Clean Access Servers that will operate as DHCP servers (not in DHCP relay or passthrough mode), you need to configure DHCP failover. Keys for the server and for the account accessing the server are required for both the HA-Primary and HA-Secondary Clean Access Servers. As a result, a total of four keys must be exchanged. The interface described below is provided to facilitate the generation and exchange of the security keys necessary to transfer DHCP failover information between the primary and secondary Clean Access Servers.

**Note**

After the DHCP server and CAS failover have been configured, both primary and secondary Clean Access Servers must be failed over in order to create the `/var/state/dhcp` directory on each server. The `/var/state/dhcp` directory must exist on both servers for DHCP failover to function correctly. See [Connect the Clean Access Servers and Complete the Configuration, page 13-21](#) and [Failing Over an HA-CAS Pair, page 13-22](#).

## To Configure DHCP Failover

To start, open the admin console of the primary CAS and the secondary CAS (`https://<Server IP Address>/admin`). You will have two browsers open during this process.

- 
- Step 1** Go to the admin console of the primary CAS and click the **Network Settings > Failover > Synchronization** tab.
- Step 2** Click the **Enable** button to enable DHCP failover on the primary CAS (notice that this button toggles to **Disable** afterwards).

Figure 13-10 Enable DHCP Failover—Primary CAS

Administration > Network Settings

IP DNS Failover

General · Synchronization

Configure SSH here to synchronize files (DHCP config, DHCP leases, Subnet and VLAN settings) between the CAS failover pair.

File Synchronization is enabled

---

SSH Client Key:

```
AAAAAB3NzaC1yc2EAAAABIAAAAEAsbbsIdawmakT46H8AbOEYL156EavQZf
SVBt1Y6dHuKza2ic2jmw8E1JUsGg7zOgHQ8r8Iws6Uw2eSnnHwdNH653kq
/2p1YHUNGb1JBZeBf1T5AeKncQHcQV6ksH80cpgZimUZcx7yKQwa6f4ciWZ
ZpZw8704YJWMTCViKZ0sa0=
```

Current peer SSH Client key:

Enter peer SSH Client key here:

SSH Server Key:

```
AAAAAB3NzaC1yc2EAAAABIAAAAEAspTsXx+XTGf36P8+35k9Vd4Au3USyh
XY1v+fCsCIB90qpJZ6X+b0ICOhf63bCdF3dr9Nw9MQED/bEnMx779C1Px2f
DxYH4gtmkeT8onI5QjUoB7iR6pgvSXevHnx9Zwh/CCJZ7hG073Q6oihJFbx
ftQL7TpgVC+87eQuZuKMMM=
```

Current peer SSH Server key:

Enter peer SSH Server key here:

Write peer SSH keys:

183821

- Step 3** Copy the value from the **SSH Client Key** field from the primary CAS.
- Step 4** Go to the admin console of the secondary CAS and click the **Network Settings > Failover > Synchronization** tab. (See [Figure 13-11](#).)

Figure 13-11 Enable DHCP Failover—Secondary CAS

Administration > Network Settings

IP DNS Failover

General Synchronization

Configure SSH here to synchronize files (DHCP config, DHCP leases, Subnet and VLAN settings) between the CAS failover pair.

File Synchronization is enabled

SSH Client Key:

```
AAAAAB3NzaC1yc2EAAAABIAAAAEIAA2AaBrcCUCdgs2vGX7I4LdEmISvalxysp
TeZBPm4a6vUHB YnEnIkBw1Vrc7aseBrcu3KzSHhI971GLB2HwqajqEvc0z6v
uF1d09fUaMK/V65IEsxj2Gu7C81cGmn9PP8QZCFYmUto5cPhhhPOJhByZfK
J1sbwL2c1B0ve/vBNSK1IU=
```

Current peer SSH Client key:

```
AAAAAB3NzaC1yc2EAAAABIAAAAEIAshhSIDAwmaKt46H8AbOExL156EavQXf
SVBt1X6dMuKzA21c2jmWh8ELJUsGg7zOgNQ8r8Ivs6UvZeSnnHwNH65SKg
/2piYHUNGb1JBZeBK1T5AeKncQhtqV6ksH80cpgXimUZtx7yKQwa6f4tiWZ
ZpXw6704YJMNTCViKZ0sAO=
```

Enter peer SSH Client key here:

