



Upgrade/Downgrade Guide, Cisco ACE 4700 Series Application Control Engine Appliance

Software Version A4(2.0) and Later
September, 2012



Note

The most current Cisco documentation for released products is available on [Cisco.com](http://www.cisco.com) from the [Support and Documentation](#) page.

Contents

This upgrade/downgrade guide applies to software version A4(2.0) and later for the Cisco ACE 4700 Series Application Control Engine Appliance. For information on the ACE features and configuration details, see the ACE appliance documentation located on www.cisco.com at:

http://www.cisco.com/en/US/products/ps7027/tsd_products_support_series_home.html

This guide contains the following sections:

- [Upgrade Scenarios Based on Licenses in Software Release A4\(1.1\), A3\(2.7\), and Earlier](#)
- [Upgrade Scenarios Based on Software Release A4\(2.0\) and Later Licenses](#)
- [Effects of Upgrading or Downgrading to or from Software Release A4\(2.0\) or Later](#)
- [Ordering an Upgrade License and Generating a Key](#)
- [Upgrading Your ACE Software in a Redundant Configuration](#)
- [Downgrading Your ACE Software in a Redundant Configuration](#)
- [ACE Documentation Set](#)
- [Obtaining Documentation and Submitting a Service Request](#)



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

© 2011 Cisco Systems, Inc. All rights reserved.

Upgrade Scenarios Based on Licenses in Software Release A4(1.1), A3(2.7), and Earlier

This section describes the possible upgrade scenarios available to you when using the licenses in software version A4(1.1), A3(2.7), and earlier.

Table 1 Upgrade Scenarios Based on Software Release A4(1.1), A3(2.7), and Earlier Licenses

Current License	Need	Solution	Result
ACE 4710 bundle licenses			
ACE-4710-0.5F-K9 <ul style="list-style-type: none"> 0.5 Gbps throughput 100 Mbps compression 100 SSL TPS 5 virtual contexts (VCs) 	Increased SSL, compression, and/or VCs	Software upgrade to version A4(2.0)	<ul style="list-style-type: none"> 0.5 Gbps throughput Up to 2 Gbps of compression (limited by device throughput) 7500 SSL TPS 20 VCs
ACE-4710-0.5F-K9 <ul style="list-style-type: none"> 0.5 Gbps throughput 100 Mbps compression 100 SSL TPS 5 VCs 	Throughput upgrade only	Start upgrade with ACE-4710-BUN-UP1=	<ul style="list-style-type: none"> 1 Gbps throughput 500 Mbps compression 5000 SSL TPS 5 VCs
ACE-4710-1F-K9 <ul style="list-style-type: none"> 1 Gbps throughput 500 Mbps compression 5000 SSL TPS 5 VCs 	Increased SSL, compression, and/or VCs	Software upgrade to version A4(2.0)	<ul style="list-style-type: none"> 1 Gbps throughput Up to 2 Gbps of compression (limited by device throughput) 7500 SSL TPS 20 VCs
ACE-4710-1F-K9 <ul style="list-style-type: none"> 1 Gbps throughput 500 Mbps compression 5000 SSL TPS 5 VCs 	Throughput upgrade only	Start upgrade with ACE-4710-BUN-UP2=	<ul style="list-style-type: none"> 2 Gbps throughput 1 Gbps compression 700 SSL TPS 5 VCs
ACE-4710-BAS-2PAK Two units each with: <ul style="list-style-type: none"> 1 Gbps throughput 100 Mbps compression 1000 SSL TPS 5 VCs 	Increased SSL, compression, and/or VCs	Software upgrade to version A4(2.0) on each 4710	Each 4710 has: <ul style="list-style-type: none"> 1 Gbps throughput Up to 2 Gbps of compression (limited by device throughput) 7500 SSL TPS 20 VCs

Table 1 Upgrade Scenarios Based on Software Release A4(1.1), A3(2.7), and Earlier Licenses (continued)

Current License	Need	Solution	Result
ACE-4710-BAS-2PAK Two units each with: <ul style="list-style-type: none"> • 1 Gbps throughput • 100 Mbps compression • 1000 SSL TPS • 5 VCs 	Throughput upgrade only	Start upgrade with ACE-4710-BUN-UP2= (Two licenses required for two 4710s in the 2PAK bundle)	Each 4710 with: <ul style="list-style-type: none"> • 2 Gbps throughput • 1 Gbps compression • 7500 SSL TPS • 5 VCs
ACE-4710-2F-K9 <ul style="list-style-type: none"> • 2 Gbps throughput • 1 Gbps compression • 7500 SSL TPS • 5 VCs 	Increased SSL, compression and/or VCs	Software upgrade to version A4(2.0)	<ul style="list-style-type: none"> • 2 Gbps throughput • 2 Gbps compression • 7500 SSL TPS • 20 VCs
ACE-4710-2F-K9 <ul style="list-style-type: none"> • 2 Gbps throughput • 1 Gbps compression • 7500 SSL TPS • 5 VCs 	Throughput upgrade only	Upgrade with ACE-4710-BUN-UP3=	<ul style="list-style-type: none"> • 4 Gbps throughput • 2 Gbps compression • 7500 SSL TPS • 5 VCs
ACE-4710-4F-K9 <ul style="list-style-type: none"> • 4 Gbps throughput • 2 Gbps compression • 7500 SSL TPS • 5 VCs 	Increased VC (only possible option, everything else is maximized)	Software upgrade to version A4(2.0)	<ul style="list-style-type: none"> • 2 Gbps throughput • 2 Gbps compression • 7500 SSL TPS • 20 VCs
ACE 4710 A-La-Carte Licenses			
ACE4710 with 1 Gbps throughput: <ul style="list-style-type: none"> • ACE-AP-01-LIC • Any combination of feature licenses 	Increased SSL, compression, and/or VCs	Software upgrade to version A4(2.0)	<ul style="list-style-type: none"> • 1 Gbps throughput • Up to 2 Gbps of compression (limited by device throughput) • 7500 SSL TPS • 20 VCs
ACE4710 with 1 Gbps throughput: <ul style="list-style-type: none"> • ACE-AP-01-LIC • Any combination of feature licenses 	Throughput upgrade to 2 Gbps	Upgrade with ACE-AP-02-UP1=	<ul style="list-style-type: none"> • 2 Gbps throughput • Retains previous combination of feature licenses

