



# **Cisco Application Control Engine Module Virtualization Configuration Guide**

Software Version A2(1.0)

March 2008

## **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Text Part Number: OL-11870-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

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.

*Cisco Application Control Engine Module Virtualization Configuration Guide*  
© 2008 Cisco Systems, Inc. All rights reserved.



# CONTENTS

## **Preface** v

- Audience vi
- How to Use This Guide vi
- Related Documentation vii
- Symbols and Conventions ix
- Obtaining Documentation, Obtaining Support, and Security Guidelines xi
- Open Source License Acknowledgements xi

---

## **CHAPTER 1**

### **Overview** 1-1

- Contexts 1-2
- Domains 1-5
- Role-Based Access Control 1-6
- Resource Classes 1-9

---

## **CHAPTER 2**

### **Configuring Virtualization** 2-1

- Virtualization Configuration Quick Start 2-2
- Managing ACE Resources 2-4
  - Creating a Resource Class for Resource Management 2-4
  - Allocating Resources within a Resource Class 2-5
  - Changing the Resource Allocation of a Resource Class 2-14
- Configuring a Context 2-15
  - Creating a Context 2-15
  - Configuring a Context Description 2-15

- Configuring a VLAN for a Context 2-16
- Associating a Context with a Resource Class 2-17
- Changing the Resource Class of a Context 2-18
- Moving Between Contexts 2-18
- Creating and Configuring User Roles 2-19
- Creating and Configuring Domains 2-23
- Configuring a User 2-25
- Example of a Virtualization Configuration 2-27

---

**CHAPTER 3**

**Displaying Virtualization Configuration and Statistics 3-1**

- Displaying Context Configurations 3-2
- Displaying Domain Configurations 3-2
- Displaying Resource Class Configurations 3-2
- Displaying Role Configurations 3-3
- Displaying Context Information 3-3
- Displaying Resource Allocation 3-4
- Displaying Resource Usage 3-5
- Displaying User Roles 3-8
- Displaying Domains 3-9
- Displaying User Information 3-10
- Logging Out a User 3-12
- Clearing All Statistics in a Context 3-12

---

**INDEX**



# Preface

---

This guide describes how to configure a single context or multiple contexts on the Cisco Application Control Engine (ACE) module for the Catalyst 6500 series switches or a Cisco 7600 series router, hereinafter referred to as the switch or router, respectively.

Multiple contexts use the concept of virtualization to partition your ACE into multiple virtual devices or contexts. In addition, the guide describes how to use the virtualization feature tools to closely and efficiently manage the system resources and users of the ACE and the services that you provide to your customers.

This preface contains the following major sections:

- [Audience](#)
- [How to Use This Guide](#)
- [Related Documentation](#)
- [Symbols and Conventions](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)
- [Open Source License Acknowledgements](#)

# Audience

This guide is intended for the following trained and qualified service personnel who are responsible for configuring the ACE:

- Web master
- System administrator
- System operator

# How to Use This Guide

This guide is organized as follows:

Chapter	Description
<a href="#">Chapter 1, Overview</a>	Provides an overview of the basic concepts to partition your ACE into multiple virtual devices or contexts. It includes information about: <ul style="list-style-type: none"> <li>• Contexts</li> <li>• Domains</li> <li>• Role-Based Access Control (RBAC)</li> <li>• Resource Classes</li> </ul>
<a href="#">Chapter 2, Configuring Virtualization</a>	Describes how to configure the ACE to operate in either a single context or in multiple contexts, allocate resources, create domains, and create users and user roles.
<a href="#">Chapter 3, Displaying Virtualization Configuration and Statistics</a>	Describes how to display configuration and statistical information for the contexts configured on your ACE.

# Related Documentation

In addition to this document, the ACE documentation set includes the following:

<b>Document Title</b>	<b>Description</b>
<i>Release Note for the Cisco Application Control Engine Module</i>	Provides information about operating considerations, caveats, and command-line interface (CLI) commands for the ACE.
<i>Cisco Application Control Engine Module Hardware Installation Note</i>	Provides information for installing the ACE into the Catalyst 6500 series switch or a Cisco 7600 series router.
<i>Cisco Application Control Engine Module Getting Started Guide</i>	Describes how to perform the initial setup and configuration tasks for the ACE.
<i>Cisco Application Control Engine Module Administration Guide</i>	Describes how to perform the following administration tasks on the ACE: <ul style="list-style-type: none"> <li>• Setting up the ACE</li> <li>• Establishing remote access</li> <li>• Managing software licenses</li> <li>• Configuring class maps and policy maps</li> <li>• Managing the ACE software</li> <li>• Configuring SNMP</li> <li>• Configuring redundancy</li> <li>• Configuring the XML interface</li> <li>• Upgrading the ACE software</li> </ul>
<i>Cisco Application Control Engine Module Routing and Bridging Configuration Guide</i>	Describes how to configure the following routing and bridging features on the ACE: <ul style="list-style-type: none"> <li>• VLAN interfaces</li> <li>• Routing</li> <li>• Bridging</li> <li>• Dynamic Host Configuration Protocol (DHCP)</li> </ul>

Document Title	Description
<i>Cisco Application Control Engine Module Server Load-Balancing Guide</i>	<p>Describes how to configure the following server load-balancing features on the ACE:</p> <ul style="list-style-type: none"> <li>• Real servers and server farms</li> <li>• Class maps and policy maps to load balance traffic to real servers in server farms</li> <li>• Server health monitoring (probes)</li> <li>• Stickiness</li> <li>• Firewall load balancing</li> <li>• TCL scripts</li> </ul>
<i>Cisco Application Control Engine Module Security Configuration Guide</i>	<p>Describes how to configure the following ACE security features:</p> <ul style="list-style-type: none"> <li>• Security access control lists (ACLs)</li> <li>• 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</li> <li>• Application protocol and HTTP deep packet inspection</li> <li>• TCP/IP normalization and termination parameters</li> <li>• Network Address Translation (NAT)</li> </ul>
<i>Cisco Application Control Engine Module SSL Configuration Guide</i>	<p>Describes how to configure the following Secure Sockets Layer (SSL) features on the ACE:</p> <ul style="list-style-type: none"> <li>• SSL certificates and keys</li> <li>• SSL initiation</li> <li>• SSL termination</li> <li>• End-to-end SSL</li> </ul>

Document Title	Description
<i>Cisco Application Control Engine Module System Message Guide</i>	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.
<i>Cisco Application Control Engine Module Command Reference</i>	Provides an alphabetical list and descriptions of all CLI commands by mode, including syntax, options, and related commands.
<i>Cisco CSM-to-ACE Conversion Tool User Guide</i>	Describes how to use the CSM-to-ACE conversion tool to migrate Cisco Content Switching Module (CSM) running- or startup-configuration files to the ACE.
<i>Cisco CSS-to-ACE Conversion Tool User Guide</i>	Describes how to use the CSS-to-ACE conversion tool to migrate Cisco Content Services Switches (CSS) running- or startup-configuration files to the ACE.

## Symbols and Conventions

This publication uses the following conventions:

Convention	Description
<b>boldface font</b>	Commands, command options, and keywords are in <b>boldface</b> . Bold text also indicates a command in a paragraph.
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> . Italic text also indicates the first occurrence of a new term, book title, emphasized text.
{ }	Encloses required arguments and keywords.
[ ]	Encloses optional arguments and keywords.
{ x   y   z }	Required alternative keywords are grouped in braces and separated by vertical bars.

Convention	Description
[x   y   z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in <code>screen font</code> .
<b>boldface screen font</b>	Information you must enter in a command line is in <b>boldface screen font</b> .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Notes use the following conventions:



**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:



**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

For additional information about CLI syntax format, see *Cisco Application Control Engine Module Command Reference*.