SSH Server Key:

```
AAAAAB3NzaC1yc2EAAAABIAAAAEIAktV5E0eIRKodcRMSZsObgCepIHUFyk2
h/SXj7ZvttZLC2pmIpQqikHmEVLXjYewk+/EztxFiaUDJnlYhhVyEgCz/3
Koag8cRG9hg1OjFVNeJkgFDOLFfgASFhtciNz/J+pDZ1gHDU23n6IBLCUe
hH0e4eQfzpd80Es5sICqV8=
```

Current peer SSH Server key:

Enter peer SSH Server key here:

Write peer SSH keys:

- Step 5** Click the **Enable** button to enable DHCP failover on the secondary CAS (notice that this button toggles to **Disable** afterwards).
- Step 6** Paste the SSH Client Key you copied from the primary CAS into the **Enter peer SSH Client key here:** field.
- Step 7** While still in the admin console of the secondary CAS, copy the value from the **SSH Client Key** field.
- Step 8** Now go back to the admin console of the primary CAS and paste the SSH Client Key of the secondary CAS into the **Enter peer SSH Client key here:** field. (See [Figure 13-10](#).)
- Step 9** While still in the admin console of the primary CAS, copy the value from the **SSH Server Key** field.
- Step 10** Now go to the admin console of the secondary CAS and paste the SSH Server Key of the primary CAS into the **Enter peer SSH Server key here:** field.
- Step 11** While in the admin console of the secondary CAS, copy the value from the **SSH Server key** field.
- Step 12** Click the **Update** button to write the peer SSH keys to the secondary CAS.
- Step 13** Go to the admin console of the primary CAS and paste the SSH Server Key from the secondary CAS into the **Enter peer SSH Server key here:** field.
- Step 14** Click the **Update** button to write the peer SSH keys to the primary CAS. DHCP failover configuration is now complete.

Figure 13-12 DHCP Failover – Configuration Complete

Administration > Network Settings

IP DNS Failover

General Synchronization

Configure SSH here to synchronize files (DHCP config, DHCP leases, Subnet and VLAN settings) between the CAS failover pair.

File Synchronization is enabled

---

SSH Client Key:

```
AAAAAB3NzaC1yc2EAAAABIwAAAIEAsbhsIdAwmakT46H8AbOExL156EavQXf
SVBt1X6dMuKzA2ic2jmWh8E1JUsGg7zOgNQ8r8Iws6UwZe8nnHWdNH65Skg
/2piYHUNGB1JBZeBK1TSaEKncQHTqV6ksH80cpgXimUZtx7yKQwa6f4tiWZ
ZpXw87O4YJWNTCViKZ0sAO=
```

Current peer SSH Client key:

```
AAAAAB3NzaC1yc2EAAAABIwAAAIEA2AzBzCUtdgz2vGXY14LdEmI5valxysp
TeXBpm4a6vUMBvYnEnIkBw1Vrt7nseDru3Kz5MhI971GLB2NWqajqEvt0z6u
uFd09fUAWK/V65IEsxj2Gu7C8lcGmn9RP8OZCFYmUto5rRhhbPOJhByZKh
J1sDwL2riBOve/vBN5K1IU=
```

Enter peer SSH Client key here:

---

SSH Server Key:

```
AAAAAB3NzaC1yc2EAAAABIwAAAIEA5spTsXx+XTGf36P8+35k9Vd4Au3USyh
XY1v+fCsCIB90qpJZ6X+b0ICOhf63bCdF3dr9NU9MQED/bEnMx779C1Px2f
DxYH4gtmkeT8onI5QjUoB7iR6pgvSXevHnx9Zwh/CCJZ7hGO73Q6oihFbx
ftQL7TpgVC+87eQuZuKMMM=
```

Current peer SSH Server key:

```
AAAAAB3NzaC1yc2EAAAABIwAAAIEA5spTsXx+XTGf36P8+35k9Vd4Au3USyh
h/SXj7ZvttZLC2pmIpQqikHMmEvLXjYewk+/EztxFiaUDJnlYhhVYegCz/3
Koag8cRG9hg10jFVNeJkgFDOLFfgASFhntciNz/J+pDZ1gHdu23n6IBLCUe
hHOe4eQfzpd80Es5sICqV8=
```

Enter peer SSH Server key here:

Write peer SSH keys:

183/820

## Modifying High Availability Settings

The following instructions describe how to change settings for an existing high-availability Clean Access Server pair. Changing the Service IP, the subnet mask, or the default gateway for a high-availability pair requires updating the Clean Access Manager and rebooting the Clean Access Server.

Additionally, if the Service IP address is changed and the SSL certificate for the Clean Access Server is based on the Service IP, a new certificate must be generated and imported to each Clean Access Server in the high-availability pair. If the SSL certificate is based on the host name of the Clean Access Server, generating a new certificate is not necessary. However, make sure to change the IP address for that host name in your DNS server.