Table 1 Upgrade Scenarios Based on Software Release A4(1.1), A3(2.7), and Earlier Licenses (continued)

Current License	Need	Solution	Result
ACE4710 with 1 Gbps throughput: <ul style="list-style-type: none"> • ACE-AP-01-LIC • Any combination of feature licenses 	Throughput upgrade to 4 Gbps	Upgrade with ACE-AP-04-UP1=	<ul style="list-style-type: none"> • 4 Gbps throughput • Retains previous combination of feature licenses
ACE4710 with 2 Gbps throughput: <ul style="list-style-type: none"> • ACE-AP-02-LIC • Any combination of feature licenses 	Increased SSL, compression, and/or VCs	Software upgrade to version A4(2.0)	<ul style="list-style-type: none"> • 2 Gbps throughput • 2 Gbps compression • 7500 SSL TPS • 20 VCs
ACE4710 with 2 Gbps throughput: <ul style="list-style-type: none"> • ACE-AP-02-LIC • Any combination of feature licenses 	Throughput upgrade to 4 Gbps	Upgrade with ACE-AP-04-UP2=	<ul style="list-style-type: none"> • 4 Gbps throughput • Retains previous combination of feature licenses
ACE4710 with 4 Gbps throughput: <ul style="list-style-type: none"> • ACE-AP-04-LIC • Any combination of feature licenses 	Increased SSL, compression, and/or VCs	Software upgrade to version A4(2.0)	<ul style="list-style-type: none"> • 4 Gbps throughput • 2 Gbps compression • 7500 SSL TPS • 20 VCs

Upgrade Scenarios Based on Software Release A4(2.0) and Later Licenses

This section describes the possible upgrade scenarios available to you when using the licenses in software version A4(2.0) and later.



Note

Software version A4(2.0) and later contain only license bundles with 0.5 Gbps, 1 Gbps, 2 Gbps, or 4 Gbps of bandwidth and with all feature licenses at their maximum values.

Table 2 Upgrade Scenarios Based on Software Release A4(2.0) and Later Licenses

Current License	Need	Solution	Result
ACE 4710 bundle licenses			
ACE-4710-0.5F-K9 <ul style="list-style-type: none"> • 0.5 Gbps throughput • 100 Mbps compression • 100 SSL TPS • 5 VCs 	Increased SSL, compression and/or VCs	Software upgrade to version A4(2.0)	<ul style="list-style-type: none"> • 0.5 Gbps throughput • Up to 2 Gbps of compression (limited by device throughput) • 7500 SSL TPS • 20 VCs
ACE-4710-0.5F-K9 <ul style="list-style-type: none"> • 0.5 Gbps throughput • 100 Mbps compression • 100 SSL TPS • 5 VCs 	Throughput upgrade only	Start upgrade with ACE-4710-BUN-UPG1=	<ul style="list-style-type: none"> • 1 Gbps throughput • Up to 2 Gbps of compression (limited by device throughput) • 7500 SSL TPS • 20 VCs
ACE-4710-1F-K9 <ul style="list-style-type: none"> • 1 Gbps throughput • 500 Mbps compression • 5000 SSL TPS • 5 VCs 	Increased SSL, compression and/or VCs	Software upgrade to version A4(2.0)	<ul style="list-style-type: none"> • 1 Gbps throughput • Up to 2 Gbps of compression (limited by device throughput) • 7500 SSL TPS • 20 VCs
ACE-4710-1F-K9 <ul style="list-style-type: none"> • 1 Gbps throughput • 500 Mbps compression • 5000 SSL TPS • 5 VCs 	Throughput upgrade only	Start upgrade with ACE-4710-BUN-UPG2=	<ul style="list-style-type: none"> • 2 Gbps throughput • Up to 2 Gbps of compression • 7500 SSL TPS • 20 VCs
ACE-4710-BAS-2PAK Two units each with: <ul style="list-style-type: none"> • 1 Gbps throughput • 100 Mbps compression • 1000 SSL TPS • 5 VCs 	Increased SSL, compression and/or VCs	Software upgrade to version A4(2.0) on each 4710	Each 4710 has: <ul style="list-style-type: none"> • 1 Gbps throughput • Up to 2 Gbps of compression (limited by device throughput) • 7500 SSL TPS • 20 VCs
ACE-4710-BAS-2PAK Two units each with: <ul style="list-style-type: none"> • 1 Gbps throughput • 100 Mbps compression • 1000 SSL TPS • 5 VCs 	Throughput upgrade only	Start upgrade with ACE-4710-BUN-UPG2= (Two licenses required for two 4710s in the 2PAK bundle)	Each 4710 with: <ul style="list-style-type: none"> • 2 Gbps throughput • Up to 2 Gbps of compression • 7500 SSL TPS • 20 VCs

Table 2 Upgrade Scenarios Based on Software Release A4(2.0) and Later Licenses (continued)