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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>

## Open Source License Acknowledgements

The following acknowledgements pertain to this software license.

### OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

#### **OpenSSL License:**

© 1998-1999 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

**Original SSLeay License:**

© 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].



# CHAPTER 1

## Overview

---

You can operate your Cisco Application Control Engine (ACE) module in a single context or in multiple contexts. Multiple contexts use virtualization to partition your ACE into multiple virtual devices or contexts. Each context contains its own set of policies, interfaces, resources, and administrators. This feature provides you with the tools that will allow you to more closely and efficiently manage the system resources and users of the ACE, and the services that you provide to your customers.

By default, your ACE provides an Admin context and five user contexts, which allows you to use multiple contexts if you choose to configure them. To increase the number of user contexts (up to a maximum of 250), you must obtain a separate license from Cisco Systems. For details about licensing, see the *Cisco Application Control Engine Module Administration Guide*.

This chapter provides an overview of the basic concepts involved with virtualization. It includes the following major sections:

- [Contexts](#)
- [Domains](#)
- [Role-Based Access Control](#)
- [Resource Classes](#)

# Contexts

The virtualized environment is divided into objects called contexts. Each context behaves like an independent ACE with its own policies, interfaces, domains, server farms, real servers, and administrators. Each context can also have its own management VLAN that you can access using Telnet or Secure Shell (SSH). For information about configuring a management policy and applying it to an interface, see the *Cisco Application Control Engine Module Administration Guide*.

As the global administrator (Admin), you can configure and manage all contexts through the Admin context, which contains the basic settings for each virtual device or context. When you log in to the ACE using the console or Telnet through the supervisor engine, you are authenticated in the Admin context.

The Admin context is similar to other contexts. The difference is that when you log in to the Admin context (for example, using SSH), you have full system administrator access to the entire ACE and all contexts and objects within it. The Admin context provides access to network-wide resources, such as a syslog server or context configuration server. All global commands for the ACE settings, contexts, resource classes, and so on, are available only in the Admin context.

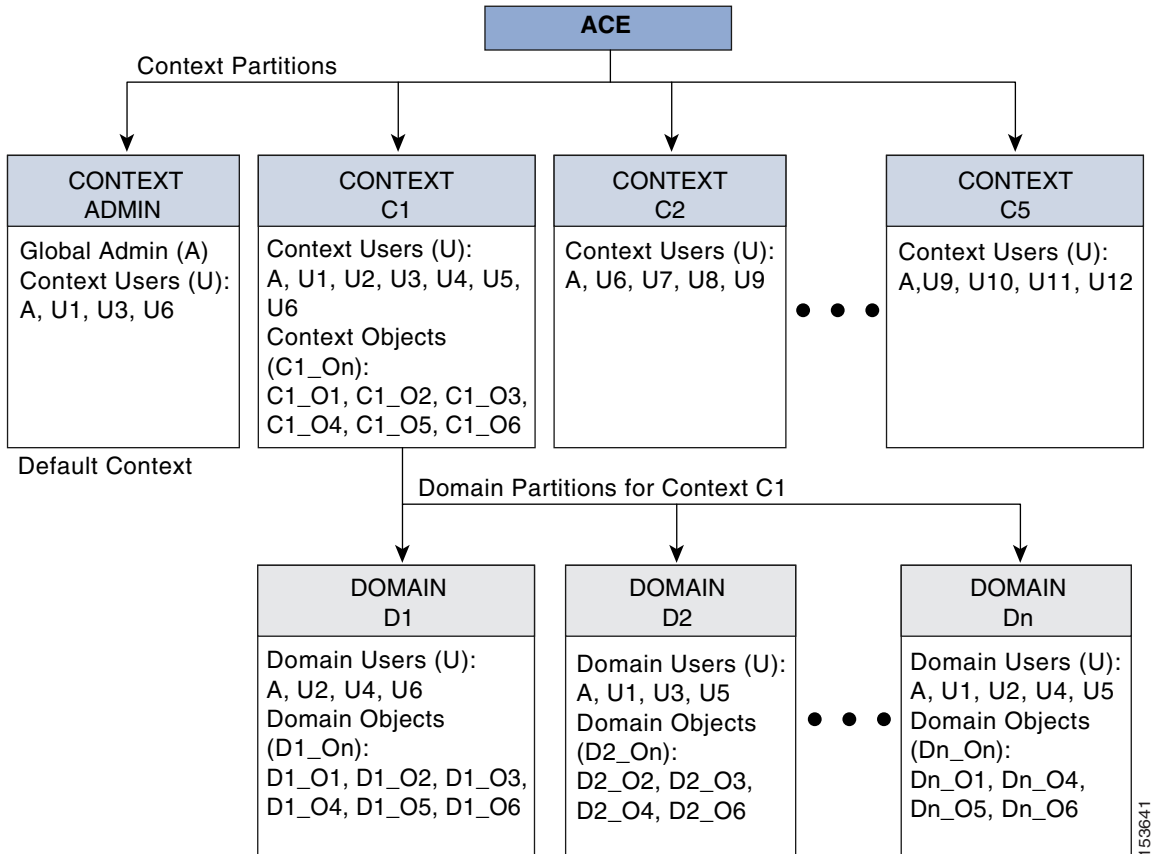
Each context, including the Admin context, has its own configuration file and local user database that are stored in the local disk partition on the flash disk or that can be downloaded from a File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), or HTTP(S) server. The startup-config file for each context is stored as the startup configuration file on the flash disk.

In the Admin context, use the **changeto** command in Exec mode or the **do changeto** command in configuration modes to move between contexts. Only users authenticated in the Admin context can use the **changeto** command.

For information about configuring a context, see [Chapter 2, Configuring Virtualization](#).

Figure 1-1 shows how you can use virtualization to create partitions that enable the ACE to function as multiple virtual devices.

Figure 1-1 ACE Virtualization Chart



153641

Each context that you create represents a virtual device. You can partition each context into domains for managing access to context resources. [Table 1-1](#) describes the various components of [Figure 1-1](#).

**Table 1-1 ACE Virtualization Elements**

Element	Description
Context ( <b>Cn</b> )	You can configure a single ACE to behave as multiple virtual devices by creating partitions called <i>contexts</i> . Each context functions as an independent device with its own set of users, objects, and allocated resources. By default, the ACE comes preconfigured with an Admin context and five configurable user contexts. To upgrade to a maximum of 250 user contexts, you must purchase a separate license from Cisco Systems. For more information about contexts, see the “ <a href="#">Contexts</a> ” section.
Domain ( <b>Dn</b> )	You can divide each context into multiple partitions called <i>domains</i> , which allow you to manage user access to the objects within a context. When you create a domain, you form an association between a select group of context users and a select group of context objects. For more information about domains, see the “ <a href="#">Domains</a> ” section.
User ( <b>A, Un</b> )	The ACE is preconfigured with a default global system administrator that provides access to all ACE functionality and allows you to create additional users. Any user that you create while you are in Admin context, by default, will have access to all resources in the ACE. Any user that you create while you are in a user-defined context will have access only to the resources within that context. You assign each user a role, which determines the commands and resources that are available to that user. For more information about users and user roles, see <a href="#">Chapter 2, Configuring Virtualization</a> .

**Table 1-1** ACE Virtualization Elements (continued)

Element	Description
Object ( <i>Cn_On</i> , <i>Dn_On</i> )	<p>The following objects are user-configurable items:</p> <ul style="list-style-type: none"> <li>• Access lists</li> <li>• Defined interfaces</li> <li>• Policy maps</li> <li>• Health probes</li> <li>• Real servers</li> <li>• Server farms</li> <li>• Scripts</li> <li>• Sticky groups</li> </ul> <p>The objects that you create are specific to the context that you are in while creating the object. If the context is partitioned into multiple domains, you allocate objects within each domain.</p>

## Domains

For management purposes, contexts are divided into objects called *domains* and each domain is fully contained within a context. A domain provides a namespace in which a user operates and each user is associated with at least one domain. The role assigned to a user determines the operations that a user can perform on the objects in a domain and the command set available to that user. When you create a context, the ACE automatically creates a default domain for that context.