The general sequence of steps is as follows:

1. Update the Clean Access Server settings in the Clean Access Manager first (but do not reboot).
2. Update the HA settings in the direct access web console for the primary CAS and reboot the primary CAS.
3. While the primary CAS reboots, wait for the secondary CAS to become active in the CAM's List of Servers.
4. Repeat steps 1-3 for the secondary CAS and reboot the secondary CAS.
5. While the secondary CAS reboots, the primary CAS becomes active in the Clean Access Manager and displays the new settings.

## To Change IP Settings for an HA-CAS

1. From the CAM web admin console, go to **Device Management > CCA Servers**.
2. Click the **Manage** button for the Clean Access Server.
3. Click the **Network** tab.
4. Change the **IP Address**, **Subnet Mask**, or **Default Gateway** settings for the trusted/untrusted interfaces as desired.
5. Click the **Update** button only.



### Caution

---

Do not click the **Reboot** button at this stage.

---

6. If the SSL certificate for the CAS was based on the previous IP address, you will need to generate a new SSL certificate based on the new IP address configured. This can be done under **Administration > SSL > X509 Certificate**. See [Manage CAS SSL Certificates, page 12-7](#) for details.
7. If the SSL certificate was based on the host name of your Clean Access Server, you do not need to generate a new certificate. However, make sure to change the IP address for that host name in your DNS server.
8. Next, open the direct access web admin console for the **primary** Clean Access Server as follows:  

```
https://<primary_CAS_eth0_IP_address>/admin
```
9. The IP form for the primary CAS will reflect the changes you made in the CAM web console under **Device Management > CCA Servers > Manage [CAS\_IP] > Network > IP**.
10. In Clean Access Server direct access console, click the **Network > Failover > General** tab.
11. Change the following as needed:
  - Trusted-side Service IP Address
  - Untrusted-side Service IP Address
  - [Secondary] Peer Host Name
  - [Secondary] Peer MAC Address (trusted-side interface)
  - [Secondary] Peer MAC Address (untrusted-side interface)
  - [Secondary] Heartbeat IP Address
12. Click the **Update** button, then the **Reboot** button.

13. From the Clean Access Manager administrator web console, go to **Device Management > CCA Servers** and wait for the secondary Clean Access Server to become active. (Note that this can take a few minutes.) The active CAS of a high-availability pair is displayed in brackets next to the Service IP for the pair, as shown in [Figure 13-1 on page 13-3](#). The IP address of the secondary CAS should appear in brackets in the **List of Servers** with a status of Connected.
14. Once the IP address of the secondary CAS appears in brackets in the **List of Servers**, and the CAS has a status of Connected, repeat steps 1-11 for the secondary CAS.
15. Once changes are made and the secondary CAS is rebooted, the primary CAS will appear as the active server on the List of Servers and displays all the new IP information.

## Upgrading an Existing Failover Pair

For instructions on upgrading an existing failover pair to a new Cisco NAC Appliance release, see “Upgrading High Availability Pairs” in the [Release Notes for Cisco NAC Appliance, Version 4.5\(1\)](#).

## Useful CLI Commands for HA

The following are useful files to know about for HA on the CAS:

- [HA CAS Configuration Status \(/etc/ha.d/perfigo.conf\)](#)
- [Heartbeat/Link-Based Connections \(/etc/ha.d/ha.cf\)](#)
- [Link-Detect Interfaces \(/etc/ha.d/linkdetect.conf\)](#)
- [Active/Standby Status \(/perfigo/common/bin/fostate.sh\)](#)

## HA CAS Configuration Status

The `/etc/ha.d/perfigo.conf` file shows a variety of configuration information for an HA-CAS, including hostname (`rjcas_1`), peer hostname (`rjcas_2`), HA mode (Primary), heartbeat interface (UDP/serial), and Link-detect interface information:

```
[root@rjcas_1 ha.d]# more perfigo.conf
#linux-ha
#Mon Aug 28 18:50:15 PDT 2006
WIRELESS_SERVICEIP=10.10.20.4
PING_DEAD=25
HOSTNAME=rjcas_1
HA_DEAD=15
PEERGUSK=
PEERMAC=00\:16\:35\:BF\:FE\:67
PEERHOSTNAME=rjcas_2
TRUSTED_PINGNODE=10.10.40.100
UNTRUSTED_PINGNODE=10.10.20.100
HAMODE=PRIMARY
PEERMAC0=00\:16\:35\:BF\:FE\:66
PEERHOSTIP=10.10.50.2
HA_FAILBACK=off
HA_UDP=eth2
WIRED_SERVICEIP=10.10.20.4
HA_SERIAL=ttys0
```