Current License	Need	Solution	Result
ACE-4710-2F-K9 <ul style="list-style-type: none"> • 2 Gbps throughput • 1 Gbps compression • 7500 SSL TPS • 5 VCs 	Increased SSL, compression and/or VCs	Software upgrade to version A4(2.0)	<ul style="list-style-type: none"> • 2 Gbps throughput • 2 Gbps compression • 7500 SSL TPS • 20 VCs
ACE-4710-2F-K9 <ul style="list-style-type: none"> • 2 Gbps throughput • 1 Gbps compression • 7500 SSL TPS • 5 VCs 	Throughput upgrade only	Start upgrade with ACE-4710-BUN-UPG3=	<ul style="list-style-type: none"> • 4 Gbps throughput • 2 Gbps compression • 7500 SSL TPS • 20 VCs
ACE-4710-4F-K9 <ul style="list-style-type: none"> • 4 Gbps throughput • 2 Gbps compression • 7500 SSL TPS • 5 VCs 	Increased VC (only possible option, other features are maximized)	Software upgrade to version A4(2.0)	<ul style="list-style-type: none"> • 4 Gbps throughput • 2 Gbps compression • 7500 SSL TPS • 20 VCs
ACE 4710 A-La-Carte Licenses			
ACE4710 with 1 Gbps throughput <ul style="list-style-type: none"> • ACE-AP-01-LIC • Any combination of feature licenses 	Increased SSL, compression and/or VCs	Software upgrade to version A4(2.0)	<ul style="list-style-type: none"> • 1 Gbps throughput • Up to 2 Gbps of compression (limited by device throughput) • 7500 SSL TPS • 20 VCs
ACE4710 with 1 Gbps throughput <ul style="list-style-type: none"> • ACE-AP-01-LIC • Any combination of feature licenses 	Throughput upgrade to 2 Gbps	Start upgrade with ACE-4710-BUN-UPG2=	<ul style="list-style-type: none"> • 2 Gbps throughput • Up to 2 Gbps of compression • 7500 SSL TPS • 20 VCs
ACE4710 with 1 Gbps throughput <ul style="list-style-type: none"> • ACE-AP-01-LIC • Any combination of feature licenses 	Throughput upgrade to 4 Gbps	Start upgrade with ACE-4710-BUN-UPG2= and then ACE-4710-BUN-UPG3=	<ul style="list-style-type: none"> • 4 Gbps throughput • 2 Gbps compression • 7500 SSL TPS • 20 VCs

Table 2 Upgrade Scenarios Based on Software Release A4(2.0) and Later Licenses (continued)

Current License	Need	Solution	Result
ACE4710 with 2 Gbps throughput <ul style="list-style-type: none"> • ACE-AP-02-LIC • Any combination of feature licenses 	Increased SSL, compression and/or VCs	Software upgrade to version A4(2.0)	<ul style="list-style-type: none"> • 2 Gbps throughput • 2 Gbps compression (limited by device throughput) • 7500 SSL TPS • 20 VCs
ACE4710 with 2 Gbps throughput <ul style="list-style-type: none"> • ACE-AP-02-LIC • Any combination of feature licenses 	Throughput upgrade to 4 Gbps	Start upgrade with ACE-4710-BUN-UPG3=	<ul style="list-style-type: none"> • 4 Gbps throughput • 2 Gbps compression • 7500 SSL TPS • 20 VCs
ACE4710 with 4 Gbps throughput <ul style="list-style-type: none"> • ACE-AP-04-LIC • Any combination of feature licenses 	Increased SSL, compression and/or VCs	Software upgrade to version A4(2.0)	<ul style="list-style-type: none"> • 4 Gbps throughput • 2 Gbps compression • 7500 SSL TPS • 20 VCs

Effects of Upgrading or Downgrading to or from Software Release A4(2.0) or Later

This section describes the licensing feature interactions when you upgrade to software version A4(2.0) and later, and then downgrade to software version A4(1.1), A3(2.7), or earlier.



Caution

If you migrate from software version A4(1.1) to A4(2.0), keep in mind that the new software features in A4(1.1) are not supported in A4(2.0) and you will lose those A4(1.1) features. However, you will gain the dynamic workload scaling (DWS) feature that is supported in A4(2.0). Conversely, if you migrate from software version A4(2.0) to software version A4(1.1), you will lose the DWS feature, but you will gain the 20 plus features that are new in software version A4(1.1). For details about the A4(1.1) features, see the *Release Note, Cisco 4700 Series ACE Application Control Engine Appliance* for software version A4(1.1). For details about the DWS feature, see the *Server Load-Balancing Guide, Cisco ACE Application Control Engine* for software version A4(2.0).

ACE Appliance with Software Release A4(1.1), A3(2.7), and Earlier Licenses

When you upgrade to software version A4(2.0) or later from an earlier version, you may obtain new feature capabilities (maximum limits for compression, SSL TPS, and the number of virtual contexts), depending on your current license levels, without having to buy new software licenses. After you have upgraded to software version A4(2.0), if you need to downgrade to an earlier software version, the earlier software version reverts to the earlier feature limits that you had prior to the upgrade. For example, if you acquired additional virtual contexts (a maximum of 20) when you upgraded to software version A4(2.0) or later, when you downgrade to software version A3(2.7), A4(1.1), or earlier, you lose those additional contexts and their configurations, and your contexts are limited again to a maximum of 5.

ACE Appliance with Software Release A4(2.0) and Later Licenses

ACE appliances that ship with software version A4(2.0) and later contain licenses that reflect the new maximum capabilities for compression, SSL TPS, and virtual contexts and vary only by bandwidth. Because these new licenses are backward compatible with earlier software versions, if you downgrade to an earlier version (for example, A4(1.1) or one of the A3(x) versions, the earlier software recognizes and retains the new licensing capabilities.