The global admin or context administrators can create additional domains. A domain name must be unique within the context with which it is associated.

You can add any object that you can create (for example, a server farm, a real server, a probe, a VLAN, and so on) to a domain, and you can add an object to multiple domains. If you add an object that has other objects associated with it (for example, a server farm configured with real servers) to a domain, the associated objects do not automatically become part of the domain. You must add each object individually. When you create an object, the ACE automatically adds it to your domain.

**Note**

A domain does not restrict the context configuration that you can display using the **show running-config** command. However, a domain does restrict a user's access to configurable objects in the ACE. You can further restrict the operations that a user can perform on those configurable objects by assigning a role to a user. For information about user roles, see the [“Role-Based Access Control”](#) section.

For information about configuring a domain, see [Chapter 2, Configuring Virtualization](#).

## Role-Based Access Control

The ACE provides role-based access control (RBAC), which is a mechanism that determines the commands and resources available to each user. A role defines a set of permissions that allow you to access the objects and resources in a context and the actions that you can perform on them. The global or context administrator assigns roles to users based on their network function and the resources to which you want them to have access.

The ACE provides the following predefined roles that you cannot delete or modify:

- **Admin**—If created in the Admin context, has complete access to, and control over, all contexts, domains, roles, users, resources, and objects in the entire ACE. If created in a user context, this role gives a user complete access to and control over all the objects in that context. A context administrator can create, configure, and modify any object in that context, including policies, roles, domains, server farms, real servers, and so on.
- **Network Admin**—Complete access to and control over the following features:
  - Interfaces
  - Routing
  - Connection parameters
  - Network Address Translation (NAT)
  - VIPs
  - Copy configurations
  - **changeto** command

- Network-Monitor—Access only to the **changeto** command and **show** commands except for the following **show** commands:
  - **show bootvar**
  - **show capture**
  - **show cde**
  - **show cfgmgr**
  - **show crypto**
  - **show debug**
  - **show ft**
  - **show hyp**
  - **show inventory**
  - **show ipcp**
  - **show licences**
  - **show login**
  - **show processes**
  - **show tech-support**
  - **show telnet**
  - **show vlans**

If you do not explicitly assign a role to a user with the **username** command, this is the default role.

- Security-Admin—Complete access to and control over the following security-related features within a context:
  - Access control lists (ACLs)
  - Application inspection
  - Connection parameters
  - Interfaces (modify privileges only)
  - Authentication, authorization, and accounting (AAA)
  - NAT

- Copy configurations
  - **changeto** command
- Server-AppIn-Maintenance—Complete access to and control over the following features:
  - Real servers
  - Server farms
  - Load balancing
  - Copy configurations
  - **changeto** command
- Server-Maintenance—Real server maintenance, monitoring, and debugging for the following features:
  - Real servers—Modify permission
  - Server farms—Debug permission
  - VIPs—Debug permission
  - Probes—Debug permission
  - Load balancing—Debug permission
  - **changeto** command—Create permission
- SLB-Admin—Complete access to and control over the following ACE features within a context:
  - Real servers
  - Server farms
  - VIPs
  - Probes
  - Load balancing (Layer 3/4 and Layer 7)
  - NAT
  - Interfaces
  - Copy configurations
  - **changeto** command

- SSL-Admin—Administrator for all Secure Sockets Layer (SSL) features:
  - SSL—Create permission
  - Public key infrastructure (PKI)—Create permission
  - Interfaces—Modify permission
  - Copy configurations—Create permission
  - **changeto** command—Create permission

In addition to these predefined roles, Admins in any context can define new roles. For more information, see [Chapter 2, “Configuring Virtualization.”](#)

## Resource Classes

Resource classes allow you to manage context access to ACE resources, such as concurrent connections or bandwidth rate. The ACE is preconfigured with a default resource class that it applies to the Admin context and any user context upon creation. The default resource class is configured to allow a context to operate within a range that can vary from no resource access (0 percent) to complete resource access (100 percent).

When you use the default resource class with multiple contexts, you run the risk of oversubscribing ACE resources because the ACE permits all contexts to have full access to all of the resources on a first-come, first-served basis. When a resource is utilized to its maximum limit, the ACE denies additional requests made by any context for that resource.

To avoid oversubscribing resources and to help guarantee access to a resource by any context, the ACE allows you to create customized resource classes that you associate with one or more contexts. A context becomes a *member* of the resource class when you make the association. Creating a resource class allows you to set limits on the minimum and maximum amounts of each ACE resource that a member context is entitled to use. You define the minimum and maximum values as a percentage of the whole. For example, you can create a resource class that allows its member contexts access to no less than 25 percent of the total number of SSL connections that the ACE supports.

You can limit and manage the allocation of the following ACE resources:

- ACL memory
- Buffers for syslog messages and TCP out-of-order (OOO) segments

- Concurrent connections (through-the-ACE traffic)
- Management connections (to-the-ACE traffic)
- Proxy connections
- Set resource limit as a rate (number per second)
- Regular expression (regexp) memory
- SSL connections
- Sticky entries
- Static or dynamic network address translations (Xlates)

By default, when you create a context, the ACE associates the context with the default resource class. The default resource class provides resources of a minimum of 0 and a maximum of unlimited for all resources except sticky entries. For stickiness to work properly, you must explicitly configure a minimum resource limit for sticky entries by using the **limit-resource** command.

For more information about configuring and limiting resources, see [Chapter 2, Configuring Virtualization](#). For more information about stickiness, see the *Cisco Application Control Engine Module Server Load-Balancing Guide*.



## CHAPTER 2

# Configuring Virtualization

---

This chapter describes how to create and configure virtualization for your ACE. As the global administrator (SuperUser), you configure and manage all contexts through the Admin context, which contains the basic settings for each virtual device or context. Each context that you configure contains its own set of policies, interfaces, resources, and administrators.

This chapter contains the following major sections:

- [Virtualization Configuration Quick Start](#)
- [Managing ACE Resources](#)
- [Configuring a Context](#)
- [Moving Between Contexts](#)
- [Creating and Configuring User Roles](#)
- [Creating and Configuring Domains](#)
- [Configuring a User](#)
- [Example of a Virtualization Configuration](#)



### Note

By default, the ACE provides an Admin context and allows you to configure five user contexts. To create from 6 to a maximum of 250 user contexts, you must purchase a license from Cisco Systems. For details about licensing, see the *Cisco Application Control Engine Module Administration Guide*.

---

# Virtualization Configuration Quick Start

Table 2-1 provides a quick overview of the steps required to create and configure the virtualization feature. Each step includes the command-line interface (CLI) command required to complete the task.