## Heartbeat/Link-Based Connections

The `/etc/ha.d/ha.cf` file shows additional information about the heartbeat and link-based connections:

```
[root@rjcas_1 ha.d]# more ha.cf
# Generated by make-hacf-ss.pl
udpport          694
ucast           eth2 10.10.50.2
baud             19200
serial         /dev/ttyS0
keepalive        2
deadtime         15
deadping         25
auto_failback    off
apiauth          default uid=root
respawn          hacluster /usr/lib64/heartbeat/ipfail
ping           10.10.20.100
ping           10.10.40.100

log_badpack      false
warntime         10
debug            0
debugfile     /var/log/ha-debug
logfile       /var/log/ha-log
watchdog         /dev/watchdog
node          rjcas_1
node          rjcas_2
```

## Link-Detect Interfaces

The `/etc/ha.d/linkdetect.conf` file is useful if your network topology restricts configuring external (pingable) interfaces for Link-detect functionality between your CAS HA pair appliances. This file specifies the CAS network interfaces (eth0, eth1, or both) to monitor for Link-detect functionality. If a monitored interface loses connectivity with its associated external interface, the active CAS fails over and the standby CAS assumes the active role.

To create and/or update the `linkdetect.conf` file in the CAS:

- 
- Step 1** Log in to the CAS direct console CLI and direct console as the root user.
  - Step 2** Navigate to the `/etc/ha.d/` directory on the CAS.
  - Step 3** Using a standard text editor (like vi), edit the `linkdetect.conf` file so that it contains the interface names you want to monitor, or (if the `linkdetect.conf` file does not currently exist on the CAS) add the `linkdetect.conf` file to this directory.

- Step 4** Verify the contents of the file:

```
[root@rjcas_1 ha.d]# more linkdetect.conf

# The following network interfaces will be monitored for link healthiness
# The active CAS will change to standby mode when any link failure is detected
#
eth0
eth1
```

- Step 5** Enable the new function by stopping and restarting CAS services with the `service perfigo stop` and `service perfigo start` commands.
-

In the above **linkdetect.conf** file example, both the eth0 and eth1 interfaces on the CAS are monitored for network connectivity.

**Note**

Any other CAS interfaces specified in the **linkdetect.conf** file (like eth2 or eth3, for example) are ignored for purposes of Link-detect behavior.

## Active/Standby Status

The following example shows how to use the CLI to determine the runtime status (active or standby) of each CAS in the HA pair. You can find the `fostate.sh` command in the `/perfigo/common/bin/` directory on new and upgraded CASs.

1. Cd to `/perfigo/common/bin/`, and run the `fostate.sh` script on the first CAS:

```
[root@rjcas_1 bin]# ./fostate.sh
My node is active, peer node is standby
[root@rjcas_1 bin]#
```

This CAS is the active CAS in the HA-pair.

2. Run the `fostate.sh` script on the second CAS:

```
[root@rjcas_2 bin]# ./fostate.sh
My node is standby, peer node is active
[root@rjcas_2 bin]#
```

This CAS is the standby CAS in the HA-pair.

# Accessing High Availability Pair Web Consoles

## Determining Active and Standby CAS

From the CAM web console, go to **Device Management > CCA Servers > List of Servers** to view your HA-CAS pairs. The List of Servers page displays the **Service IP** of the CAS pair first, followed by the IP address of the Active CAS in brackets. When a secondary CAS takes over, its IP address will be listed in the brackets as the Active server.

**Note**

The CAS configured in HA-Primary Mode may not be the currently Active CAS.

## Determining Primary and Secondary CAS

Open the direct access console for each CAS in the pair by typing the following in the URL/Address field of a web browser (you should have two browsers open):

- For the Primary CAS, type: **https://<primary\_CAS\_eth0\_IP\_address>/admin**. For example, `https://172.16.1.2/admin`.

- For the Secondary CAS, type: **https://<secondary\_CAS\_eth0\_IP\_address>/admin**. For example, `https://172.16.1.3/admin`.

In each CAS web console, go to **Administration > Network Settings > Failover > General**.

- The Primary CAS is the CAS you configured in **HA-Primary Mode** when you initially set up HA.
- The Secondary CAS is the CAS you configured in **HA-Secondary Mode** when you initially set up HA.