Ordering an Upgrade License and Generating a Key

This section describes how to order an upgrade license and generate a license key for your ACE. To order an upgrade license, follow these steps:

-
- Step 1** Order one of the available licenses using any of the available Cisco ordering tools on cisco.com.
- Step 2** When you receive the Software License Claim Certificate from Cisco, follow the instructions that direct you to the following Cisco.com website:
- If you are a registered user of cisco.com, go to the following location:
<http://www.cisco.com/go/license>
 - If you are not a registered user of cisco.com, go to the following location:
<http://www.cisco.com/go/license/public>
- Step 3** Enter the Product Authorization Key (PAK) number found on the Software License Claim Certificate as your proof of purchase.
- Step 4** Provide all the requested information to generate a license key. Once the system generates the license key, you will receive a license key e-mail with an attached license file and installation instructions.
- Step 5** Save the license key e-mail in a safe place in case you need it in the future (for example, to transfer the license to another ACE).
-

For information on installing and managing ACE licenses:

- Using the ACE CLI, see Chapter 3, Managing ACE Software Licenses, in the *Administration Guide, Cisco ACE Application Control Engine*.
- Using the ACE Device Manager, see Chapter 2, Configuring Virtual Contexts, in the *Device Manager Guide, Cisco ACE 4700 Series Application Control Engine Appliance*.
- Using ANM, see Chapter 5, Configuring Virtual Contexts, in the *User Guide, Cisco Application Networking Manager*.

Upgrading Your ACE Software in a Redundant Configuration

This procedure assumes that your ACE appliances are configured as redundant peers to ensure that there is no disruption to existing connections during the upgrade process. In the following procedure, the active ACE is referred to as ACE-1 and the standby ACE is referred to as ACE-2.

This section includes the following topics:

- [Upgrade Guidelines and Limitations](#)
- [Before You Begin](#)
- [Upgrade Procedure](#)

Upgrade Guidelines and Limitations

When you are upgrading the ACE, consider the following guidelines and limitations:

- All DM GUI browsers require that you enable cookies, JavaScript/scripting, Adobe Flash Player 9, and popup windows. Whenever you plan to upgrade the ACE appliance software, end clients will need to clear their browser cache of each client to properly use the DM GUI.
- During an upgrade of two redundant ACEs from software version A4(1.0) to software version A4(2.0) or later, while the two ACEs are in split mode with A4(1.0) running on the active ACE and A4(2.0) or later running on the standby, config sync is disabled because of a license incompatibility between the two versions. Do not make any configuration changes while the two ACEs are in split mode. If you make any configuration changes on the active ACE during this time, your changes are not synchronized to the standby and are lost.

After you complete the upgrade, config sync is automatically reenabled and works normally. To avoid this license incompatibility issue, you can install a 20-virtual context license before you upgrade your ACEs to software version A4(2.0) and later.

- In software version A4(2.0) and later, the maximum number of concurrent connections for optimization is reduced to 100 connections. If the ACE startup configuration contains the **concurrent-connections** command in optimize configuration mode, consider the following:
 - If you upgrade the ACE to version A4(2.0) or later, the ACE software ignores the configured command and sets it to 100 connections.
 - If you downgrade the ACE from version A4(2.0) or later, the command is removed from the startup configuration, and you must reconfigure it after the downgrade process is completed.
- In a redundant configuration, dynamic incremental sync is a form of config sync that copies configuration changes that you make on the active ACE to the standby ACE when the two ACEs are running the same version of software and when both ACEs are up. When you upgrade from one major release of ACE software to another major release (for example, from A3(2.0) to A4(1.0)) or later, dynamic incremental sync is automatically disabled only while the active ACE is running software version A4(1.0) and the standby ACE is running software version A3(2.0). See [Table 3](#).

We recommend that you do not make any configuration changes during this time and that you do not keep the ACEs in this state for a long time. However, if you must make configuration changes while the ACEs are in split mode, ensure that you manually synchronize to the standby ACE any configuration changes that you make on the active ACE. After you complete the software upgrade of both ACEs, a bulk sync occurs automatically to replicate the entire configuration of the new active ACE to the new standby ACE. At this time, dynamic incremental sync will be enabled again. For details about config sync, see Chapter 6, “Configuring Redundant ACEs” in the *Administration Guide, Cisco ACE Application Control Engine*.

Table 3 Redundancy Feature Availability Between Major ACE Software Versions

Platform	Active	Standby	Bulk Sync	Incr Sync	Conn Repl	Sticky Repl	Operation	Comments
Appliance	A3(x)	A5(x)	Yes	No	Yes	Yes	Upgrade	—
Appliance	A4(1.x)	A5(x)	Yes	No	Yes	Yes	Upgrade	—
Appliance	A4(2.x)	A5(x)	Yes	No	Yes	Yes	Upgrade	—
Appliance	A5(x)	A3(x)	Yes	No	Yes (IPv4 flows)	Yes (IPv4 flows)	Downgrade	Standby supports only IPv4
Appliance	A5(x)	A4(1.x)	Yes	No	Yes (IPv4 flows)	Yes (IPv4 flows)	Downgrade	Standby supports only IPv4
Appliance	A5(x)	A4(2.x)	Yes	No	Yes (IPv4 flows)	Yes (IPv4 flows)	Downgrade	Standby supports only IPv4

- Starting in version A1(8.0), the ACE introduced the STANDBY_WARM and WARM_COMPATIBLE redundancy states to handle any CLI incompatibility issue between peers during the upgrading and downgrading of the ACE software. When you upgrade or downgrade the ACE software in a redundant configuration with a different software version, the STANDBY_WARM and WARM_COMPATIBLE states allow the configuration and state synchronization process to continue on a best-effort basis. This basis allows the active ACE to synchronize configuration and state information to the standby ACE even though the standby ACE may not recognize or understand the CLI commands or state information. These states allow the standby ACE to come up with best-effort support. In the STANDBY_WARM state, as with the STANDBY_HOT state, configuration mode is disabled on the standby ACE and configuration and state synchronization continues. A failover from the active ACE to the standby ACE based on priorities and preemption can still occur while the standby is in the STANDBY_WARM state. When redundancy peers run on different version images, the SRG compatibility field of the **show ft peer detail** command output displays WARM_COMPATIBLE instead of COMPATIBLE. When the peer is in the WARM_COMPATIBLE state, the FT groups on standby go to the STANDBY_WARM state instead of the STANDBY_HOT state.