**Table 2-1** *Virtualization Configuration Quick Start*

Task and Command Example
<p>1. Log in to the ACE as the global administrator using the console. By default, the console comes up with a single context called Admin.</p>
<p>2. Enter configuration mode.</p> <pre>host1/Admin# <b>config</b> Enter configuration commands, one per line. End with CNTL/Z. host1/Admin(config)#</pre>
<p>3. Configure a resource class to limit resources used by user contexts. For example, to limit the resources of a context to 10 percent of the total resources available, enter the following commands:</p>
<pre>host1/Admin(config)# <b>resource-class RC1</b> host1/Admin(config-resource)# <b>limit resource all minimum 10</b> <b>maximum equal-to-min</b> host1/Admin(config-resource)# <b>exit</b></pre>
<p>4. Create a new context.</p>
<pre>host1/Admin(config)# <b>context C1</b> host1/Admin(config-context)#</pre>
<p>5. Associate an existing VLAN with the context so that the context can receive traffic classified for it.</p>
<pre>host1/Admin(config-context)# <b>allocate-interface vlan 100</b></pre>
<p>6. Associate the context with the resource class that you created in Step 3.</p>
<pre>host1/Admin(config-context)# <b>member RC1</b></pre>
<p>7. Change to the C1 context that you created in Step 4 and enter configuration mode in that context.</p>
<pre>host1/Admin(config-context)# <b>do changeto C1</b> host1/C1(config-context)# <b>exit</b> host1/C1(config)#</pre>

**Table 2-1** *Virtualization Configuration Quick Start (continued)*

---

**Task and Command Example**

---

8. (Optional) Create a domain for the context.

```
host1/C1(config)# domain D1
host1/C1(config-domain)#
```

---

9. Allocate objects (for example, real servers, server farms, probes, ACLs, and so on) to the domain as needed.

```
host1/C1(config-domain)# add-object rserver SERVER1
```

---

10. (Optional) Create roles to define the object and resource permissions for different groups of users.

```
host1/C1(config)# role UR1
```

---

11. Create rules to define the role permissions.

```
host1/C1(config-role)# rule 1 permit create feature real
host1/C1(config-role)# rule 2 deny create feature acl
```

---

12. Configure users as required and associate roles and domains with the users.

```
host1/C1(config)# username user1 password 5 MYPASSWORD role UR1
domain D1
```

---

13. Verify the virtualization configuration by entering one of the following commands:

```
host1/C1# show running-config context
host1/C1# show running-config domain
host1/C1# show running-config resource-class
host1/C1# show running-config role
```

---

# Managing ACE Resources

You can allocate system resources to multiple contexts by creating and defining one or more resource classes and then associating the contexts with a resource class. The section contains the following topics:

- [Creating a Resource Class for Resource Management](#)
- [Allocating Resources within a Resource Class](#)
- [Changing the Resource Allocation of a Resource Class](#)

## Creating a Resource Class for Resource Management

You can create a resource class to allocate and manage system resources by one or more contexts. The ACE supports a maximum of 100 resource classes. After you create and configure the resource class, use the **member** command in context configuration mode to assign a resource class to the context (see the [“Associating a Context with a Resource Class”](#) section). To create a resource class, use the **resource-class** command in configuration mode. The syntax of the command is as follows:

```
resource-class name
```

For the *name* argument, enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/Admin(config)# resource-class RC1  
host1/Admin(config-resource)
```

To remove the resource class from the configuration, enter:

```
host1/Admin(config)# no resource-class RC1
```

When you remove a resource class from the ACE, any contexts that were members of that resource class automatically become members of the default resource class. The default resource class allocates a minimum of 0.00 percent to a maximum of 100.00 percent of all ACE resources to each context. You cannot modify the default resource class.

## Allocating Resources within a Resource Class

When you plan the initial resource allocations for the virtual contexts in your configuration, allocate only the minimum required or estimated resources. The ACE protects resources that are in use, so to decrease a context's resources, those resources must be unused. Although it is possible to decrease the resource allocations in real time, it may require additional management overhead to clear any used resources before reducing them. Therefore, it is considered a best practice to initially keep as many resources in reserve as possible and allocate the unused reserved resources as needed.

To address scaling and capacity planning, we recommend that new ACE installations do not exceed 60 to 80 percent of the module's total capacity. To accomplish this goal, create a reserved resource class with a guarantee of 20 to 40 percent of all the ACE resources and configure a virtual context dedicated solely to ensuring that these resources are reserved. Then, you can efficiently distribute such reserved resources to contexts as capacity demands for handling client traffic increase over time.

You can allocate all resources or individual resources to all member contexts of a resource class. For example, you can allocate only concurrent connections or sticky table memory or management traffic, to name a few. To allocate system resources to all members (contexts) of a resource class, use the **limit-resource** command in resource-class configuration mode.

The syntax of this command is as follows:

```
limit-resource { acl-memory | all | buffer { syslog } | conc-connections |  
  mgmt-connections | proxy-connections | rate { bandwidth |  
  connections | inspect-conn | mac-miss | mgmt-traffic | ssl-bandwidth |  
  syslog } | regexp | sticky | xlates } { minimum number } { maximum  
  { equal-to-min | unlimited } }
```

The arguments and keywords are as follows:

- **acl-memory**—Limits the memory space allocated for ACLs.
- **all**—Limits all resources to the specified value for all contexts assigned to this resource class, except for management traffic bandwidth. Management traffic bandwidth remains at the default values until you explicitly configure a minimum value for management traffic.
- **buffer**—Limits the number of syslog buffers.

- **conc-connections**—Limits the number of simultaneous connections.
- **mgmt-connections**—Limits the number of management (to-the-ACE) connections.
- **proxy-connections**—Limits the number of proxy connections.
- **rate**—Limits the resource as a number per second for the following:
  - **bandwidth**—Limits total ACE throughput in bytes per second for one or more contexts. The maximum bandwidth rate per context is determined by your bandwidth license. By default, the entry-level ACE has a 4-Gbps through-traffic bandwidth and a 1-Gbps management-traffic bandwidth for a total maximum bandwidth of 5 Gbps. You can upgrade the ACE with an optional 8-Gbps or 16-Gbps bandwidth license. With the 8-Gbps license, the ACE has a 8-Gbps through-traffic bandwidth and a 1-Gbps management-traffic bandwidth for a total maximum bandwidth of 9 Gbps.

When you configure a minimum bandwidth value for a resource class in the ACE, the ACE subtracts that configured value from the total bandwidth maximum value of all contexts in the ACE, regardless of the resource class with which they are associated. The total bandwidth rate of a context consists of the following two components:

**throughput**—Limits through-the-ACE traffic. This is a derived value (you cannot configure it directly) and it is equal to the **bandwidth** rate minus the **mgmt-traffic** rate for the 4-Gbps and 8-Gbps licenses. With a 16-Gbps license, this value is calculated slightly differently. For details, see the examples of the **show resource-usage** command output below.

**mgmt-traffic**—Limits management (to-the-ACE) traffic in bytes per second. This parameter is independent of the **limit-resource all minimum** command. To guarantee a minimum amount of management traffic bandwidth, you must explicitly allocate a minimum percentage to management traffic using the **limit-resource rate mgmt-traffic minimum** command. When you allocate a minimum percentage of bandwidth to management traffic, the ACE subtracts that value from the maximum available management traffic bandwidth for all contexts in the ACE. By default, management traffic is guaranteed a minimum bandwidth rate of 0 and a maximum bandwidth rate of 1 Gbps, regardless of which bandwidth license that you install in the ACE.

For details about how the ACE manages bandwidth for throughput and management traffic rates, see the examples of the **show resource-usage** command output that follow. For each bandwidth license, there are examples for the default values, 25 percent minimum allocation to all resources, and both a 25 percent minimum allocation to all resources and a 10 percent minimum allocation to management traffic. The output has been modified to show only the relevant fields. All values are in bytes per second; to convert to bits per second, multiply each value by 8.