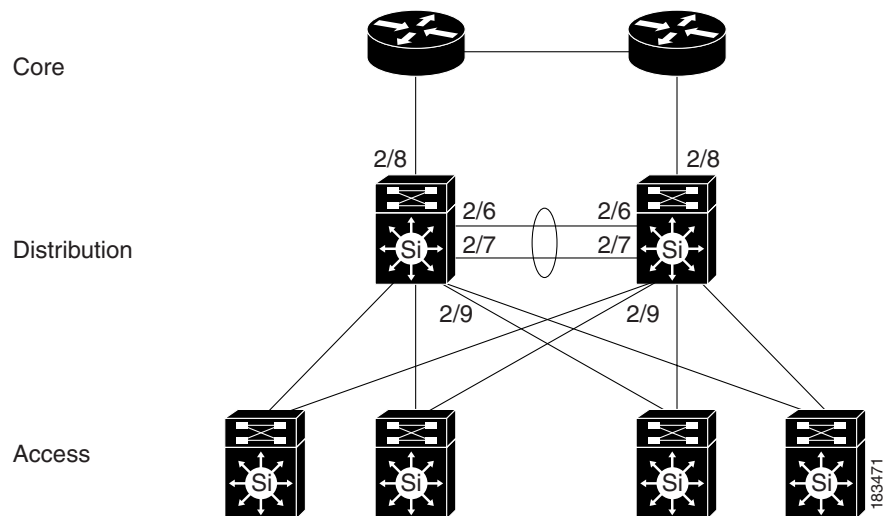
For releases prior to 4.0(0), the Secondary CAS is labelled as **HA-Standby Mode (CAS)** for the initial HA configuration.

## Adding High Availability Cisco NAC Appliance To Your Network

The following diagrams illustrate how HA-CAMs and HA-CASs can be added to an example core-distribution-access network (with Catalyst 6500s in the distribution and access layers).

[Figure 13-13](#) shows a network topology without Cisco NAC Appliance, where the core and distribution layers are running HSRP (Hot Standby Router Protocol), and the access switches are dual-homed to the distribution switches.

**Figure 13-13** Example Core-Distribution-Access Network Before Cisco NAC Appliance



[Figure 13-14](#) shows how HA-CAMs can be added to the core-distribution-access network. In this example, the HA heartbeat connection is configured over both serial and eth1 interfaces.

Figure 13-14 Adding HA CAMs to Network

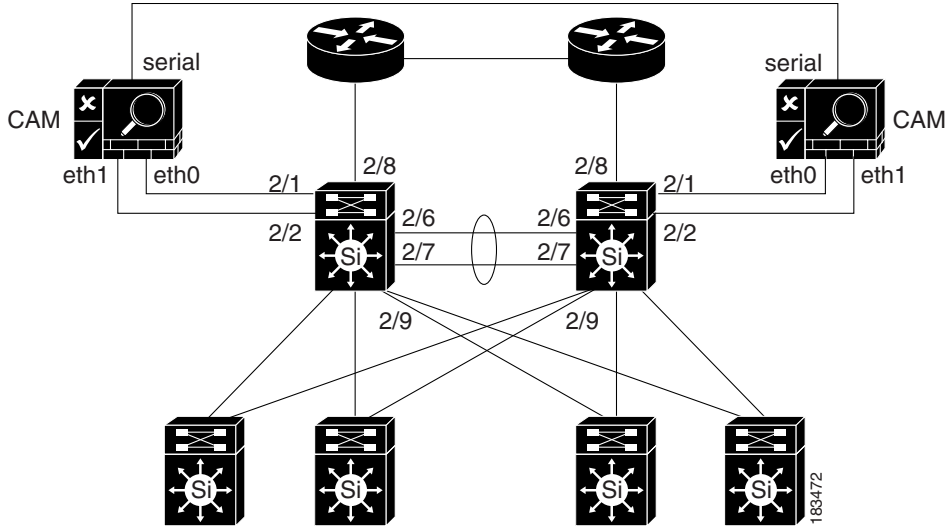


Figure 13-15 shows how HA-CASs can be added to the core-distribution-access network. In this example, the CAS is configured as an L2 OOB Virtual Gateway in Central Deployment. The HA heartbeat connection is configured over both a serial interface and a dedicated eth2 interface. Link-failure based failover connection can also be configured over the eth0 and/or eth1 interfaces.



**Note**

Cisco NAC network modules installed in Cisco Integrated Services Routers (ISRs) do not support high availability.

Figure 13-15 Adding HA CAS to Network