The following software version combinations in [Table 4](#) indicate whether the SRG compatibility field displays WARM_COMPATIBLE (WC) or COMPATIBLE (C):



Note By default, software versions are considered compatible unless they are explicitly declared as incompatible.

Table 4 Software Release Compatibility Matrix

Active ACE Software Version	Standby ACE Software Version												
	A3(2.1)	A3(2.2)	A3(2.3)	A3(2.4)	A3(2.5)	A3(2.6)	A3(2.7)	A4(1.0)	A4(1.1)	A4(2.0)	A4(2.1)	A4(2.2)	A5(1.0)
A3(2.1)	C	C	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC
A3(2.2)	C	C	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC
A3(2.3)	WC	WC	C	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC
A3(2.4)	WC	WC	WC	C	WC	WC	WC	WC	WC	WC	WC	WC	WC
A3(2.5)	WC	WC	WC	WC	C	WC	WC	WC	WC	WC	WC	WC	WC
A3(2.6)	WC	WC	WC	WC	WC	C	WC	WC	WC	WC	WC	WC	WC
A3(2.7)	WC	WC	WC	WC	WC	WC	C	WC	WC	WC	WC	WC	WC
A4(1.0)	WC	WC	WC	WC	WC	WC	WC	C	WC	WC	WC	WC	WC
A4(1.1)	WC	WC	WC	WC	WC	WC	WC	WC	C	WC	WC	WC	WC
A4(2.0)	WC	WC	WC	WC	WC	WC	WC	WC	WC	C	WC	WC	WC
A4(2.1)	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC	C	WC	WC
A4(2.2)	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC	C	WC
A5(1.0)	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC	WC	C

Before You Begin

Before you upgrade your ACE software, be sure that your ACE configurations meet the upgrade prerequisites in the following sections:

- [Changing the Admin Password](#)
- [Changing the www User Password](#)
- [Removing the duplex Command from the ACE Configuration](#)
- [Removing the Underscore Character from a Hostname](#)
- [Creating a Checkpoint](#)
- [Consideration for a Startup Configuration with Optimization Concurrent Connections](#)
- [Copying the Startup Configuration of Each Context](#)
- [Consideration for a Startup Configuration with Optimization Concurrent Connections](#)



Note

To upgrade from software version A1(8a) to A4(1.0) or later, you must first upgrade software version A1(8a) to A3(2.6). Then, upgrade software version A3(2.6) to A4(1.0) or later.



Note

If you are upgrading a redundant configuration from software version A3(2.x) or A4(1.0) to software version A4(2.0) or later, while the two ACEs are in split mode with the earlier software version running on the active ACE and software version A4(2.0) running on the standby, config sync is disabled because of a license incompatibility. If you make any configuration changes on the active ACE during this time, your changes are not synchronized to the standby and are lost. After you complete the upgrade, config sync is automatically reenabled. We recommend that you do not make any configuration changes while the two ACEs are in split mode.

Changing the Admin Password

Before you upgrade to ACE software version A3(1.0) or higher, you **must** change the default Admin password if you have not already done so. Otherwise, after you upgrade the ACE software, you will be able to log in to the ACE only through the console port.



Caution

If you do not change the Admin password prior to upgrading to ACE software version A3(1.0) or higher, configuration synchronization may fail and the context may not be in the STANDBY_HOT state.

For details on changing the default Admin password, do one of the following:

- From the CLI, see Chapter 1, Setting Up the ACE, in the *Administration Guide, Cisco ACE Application Control Engine*.
- From the Device Manager GUI, see Chapter 1, Overview, in the *Device Manager Guide, Cisco ACE 4700 Series Application Control Engine Appliance*.



Note

If your ACE is managed by the Cisco Application Networking Manager (ANM) software, you **must** change the Admin password on the ANM in the Primary Attributes page instead of the ACE CLI. From the ANM, click the **Change Password** button on the Primary Attributes page (**Config > Devices > System > Primary Attributes**).

Changing the www User Password

Before you upgrade the ACE software, you **must** change the default www user password if you have not already done so. Otherwise, after you upgrade the ACE software, the www user password will be disabled and you will not be able to use Extensible Markup Language (XML) to remotely configure an ACE until you change the default www user password.

For details on changing a user account password, see Chapter 2, Configuring Virtualization, in the *Virtualization Guide, Cisco ACE Application Control Engine*. In this case, the username is **www**.



Caution

If you do not change the www user password prior to upgrading the ACE software, the configuration synchronization may fail and the context may not be in the STANDBY_HOT state.

Removing the duplex Command from the ACE Configuration

As a result of a **duplex** command syntax change between A3(2.1) and A3(2.2), if your ACE configuration includes one or more Gigabit Ethernet ports that are configured for full or half duplex operation, before you upgrade from A3(2.1) to A3(2.2), or A3(2.2) to software version A3(2.3) or later, you must first remove the duplex configuration from the startup-configuration file on both the active ACE and standby (peer) ACE.

Perform the following configuration change on both the active ACE and standby (peer) ACE before you begin the upgrade procedure:

-
- Step 1** Use the **no** form of the **duplex** command in interface configuration mode to remove the duplex configuration from all configured Gigabit Ethernet ports.
 - Step 2** Use the **copy running-config startup-config** command to save the changes from the running-configuration file to the startup-configuration file.
-

After you complete the upgrade procedure, you can update the duplex settings for the configured Gigabit Ethernet ports using software version A3(2.3) or later. See Chapter 1, Configuring Ethernet Interfaces, in the *Routing and Bridging Guide, Cisco ACE Application Control Engine*.

Removing the Underscore Character from a Hostname

Before you upgrade the ACE appliance software from A3(2.0) to A4(1.0) or later as a result of addressing CSCsr90184, the underscore character (`_`) is no longer allowed in the hostname. As a result of this change, if you do not modify a hostname by removing the underscore character (`_`), after you perform an upgrade, the standby ACE remains in the STANDBY_COLD state because the configuration cannot synchronize with the illegal character.