```
switch/Admin# show resource usage
```

**Example 2-1 Default Show Resource Usage Command Output for 4-Gbps License**

Resource	Allocation	
	Min	Max
bandwidth	0	625000000
throughput	0	500000000
mgmt-traffic rate	0	125000000

**Example 2-2 Show Resource Usage Command Output for 4-Gbps License with 25 Percent Minimum Allocation for All Resources (continued)**

Resource	Allocation	
	Min	Max
bandwidth	125000000	500000000
throughput	125000000	375000000
mgmt-traffic rate	0	125000000

**Example 2-3 Show Resource Usage Command Output for 4-Gbps License with 25 Percent Minimum Allocation for All Resources and 10 Percent Minimum Allocation for Management Traffic**

Resource	Allocation	
	Min	Max
bandwidth	137500000	487500000
throughput	125000000	375000000
mgmt-traffic rate	12500000	112500000

**Example 2-4 Default Show Resource Usage Command Output for 8-Gbps License**

Resource	Allocation	
	Min	Max
bandwidth	0	1125000000
throughput	0	1000000000
mgmt-traffic rate	0	125000000

**Example 2-5 Show Resource Usage Command Output for 8-Gbps License with 25 Percent Minimum Allocation for All Resources**

Resource	Allocation	
	Min	Max
bandwidth	250000000	875000000
throughput	250000000	750000000
mgmt-traffic rate	0	125000000

**Example 2-6 Show Resource Usage Command Output for 8-Gbps License with 25 Percent Minimum Allocation for All Resources and 10 Percent Minimum Allocation for Management Traffic**

Resource	Allocation	
	Min	Max
bandwidth	262500000	862500000
throughput	250000000	750000000
mgmt-traffic rate	12500000	112500000

**Example 2-7 Default Show Resource Usage Command Output for 16-Gbps License**

Resource	Allocation	
	Min	Max
bandwidth	0	2000000000
throughput	0	2000000000
mgmt-traffic rate	0	125000000

**Example 2-8 Show Resource Usage Command Output for 16-Gbps License with 25 Percent Minimum Allocation for All Resources**

Resource	Allocation	
	Min	Max
bandwidth	500000000	1500000000
throughput	500000000	1500000000
mgmt-traffic rate	0	125000000

**Example 2-9 Show Resource Usage Command Output for 16-Gbps License with 25 Percent Minimum Allocation for All Resources and 10 Percent Minimum Allocation for Management Traffic**

Resource	Allocation	
	Min	Max
bandwidth	500000000	1500000000
throughput	487500000	1500000000
mgmt-traffic rate	12500000	112500000

- **connections**—Limits the number of connections per second of any kind.
- **inspect conn**—Limits the number of application protocol inspection connections per second for File Transfer Protocol (FTP) and Real-Time Streaming Protocol (RTSP) only.
- **mac-miss**—Limits the ACE traffic sent to the control plane when the encapsulation is not correct in bytes per second.
- **ssl-bandwidth**—Limits the number of SSL connections per second.
- **syslog**—Limits the number of syslog messages per second.
- **regexp**—Limits the amount of regular expression memory.
- **sticky**—Limits the number of entries in the sticky table. You must configure a minimum value for sticky to allocate resources for sticky database entries, because the sticky software receives no resources under the **unlimited** setting. You can allocate resources to sticky by either configuring a minimum percentage of resources specifically for sticky (**limit-resource sticky**) or by configuring a minimum percentage of resources for all (**limit-resource all**).
- **xlates**—Limits the number of network and port address translation entries.

- minimum number**—Specifies the lowest acceptable value for a resource. Enter an integer from 0.00 to 100.00 percent (two-decimal places of granularity). The *number* argument specifies a percentage value for all contexts that are members of the resource class. When used with the **rate** keyword, the *number* argument specifies a value per second. When you configure a minimum value for a resource in a particular resource class in the ACE, the ACE assigns the minimum resources only to the contexts that are members of the resource class. For all contexts, the ACE subtracts that configured minimum value from the maximum value of that resource, regardless of the resource class with which the contexts are associated. If the resource class has more than one context associated with it, the minimum value that the ACE subtracts from the maximum value is multiplied by the number of contexts in the resource class. For example, with a 4-Gbps bandwidth license, if there are two contexts associated with the resource class and you configure a 25 percent minimum allocation for the bandwidth rate for the class, each context in the resource class would have the values that are shown in [Example 2-10](#) for the **show resource usage** command output for the bandwidth rate and throughput rate.

**Example 2-10 Show Resource Usage Command Output for 4-Gbps License with 25 Percent Minimum Allocation for Bandwidth (continued)**

Resource	Allocation	
	Min	Max
bandwidth	125000000	375000000
throughput	125000000	250000000
mgmt-traffic rate	0	125000000

All other contexts in the ACE would have the same maximum values as shown in [Example 2-10](#), but would have zero minimum values. Compare the values in [Example 2-10](#) with the values in [Example 2-2](#), which represents one context in a resource class.

- maximum {equal-to-min | unlimited}**—Specifies the maximum resource value: either the same as the minimum value or no limit.

**Note**

The limit that you set for individual resources when you use the **limit-resource** command overrides the limit that you set for all resources when you use the **limit-resource all** command.

If you lower the limits for one context (context A) in order to increase the limits of another context (context B), you may experience a delay in the configuration change because the ACE will not lower the limits of context A until the resources are no longer being used by the context.

For example, to allocate 20 percent of all resources (minimum and maximum) to all member contexts of the resource class, enter:

```
(config-resource)# limit-resource all minimum 20% maximum equal-to-min
```

To restore resource allocation to the default values of 0 percent minimum and 100 percent maximum for all resources to all member contexts, enter:

```
(config-resource)# no limit-resource all
```

[Table 2-2](#) lists the managed system resources of the ACE. You can limit these resources per context or for all contexts associated with the resource class by using the **limit-resource** command. See the [“Allocating Resources within a Resource Class”](#) section.

**Table 2-2** System Resource Maximum Values

Resource	Maximum Value
ACL Memory	78,610,432 bytes
Buffer Memory (Syslog)	4,000,000 bytes
Concurrent Connections (Layer 4)	4,000,000 connections
Concurrent Connections (SSL)	200,000
Management Connections	100,000 connections
Proxy Connections (Layer 7)	524,286 connections
SSL Proxy Connections	200,000

**Table 2-2** System Resource Maximum Values (continued)

Resource	Maximum Value
Rate	
Bandwidth	4 gigabits per second (Gbps) You can upgrade the ACE maximum bandwidth to 8 Gbps or 16 Gbps by purchasing a separate license from Cisco Systems. For more information, see the <i>Cisco Application Control Engine Module Administration Guide</i> .
Connections (any kind)	325,000 connections per second
MAC miss	2000 packets per second
Management Traffic	1 Gbps
SSL transactions	1000 transactions per second (TPS), upgradeable to 15000 TPS with a separate license. For more information, see the <i>Cisco Application Control Engine Module Administration Guide</i> .
syslog	For traffic going to the ACE (control plane), 5000 messages per second For traffic going through the ACE (data plane), 350,000 messages per second
Regular Expression Memory	1,048,576 bytes
Sticky Entries	4,194,304 entries
Xlates (network and port address translation entries)	524,286 translations

## Changing the Resource Allocation of a Resource Class

If you (as the global Admin) need to change the resource allocation in a resource class of which two or more user contexts are members, you may do so at any time by entering the appropriate CLI commands. (For details about allocating resources, see the [“Allocating Resources within a Resource Class”](#) section.)

However, the shift in resources between the contexts does not take place immediately unless the appropriate resources are available to accommodate the change. In most cases, to effect a change in resource allocation, you must inform the context administrators involved to ensure that the new resource allocation is possible.

For example, suppose that context A is using 100 percent of the available resources of the class and you want to allocate 50 percent of the resources to context A and 50 percent of the resources to context B. Although the CLI accepts your resource allocation commands, context B cannot allocate 50 percent of the resources until context A deallocates 50 percent of its resources.

In this case, you must perform the following:

- Inform the Context A administrator to start deallocating resources
- Inform the Context B administrator to start allocating resources after the Context A administrator releases the resources



---

**Note**

As resources are released from other contexts, the ACE assigns the resources to resource-starved contexts (contexts where the resource-class minimum allocations have not been met).

---

# Configuring a Context

A context provides a user view into the ACE and determines the resources available to a user. This section contains the following topics:

- [Creating a Context](#)
- [Configuring a Context Description](#)
- [Configuring a VLAN for a Context](#)
- [Associating a Context with a Resource Class](#)
- [Changing the Resource Class of a Context](#)

## Creating a Context

To create a context, use the **context** command in configuration mode. The syntax of this command is as follows:

```
context name
```

The *name* argument is a unique identifier of the context. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, to create a context called C1, enter:

```
host1/Admin(config)# context C1  
host1/Admin(config-context)#
```

To remove the context from the configuration, enter:

```
host1/Admin(config)# no context C1
```

## Configuring a Context Description

You can enter a description for the context by using the **description** command in context configuration mode. The syntax of this command is as follows:

```
description text
```

For the *text* argument, enter a description as an unquoted text string with a maximum of 240 alphanumeric characters.

For example, enter:

```
host1/Admin(config-context)# description context for accounting users
```

To remove the context description from the configuration, enter:

```
host1/Admin(config-context)# no description
```

## Configuring a VLAN for a Context

The ACE uses class maps and policy maps to classify (filter) traffic and direct it to different interfaces (VLANs) using a service policy. A context uses VLANs to receive packets classified for that VLAN. To allocate one or more existing VLANs on which a user context can receive packets, use the **allocate-interface** command in context configuration mode in the Admin context. You can enter this command multiple times to specify multiple VLANs for a user context.



### Note

You can configure an interface directly in a user context, but the state of the interface remains Down until you enter the **allocate-interface** command for that interface in the Admin context. You can configure the interface and allocate the interface in any order.

The syntax of this command is as follows:

```
allocate-interface vlan number1
```

For the *number* argument, enter the number of an existing VLAN or a range of VLANs that you want to assign to the context as integers from 2 to 4094.



### Note

If you remove an interface in the Admin context and the same interface is in use in a user context, the state of the interface becomes Down. Entering the **show interface** command in the user context shows the interface as Down and the reason that the interface is no longer allocated in the Admin context.

For example, to allocate VLAN 100 to a context, enter:

```
host1/Admin(config-context)# allocate-interface vlan 100
```

To allocate an inclusive range of VLANs from VLAN 100 through VLAN 200 to a context, enter:

```
host1/Admin(config-context)# allocate-interface vlan 100-200
```

To deallocate a VLAN from a context, enter:

```
host1/Admin(config-context)# no allocate-interface vlan 100
```

To deallocate a range of VLANs from a context, enter:

```
host1/Admin(config-context)# no allocate-interface vlan 100-200
```

**Note**

---

You cannot deallocate a VLAN from a user context if the VLAN is in use in that context.

---

## Associating a Context with a Resource Class

Resource classes limit the resources available to one or more contexts. If you do not specify a resource class, the context automatically is a member of the default resource class. The default resource class allocates a minimum of 0.00 percent to a maximum of 100.00 percent of all ACE resources to each context. You can associate a context with only one resource class. For more information about resource classes, see the [“Creating a Resource Class for Resource Management”](#) section. To associate a context with a resource class, use the **member** command in context configuration mode.

The syntax of this command is as follows:

```
member class
```

For the *class* argument, enter the name of an existing resource class as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. For information about configuring a resource class, see the [“Creating a Resource Class for Resource Management”](#) section.

For example, to associate a context with the RC1 resource class, enter:

```
host1/Admin(config-context)# member RC1
```

To disassociate a context from the RC1 resource class, enter:

```
host1/Admin(config-context)# no member RC1
```

## Changing the Resource Class of a Context

To remove a context from a resource class, use the **no member** command in context configuration mode (see the [“Associating a Context with a Resource Class”](#) section). When you remove a context from a resource class, the ACE releases all resources associated with that context and makes the resources available to other contexts in the class.

To associate the same context with a different resource class, use the **member** command in context configuration mode (see the [“Associating a Context with a Resource Class”](#) section). When you add a context to a resource class, the ACE adds only those resources that can remain within their configured limits. If you want to allocate additional resources to the context, you can do so if the resources are available. Otherwise, you must first release some resources from other contexts within the resource class. For details about modifying the resource allocation among contexts, see the [“Changing the Resource Allocation of a Resource Class”](#) section.

## Moving Between Contexts

You can move between contexts by using the **changeto** command in Exec mode or the **do changeto** command in configuration mode. You must have one of the predefined user roles in the Admin context to use the **changeto** command. For information about the predefined user roles, see the [“Role-Based Access Control”](#) section in [Chapter 1, Overview](#). Context administrators, who have access to multiple contexts, must explicitly log in to the other contexts to which they have access.

Note the following operating considerations when moving between contexts:

- The user role that is enforced after you enter the **changeto** command is that of the Admin context and not that of the non-Admin context.
- You cannot add, modify, or delete objects in a custom domain after you change to a non-Admin context.
  - If you originally had access to the default-domain in the Admin context prior to moving to a non-Admin context, the ACE allows you to configure any object in the non-Admin context.

- If you originally had access to a custom domain in the Admin context prior to moving to a non-Admin context, any created objects in the new context will be added to the default-domain. However, an error message will appear when you attempt to modify existing objects in the non-Admin context.

The syntax of this command is as follows:

**changeto** *name*

The *name* argument specifies the identifier of an existing context. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/Admin# changeto C1
host1/C1#
```

## Creating and Configuring User Roles

User roles determine the privileges that a user has, the commands that a user can enter, and the actions that a user can perform in a particular context. For a list of the predefined roles that the ACE provides, see [Chapter 1, Overview](#). To display the predefined roles in the CLI, enter the **show role** command in Exec mode. The global administrator or a context administrator can configure additional roles. You can apply the roles that you create only in the context in which you create them.

To configure roles, use the **role** command in configuration mode. The syntax of this command is as follows:

**role** *name*

The *name* argument is an identifier associated with a role. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

If you do not assign a role to a new user, the default role is Network-Monitor. For users that you create in the Admin context, the default scope of access is the entire device. For users that you create in other contexts, the default scope of access is the entire context. If you need to restrict a user's access, you must assign a role-domain pair using the **username** command (see the “Configuring a User” section).

For example, enter:

```
host1/C1(config)# role TECHNICIAN
host1/C1(config-role)#
```

To remove the role from the configuration, enter:

```
host1/C1(config)# no role TECHNICIAN
```

After you create a user role, you can limit the features that a user has access to and the commands the user can enter for that feature by configuring rules for that role. To assign privileges per feature to a role, use the **rule** command in role configuration mode.

The syntax of this command is as follows:

```
rule number {permit | deny} {create | modify | debug | monitor} [feature
{AAA | access-list | config-copy | connection | dhcp | fault-tolerant |
inspect | interface | loadbalance | nat | pki | probe | real-inservice |
routing | rserver | serverfarm | ssl | sticky | syslog | vip}]
```

The keywords, arguments, and options are as follows:

- **number**—Identifier of the rule and order of precedence. Enter a unique integer from 1 to 16. The rule number determines the order in which the ACE applies the rules, with a higher-numbered rule applied after a lower-numbered rule.
- **permit**—Allows the role to perform the operations defined by the rest of the command keywords.
- **deny**—Disallows the role to perform the operations defined by the rest of the command keywords.
- **create**—Specifies commands for the creation of new objects or the deletion of existing objects (includes **modify**, **debug**, and **monitor** commands).
- **modify**—Specifies commands for modifying existing configurations (includes **debug** and **monitor** commands).

- **debug**—Specifies commands for debugging problems (includes **monitor** commands).
- **monitor**—Specifies commands for monitoring resources and objects (**show** commands).
- **feature**—(Optional) Specifies one of the following ACE features for configuring this rule:
  - **AAA**—Specifies commands for authentication, authorization, and accounting.
  - **access-list**—Specifies commands for access control lists (ACLs). Includes ACL configuration, class maps for ACL, and policy maps that contain ACL class maps.
  - **config-copy**—Specifies commands for copying the running-config file to the startup-config file, startup-config file to the running-config file, and copying both config files to the flash disk (disk0:) or a remote server.
  - **connection**—Specifies commands for network connections.
  - **dhcp**—Specifies commands for Dynamic Host Configuration Protocol.
  - **fault-tolerant**—Specifies commands for redundancy.
  - **inspect**—Specifies commands for packet inspection used in data-center security.
  - **interface**—Specifies all interface commands.
  - **loadbalance**—Specifies commands for load balancing. Allows adding a load-balancing action in a policy map.
  - **nat**—Specifies commands for Network Address Translation (NAT) associated with a class map in a policy map used in data-center security.
  - **pki**—Specifies commands for SSL public key infrastructure (PKI).
  - **probe**—Specifies commands for keepalives for real servers.
  - **real-inservice**—Specifies commands for placing a real server in service.
  - **routing**—Specifies all commands for routing, both global and per interface.
  - **rserver**—Specifies commands for physical servers.
  - **serverfarm**—Specifies commands for server farms.
  - **ssl**—Specifies commands for SSL.

- **sticky**—Specifies commands for server persistence.
- **syslog**—Specifies the system logging facility setup commands.
- **vip**—Specifies commands for virtual IP addresses and virtual servers.

For example, to configure a rule that allows a role to create and configure real servers, enter:

```
host1/C1(config-role)# rule 1 permit create rserver
```

To remove the rule from a role, enter:

```
host1/C1(config-role)# no rule 1 permit create rserver
```

# Creating and Configuring Domains

A domain is the namespace in which a user operates. When you create a context, the ACE automatically creates a default domain (default-domain) for that context. You can configure a maximum of 63 additional domains in each context. For information about configuring a context, see the “[Configuring a Context](#)” section. To create a domain, use the **domain** command in configuration mode. The syntax of this command is as follows:

**domain** *name*

For the *name* argument, enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, to create a domain called D1, enter:

```
host1/C1(config)# domain D1
host1/C1(config-domain)#
```

To remove a domain from the configuration, enter:

```
host1/C1(config)# no domain D1
```



## Note

---

A domain does not restrict the context configuration that you can display using the **show running-config** command. You can still display the running configuration for the entire context. However, a domain can restrict your access to the configurable objects within a context by adding only a limited subset of all the objects available to a context to the domain. You can further restrict the operations that a user can perform on those configurable objects by assigning a role to a user. For information about configuring user roles, see the “[Creating and Configuring User Roles](#)” section.

---

After you create a domain, you can associate configurable objects with that domain (for example, a real server, server farm, interface, and so on). To associate a configurable object with a domain, use the **add-object** command in domain configuration mode.

The syntax of this command is as follows:

```
add-object {access-list {ethertype | extended} | all | class-map | interface
{bvi | vlan} | parameter-map | policy-map | probe | rserver | script |
serverfarm | sticky} name
```

The keywords, arguments, and option are as follows:

- **access-list**—Specifies an existing access control list (ACL) that you want to associate with the domain.
- **all**—Specifies that all existing configuration objects in the context are added to the domain.
- **class-map**—Specifies an existing class map for flow classification that you want to associate with the domain.
- **interface**—Specifies an existing interface that you want to associate with the domain.
- **parameter-map**—Specifies an existing parameter map that you want to associate with the domain.
- **policy-map**—Specifies an existing policy map that you want to associate with the domain.
- **probe**—Specifies an existing real server probe (keepalive) that you want to associate with the domain.
- **rserver**—Specifies an existing real server that you want to associate with the domain.
- **script**—Specifies an existing script that you created with the ACE TCL scripting language.
- **serverfarm**—Specifies an existing server farm that you want to associate with the domain.
- **sticky**—Specifies an existing sticky group that you want to associate with the domain to maintain persistence with a server.
- *name*—Identifier of the specified object. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, to associate an interface called VLAN 10 with the domain, enter:

```
host1/C1(config-domain)# add-object interface vlan 10
```

To remove the object from the domain, enter:

```
host1/C1(config-domain)# no add-object interface vlan 10
```

# Configuring a User

The ACE creates two default user accounts at startup: admin and www. The admin user is the global administrator and cannot be deleted. The ACE uses the www user account for the XML interface and cannot be deleted.

The global administrator (admin) assigns one user in each context as the context administrator. The context administrator can then log in to the context or contexts for which he or she is responsible and create additional users.

If you do not assign a role to a new user, the default role is Network-Monitor. For users that you create in the Admin context, their default scope of access is the entire device. For users that you create in other contexts, their default scope of access is the entire context. If you need to restrict a user's access, you must assign a role-domain pair.

To create a user, use the **username** command in configuration mode. The syntax of this command is as follows:

```
username name1 [password [0 | 5] {password}] [expire date] [role name2  
{domain name3 name4 . . . namen}]
```

The keywords, arguments, and options are as follows:

- *name1*—Identifier of the user that you are creating. Enter an unquoted text string with no spaces and a maximum of 24 alphanumeric characters.
- **password**—(Optional) Keyword that indicates that a password follows.
- **0**—(Optional) Specifies a clear text password.
- **5**—(Optional) Specifies an MD5-hashed strong encryption password.

- *password*—(Optional) Password in clear text or MD5 strong encryption, depending on the numbered option (0 or 5) that you enter. If you do not enter a numbered option, the password is in clear text by default. If you enter the **password** keyword, you must enter a password. Enter a password as an unquoted text string with a maximum of 64 alphanumeric characters. The ACE supports the following special characters in a password:

, . / = + - ^ @ ! % ~ # \$ \* ( )

Note that the ACE encrypts clear text passwords in the running-config.




---

**Note** If you specify an MD5-hashed strong encryption password, the ACE considers a password to be weak if it is less than eight characters in length.

---

- **expire date**—(Optional) Specifies the expiration date of the user account. Enter the expiration date in the format *yyyy-mm-dd*.
- **role name2**—(Optional) Specifies an existing role that you want to assign to the user.
- **domain name3 name4 . . . namen**—Specifies the domains in which the user can operate. You can enter multiple domain names up to a maximum of 10, including **default-domain**.

For example, enter:

```
host1/C1(config)# username USER1 password MYSECRET expire 2005-12-31
role TECHNICIAN domain D1 default-domain
```

```
host1/C1(config)# username USER2 password HERSECRET expire 2005-12-31
role Admin domain default-domain D2
```

To delete a user from the configuration, enter:

```
host1/C1(config)# no username USER1
```

## Example of a Virtualization Configuration

The following running-configuration example shows a basic virtualization configuration with one user-defined context, one resource class, one domain, and one user.

```
resource-class RC1
  limit-resource rate syslog minimum 10.00 maximum equal-to-min
  limit-resource acl-memory minimum 10.00 maximum unlimited

access-list ACL1 line 10 extended permit ip any any

rserver host RS1
  ip address 192.168.2.251
  inservice
rserver host RS2
  ip address 192.168.2.252
  inservice
serverfarm host SF1
  rserver RS1
    inservice
  rserver RS2
    inservice

domain D1
  add-object access-list extended ACL1
  add-object rserver RS1
  add-object rserver RS2
  add-object serverfarm SF1

role SLB-Admin

context C1
  allocate-interface vlan 100-200
  description accounting department
  member RC1

username JANE password 5 adropgijaeprgja9erjg2uWgtce1 role SLB-Admin
  domain D1
```

■ Example of a Virtualization Configuration



## CHAPTER 3

# Displaying Virtualization Configuration and Statistics

---

This chapter describes the **show** commands that allow you to display a range of configuration and statistical information for the contexts configured on your Cisco Application Control Engine (ACE) module.