Creating a Checkpoint

We strongly recommend that you create a checkpoint of the running-configuration of each context in your ACE. A checkpoint creates a snapshot of your configuration that you can later roll back to in case a problem occurs with an upgrade and you want to downgrade the software to a previous version. Use the **checkpoint create** command in Exec mode in each context for which you want to create a configuration checkpoint and name the checkpoint. For details about creating a checkpoint and rolling back a configuration, see the *Administration Guide, Cisco ACE Application Control Engine*.

Consideration for a Startup Configuration with Optimization Concurrent Connections

In software version 4(2.0) and later, the **concurrent-connections** command has been deprecated and the maximum number of concurrent connections for application acceleration has been reduced to 100 connections. If your startup configuration contains the **concurrent-connections** command in optimize configuration mode and you upgrade the ACE to software version A4(2.0) or later, the ACE software ignores the configured command and sets the number of connections to 100 connections. This number is not configurable.

Copying the Startup Configuration of Each Context

In addition to creating a checkpoint of the running-configuration of each context in your ACE, we also strongly recommend that you use the **copy startup-config** command to copy the startup configuration of each context to either:

- The disk0: file system on your ACE.
- An TFTP, FTP, or SFTP server.

Having a backup of the startup configuration of each context ensures that you can recover your ACE should an issue arise during the upgrade procedure. In that case, you can then downgrade and restore the existing startup configuration to your ACE. For more information about the **copy** command, see the *Administration Guide, Cisco ACE Application Control Engine*.

Upgrade Procedure



Note

Ensure that the preempt command is disabled before you start your upgrade.

To upgrade your ACE software in a redundant configuration, follow these steps:

- Step 1** Log in to both the active and standby ACEs. The Exec mode prompt appears.
- If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the Admin context. If necessary, log directly in to, or change to the Admin context.
- ```
ACE-1/Admin#
```
- Step 2** Save the running configurations of every context to their respective startup configurations by entering the **write memory all** command in Exec mode in the Admin context of each ACE.
- ```
ACE-1/Admin# write memory all
```
- Step 3** Create a checkpoint in each context of both ACEs by entering the **checkpoint create** command in Exec mode.
- ```
ACE-1/Admin# checkpoint create ADMIN_CHECKPOINT
ACE-1/Admin# changeto C1
ACE-1/C1# checkpoint create C1_CHECKPOINT
```
- Step 4** Copy the new software image to the image directory of each ACE (active and standby) by entering the **copy ftp**, **copy sftp**, or the **copy tftp** command in Exec mode. For example, to copy the image with the name c4710ace-t1k9-mz.A5\_1\_0.bin through FTP, enter:
- ```
ACE-1/Admin# copy ftp://server1/images/c4710ace-t1k9-mz.A5_1_0.bin image:
Enter source filename[/images/c4710ace-t1k9-mz.A5_1_0.bin]?
```

```

Enter the destination filename[]? [c4710ace-t1k9-mz.A5_1_0.bin] File already exists, do
you want to overwrite?[y/n]: [y]
Enter hostname for the ftp server[server1]?
Enter username[]? user1
Enter the file transfer mode[bin/ascii]: [bin] Enable Passive mode[Yes/No]: [Yes] no
Password:

```

- Step 5** Ensure that the new software image is present on both the active and standby ACEs by entering the **dir** command in Exec mode. For example, enter:

```

ACE-1/Admin# dir image:c4710ace-t1k9-mz.A4_2_0.bin
35913728 Oct 25 2010 01:17:01 c4710ace-t1k9-mz.A5_1_0.bin

Usage for image: filesystem
      828182528 bytes total used
      54165504 bytes free
      882348032 bytes total

```

- Step 6** Verify the current BOOT environment variable and configuration register setting by entering the **show bootvar** command in Exec mode. For example, enter:

```

ACE-1/Admin# show bootvar
BOOT variable = "image:c4710ace-t1k9-mz.A5_1_0.bin"
Configuration register is 0x1

```

- Step 7** Remove the existing image from the boot variable on ACE-1 by entering the **no boot system image:ACE_image** command in configuration mode. For example, to remove the A3(2.1) image, enter:

```

ACE-1/Admin# configure
Enter configuration commands, one per line. End with CNTL/Z.
ACE-1/Admin(config)# no boot system image:c4710ace-t1k9-mz.A3_2_1.bin

```

- Step 8** Configure ACE-1 to autoboot from the latest ACE appliance image. To set the boot variable and configuration register to 0x1 (perform auto boot and use startup-config file), use the **boot system image:** and **config-register** commands in configuration mode. For example, enter:

```

ACE-1/Admin(config)# boot system image:c4710ace-t1k9-mz.A5_1_0.bin
ACE-1/Admin(config)# config-register 0x1
ACE-1/Admin(config)# exit
ACE-1/Admin# show bootvar
BOOT variable = "image:c4710ace-t1k9-mz.A5_1_0.bin"
Configuration register is 0x1

```

- Step 9** On the standby ACE ACE (ACE-2), perform the following:

- Enter the **show running-config** command and ensure that all the changes made in the active ACE (ACE-1) are also reflected on the standby ACE.
- Enter the **show bootvar** command to verify that the boot variable was synchronized with ACE-1.

- Step 10** Verify the state of each ACE by entering the **show ft group detail** command in Exec mode. Upgrade the ACE that has its Admin context in the STANDBY_HOT state (ACE-2) first by entering the **reload** command in Exec mode.

```

ACE-2/Admin# reload
This command will reboot the system
Save configurations for all the contexts. Save? [yes/no]: [yes]

```

After ACE-2 boots up, it may take a few minutes to reach the STANDBY_WARM state again. Configuration synchronization is still enabled and the connections through ACE-1 are still being replicated to ACE-2.



Note We do not recommend that you make any changes to the ACE-1 configuration. At this point in the upgrade procedure with ACE-2 in the STANDBY_WARM state, any incremental commands that you add to the ACE-1 configuration may not be properly synchronized to the ACE-2 configuration. To make any changes to ACE-1, disable incremental sync on ACE-1 and manually synchronize the changes to ACE-2.

Step 11 After the standby ACE reboots, log in and perform the following actions to verify the state of the standby ACE:

- Enter the **show version** command in Exec mode to verify that the ACE has properly rebooted with the latest ACE appliance software image.
- Enter the **show ft group detail** command in Exec mode to verify that the standby ACE has recovered to a STANDBY_HOT state. If the standby ACE is running software version A3(2.2) or later, the state is STANDBY_WARM.

Step 12 Perform a graceful failover of all contexts from ACE-1 to ACE-2 by entering the **ft switchover all** command in Exec mode on ACE-1. ACE-2 becomes the new active ACE and assumes control of all active connections with no interruption to existing connections.

```
ACE-1/Admin# ft switchover all
```

Step 13 Upgrade ACE-1 by reloading it. Verify that ACE-1 enters the STANDBY_WARM state (this action may take several minutes) by entering the **show ft group detail** command in Exec mode.

Because the standby ACE has changed its state to either STANDBY_COLD or STANDBY_HOT, the configuration mode is enabled. The configuration is synchronized from ACE 2 (currently active) to ACE-1. If ACE-1 is configured with a higher priority and **preempt** is configured on the FT group, ACE-1 reasserts control after it has received all configuration and state information from ACE-2, making ACE-2 the new standby. ACE-1 becomes the active ACE again.

```
ACE-1/Admin# reload
This command will reboot the system
Save configurations for all the contexts. Save? [yes/no]: [yes]
```

Step 14 Verify that ACE-1 is in the ACTIVE state and ACE-2 is in the STANDBY_WARM state by entering the **show ft group detail** command in Exec mode.

Downgrading Your ACE Software in a Redundant Configuration

If you need to downgrade your ACE software to an earlier ACE software version, use the procedure that follows. This procedure assumes that your ACEs are configured as redundant peers to ensure that there is no disruption to existing connections during the downgrade process. In the following procedure, the active ACE is referred to as ACE-1 and the standby ACE is referred to as ACE-2.

Before You Begin

Before you downgrade your ACE software, be sure that your ACE meets the following downgrade prerequisites:

- Before you downgrade your ACE software, ensure that the following conditions exist:
 - Identical versions of the previous software image resides in the image: directory of both ACEs.

- The active ACE has a higher priority than the standby ACE and **preempt** is enabled on the FT group if you want the active ACE to remain active after the downgrade procedure.
- All DM GUI browsers require that you enable cookies, JavaScript/scripting, Adobe Flash Player 9, and popup windows. Whenever you plan to downgrade the ACE appliance software, end clients will need to clear their browser cache of each client to properly use the DM GUI.
- Starting in software version A4(2.0), the maximum number of concurrent connections for optimization is reduced to 100 connections. If your startup configuration contains the **concurrent-connections** command in optimize configuration mode and you downgrade the ACE from software version A4(2.0), this command is removed from the startup configuration. You must reconfigure it after the downgrade process is completed.
- If your ACE includes the 0.5-Gbps bundled license (ACE-4710-0.5F-K9) that is available with software version A3(2.0) or later, ensure that you first uninstall the 0.5-Gbps bundle prior to downgrading to an earlier ACE software version. The ACE defaults to the 1-Gbps license.



Note If you have installed one of the other available ACE license bundles in addition to the 0.5-Gbps bundled license, and you downgrade to an earlier software version without first uninstalling those bundled licenses, the ACE may not downgrade properly to the original system defaults. In this case, you may observe an inconsistent behavior in the system defaults of the ACE.

Downgrade Procedure

To downgrade your A4(2.0) or later ACE software to an earlier ACE software version in a redundant configuration, perform these steps:

- Step 1** If you have previously created checkpoints in your running-configuration files (highly recommended), roll back the configuration in each context on each ACE to the configuration defined by the checkpoint. For example:

```
ACE-1/Admin# checkpoint rollback CHECKPOINT_ADMIN
ACE-1/Admin# changeto C1
ACE-1/C1# checkpoint rollback CHECKPOINT_C1
```

Do the same on the other ACE. For information about creating checkpoints and rolling back configurations, see the *Administration Guide, Cisco ACE Application Control Engine*.

- Step 2** Configure ACE-1 to automatically boot from the earlier ACE software image. To set the boot variable and configuration register to 1, use the **boot system image:** and **config-register** commands in configuration mode. For example, enter:

```
ACE-1/Admin# config
ACE-1/Admin(config)# boot system image:c4710ace-mz.A3_2_7.bin
ACE-1/Admin(config)# config-register 1
ACE-1/Admin(config)# exit
ACE-1/Admin#
```

You can set up to two images through the **boot system** command. If the first image fails, the ACE tries to boot from the second image.



Note Use the **no boot system image:ACE_image** command to remove the configured A3(x.x) boot variable.

- Step 3** Verify that the boot variable was synchronized to ACE-2 by entering the following command on ACE-2:

```
ACE-2/Admin# show bootvar
BOOT variable = "disk0:c4710ace-mz.A3_2_7.bin"
Configuration register is 0x1
host1/Admin#
```

- Step 4** Verify the state of each ACE by entering the **show ft group detail** command in Exec mode. Downgrade first the ACE that has its Admin context in the STANDBY_HOT state (ACE-2) by entering the **reload** command.

```
ACE-2/Admin# reload
This command will reboot the system
Save configurations for all the contexts. Save? [yes/no]: [yes]
```

When ACE-2 loads the startup-configuration file, you may observe a few errors if you did not roll back the configuration to a checkpoint. These errors are harmless and occur because the ACE software does not recognize the A4(2.0) (or later) commands in the startup-configuration file.



Note Dynamic incremental sync is automatically disabled while the active ACE is running software version A4(2.0) or later and the standby ACE is running an earlier software version.

- Step 5** Perform a graceful failover of all contexts from ACE-1 to ACE-2 by entering the **ft switchover all** command in Exec mode on ACE-1. ACE-2 becomes the new active ACE and assumes control of all active connections with no interruption to existing connections.

```
ACE-1/Admin# ft switchover all
```

- Step 6** Reload ACE-1 with the same ACE software version as ACE-2. You may observe a few errors as ACE-1 loads the startup-configuration file.

```
ACE-1/Admin# reload
```

After ACE-1 boots up, it assumes the role of standby and enters the STANDBY_HOT state (this can take several minutes). You can verify the states of both ACEs by entering the **show ft group detail** command in Exec mode. Because the standby ACE has changed its state to either STANDBY_COLD or STANDBY_HOT, the configuration mode is enabled. The configuration is synchronized from ACE 2 (currently active) to ACE-1. If ACE-1 is configured with a higher priority and **preempt** is configured on the FT group, ACE-1 reasserts control after it has received all configuration and state information from ACE-2, making ACE-2 the new standby. ACE-1 becomes the active ACE again.

- Step 7** Enter the **write memory all** command in both ACEs to save the running-configuration files in all configured contexts to their respective startup-configuration files. This action eliminates future errors when the ACEs reload their startup-configuration files.

ACE Documentation Set

You can access the ACE documentation on www.cisco.com at:

http://www.cisco.com/en/US/products/ps7027/tsd_products_support_series_home.html

For information about installing and configuring the ACE, see the following documents on Cisco.com:

Document Title	Description
<i>Application Acceleration and Optimization Guide, Cisco ACE 4700 Series Application Control Engine Appliance</i>	Describes how to configure the web optimization features of the ACE appliance. This guide also provides an overview and description of those features.
Cisco ACE Application Control Engine Configuration Examples Wiki	Provides examples of common configurations for load balancing, security, SSL, routing and bridging, virtualization, and so on.
Cisco ACE Application Control Engine Troubleshooting Wiki	Describes the procedures and methodology in wiki format to troubleshoot the most common problems that you may encounter during the operation of your ACE.
<i>Command Reference, Cisco ACE 4700 Series Application Control Engine</i>	Provides an alphabetical list and descriptions of all CLI commands by mode, including syntax, options, and related commands.
<i>CSS-to-ACE Conversion Tool Guide, Cisco ACE 4700 Series Application Control Engine</i>	Describes how to use the CSS-to-ACE conversion tool to migrate Cisco Content Services Switches (CSS) running-configuration or startup-configuration files to the ACE.
<i>Device Manager Guide, Cisco ACE Application Control Engine Appliance</i>	Describes how to use the Device Manager GUI, which resides in flash memory on the ACE appliance, to provide a browser-based interface for configuring and managing the appliance.
<i>Hardware Installation Guide, Cisco ACE 4700 Series Application Control Engine Appliance</i>	Provides information about installing the ACE appliance.
<i>Getting Started Guide, Cisco ACE 4700 Series Application Control Engine Appliance</i>	Describes how to use the ACE appliance CLI and Device Manager GUI to perform the initial setup and configuration tasks.

Document Title	Description
<i>Routing and Bridging Guide, Cisco ACE Application Control Engine</i>	<p>Describes how to perform the following routing and bridging tasks on the ACE:</p> <ul style="list-style-type: none"> • Ethernet ports • VLAN interfaces • IPv6, including transitioning IPv4 networks to IPv6, IPv6 header format, IPv6 addressing, and supported protocols. • Routing • Bridging • Dynamic Host Configuration Protocol (DHCP)
<i>Security Guide, Cisco ACE Application Control Engine</i>	<p>Describes how to perform the following ACE security configuration tasks:</p> <ul style="list-style-type: none"> • Security access control lists (ACLs) • User authentication and accounting using a Terminal Access Controller Access Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS), or Lightweight Directory Access Protocol (LDAP) server • Application protocol and HTTP deep packet inspection • TCP/IP normalization and termination parameters • Network Address Translation (NAT)
<i>Server Load-Balancing Guide, Cisco ACE Application Control Engine</i>	<p>Describes how to configure the following server load-balancing features on the ACE:</p> <ul style="list-style-type: none"> • Real servers and server farms • Class maps and policy maps to load balance traffic to real servers in server farms • Server health monitoring (probes) • Stickiness • Firewall load balancing • TCL scripts
<i>SSL Guide, Cisco ACE Application Control Engine</i>	<p>Describes how to configure the following Secure Sockets Layer (SSL) features on the ACE:</p> <ul style="list-style-type: none"> • SSL certificates and keys • SSL initiation • SSL termination • End-to-end SSL
<i>System Message Guide, Cisco ACE Application Control Engine</i>	<p>Describes how to configure system message logging on the ACE. This guide also lists and describes the system log (syslog) messages generated by the ACE.</p>
<i>Virtualization Guide, Cisco ACE Application Control Engine</i>	<p>Describes how to operate your ACE in a single context or in multiple contexts.</p>

Document Title	Description
<i>Regulatory Compliance and Safety Information, Cisco ACE 4710 Application Control Engine Appliance</i>	Regulatory compliance and safety information for the ACE appliance.
<i>Release Note, Cisco ACE 4700 Series Application Control Engine Appliance</i>	Provides information about operating considerations, caveats, and command-line interface (CLI) commands for the ACE appliance.
<i>User Guide, Cisco Application Networking Manager</i>	Describes how to use the Cisco Application Networking Manager (ANM), a networking management application for monitoring and configuring network devices, including the ACE.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2011 Cisco Systems, Inc. All rights reserved.