This chapter contains the following major sections:

- [Displaying Context Configurations](#)
- [Displaying Domain Configurations](#)
- [Displaying Resource Class Configurations](#)
- [Displaying Role Configurations](#)
- [Displaying Context Information](#)
- [Displaying Resource Allocation](#)
- [Displaying Resource Usage](#)
- [Displaying User Roles](#)
- [Displaying Domains](#)
- [Displaying User Information](#)
- [Logging Out a User](#)
- [Clearing All Statistics in a Context](#)

## Displaying Context Configurations

You can display context configurations by using the **show running-config context** command in Exec mode. This command displays all configured user contexts and their descriptions, resource classes, and allocated VLANs. The syntax of this command is as follows:

```
show running-config context
```

For example, enter:

```
host1/Admin# show running-config context
```

## Displaying Domain Configurations

You can display domain configurations by using the **show running-config domain** command in Exec mode. This command displays all configured domains and their objects (access control lists [ACLs], class maps, interfaces, and so on). The syntax of this command is as follows:

```
show running-config domain
```

For example, enter:

```
host1/Admin# show running-config domain
```

## Displaying Resource Class Configurations

You can display resource-class configurations by using the **show running-config resource-class** command in Exec mode. This command displays all configured resource classes and their resource allocation statements. The syntax of this command is as follows:

```
show running-config resource-class
```

For example, enter:

```
host1/Admin# show running-config resource-class
```

## Displaying Role Configurations

You can display role configurations by using the **show running-config role** command in Exec mode. This command displays all configured roles, their descriptions, and associated rules. The syntax of this command is as follows:

```
show running-config role
```

For example, enter:

```
host1/Admin# show running-config role
```

## Displaying Context Information

You can display a list of contexts including the name, description, resource class, and interfaces by using the **show context** command in Exec mode. The syntax of this command is as follows:

```
show context name
```

For the *name* argument, enter the unique identifier of an existing context as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/Admin# show context C1
```

[Table 3-1](#) describes the fields in the **show context** command output.

**Table 3-1** Field Descriptions for the **show context** Command Output

Field	Description
Name	Lists identifiers of all configured contexts. If you specify the <i>name</i> argument, the ACE displays the name of the context that you specify only.
Description	Previously configured text description of the context.
Resource-class	Resource class of which the context is a member.
VLANs	VLANs allocated to a user context from the Admin context.

# Displaying Resource Allocation

You can view the allocation for each resource across all resource classes and class members by using the **show resource allocation** command in Exec mode. The syntax of this command is as follows:

## **show resource allocation**

This command shows the resource allocation but does not show the actual resources being used. See the “[Displaying Resource Usage](#)” section for more information about actual resource usage.

For example, enter:

```
host1/Admin# show resource allocation
```

[Table 3-2](#) describes the fields in the **show resource allocation** command output.

**Table 3-2** *Field Descriptions for the show resource allocation Command Output*

Field	Description
Parameter	Name of the resource that you can limit. See <a href="#">Chapter 2, Configuring Virtualization</a> , for more information about each resource name.
Min	Minimum percentage of the total system resources that is allocated for a parameter in the specified resource class. For the default resource class, the minimum value for each resource is 0.00 percent.
Max	Maximum percentage of the total system resources that is allocated to a parameter in the specified resource class. For the default resource class, the Max value for each resource is equal to the total Max value of all contexts using the default resource class. For example, if you configure two user contexts and do not associate them with a resource class, the ACE automatically assigns the default resource class. If the Admin context also uses the default resource class, the Max value would equal 300% for each resource.
Class	Name of the resource class.

# Displaying Resource Usage

You can display the resource usage for each context from the Admin context by using the **show resource usage** command in Exec mode. The syntax of this command is as follows:

```
show resource usage [all | [[context name | summary | top number]
[resource {acl-memory | all | conc-connections | mgmt-connections |
probes | proxy-connections | rate {bandwidth | connections |
inspect-conn | mac-miss | mgmt-traffic | ssl-connections | syslog} |
regex | sticky | syslogbuffer | xlates}]]] [counter [all | current | denied
| peak [count_threshold]]]
```

The keywords, arguments, and options are as follows:

- **all**—(Optional) Displays the resource usage for each context individually. This is the default setting.
- **context name**—(Optional) Displays the resource usage for the specified context. The *name* argument is case sensitive.
- **summary**—(Optional) Displays the total resource usage for all contexts. For example, the denied column shows the items that have been denied for each context limit.
- **top number**—(Optional) Displays the greatest *n* users of a single resource arranged from the highest to the lowest percentage of resources used. You must specify a single resource type. You cannot use the **resource all** keywords with this option.
- **resource**—(Optional) Displays statistics for one of the following specified resources:
  - **acl-memory**—Displays the ACL memory usage.



## Note

If a context has fewer ACL memory resources than the configured Allocation Minimum, the ACE displays the Actual Minimum value that you can assign to the context.

- **all**—Displays the resource usage for all resources used by the specified context or contexts.
- **conc-connections**—Displays the resource usage for the number of simultaneous connections.

- **mgmt-connections**—Displays the resource usage for the number of management connections.
- **probes**—Displays the resource usage for the probes.
- **proxy-connections**—Displays the resource usage for the proxy connections.
- **rate**—Displays the rate per second for the specified connections or syslog messages.
- **regexp**—Displays the resource usage for regular expressions.




---

**Note** If a context has fewer regexp resources than the configured Allocation Minimum, the ACE displays the Actual Minimum value that you can assign to the context.

---

- **sticky**—Displays the resource usage for the sticky entries.




---

**Note** If a context has fewer sticky resources than the configured Allocation Minimum, the ACE displays the Actual Minimum value that you can assign to the context.

---

- **syslogbuffer**—Displays the resource usage for the syslog buffer. To free up syslog buffers, use the **clear logging** command.




---

**Note** The ACE assigns syslog buffers in increments of 1024. If the resource-class Allocation Minimum value was satisfied, then the Current field of the **show resource usage syslogbuffer** command would display the highest multiple of 1024 that is less than the Allocation Min value.

---

- **xlates**—Displays the resource usage by Network Address Translation (NAT) and Port Address Translation (PAT) entries.
- **counter**—(Optional) Specify one of the following keywords as the counter name:
  - **all**—(Optional) Displays all statistics. This is the default setting.
  - **current**—(Optional) Displays the active concurrent instances or the current rate of the resource.

- **denied**—(Optional) Displays the number of denied uses of the resource since the resource statistics were last cleared.
- **peak**—(Optional) Displays the peak concurrent instances, or the peak rate of the resource since the statistics were last cleared, either by using the **clear resource usage** command or because the device rebooted.
- *count\_threshold*—(Optional) Number above which resources are shown. Enter an integer from 0 to 4294967295. The default is 1. If the usage of the resource is below the number that you set, then the resource is not shown. If you specify **all** for the counter name, then the *count\_threshold* applies to the current usage. To show all resources, set the *count\_threshold* to **0**.

For example, enter:

```
host1/Admin# show resource usage context C1 resource conc-connections
counter denied 0
```

Table 3-3 describes the fields in the **show resource usage** command output.

**Table 3-3** *Field Descriptions for the show resource usage Command Output*

Field	Description
Resource	The name of the limited resource in each context. See <a href="#">Chapter 2, Configuring Virtualization</a> , for more information about each resource name.
Current	Active concurrent instances or the current rate of the resource.
Peak	Highest value of resource usage.
Allocation (Min/Max)	Allocation minimum value indicates the resource units that are guaranteed to be available to each context. The allocation maximum value indicates the resource units that may be available to each context and are shared among all contexts from the oversubscription pool. When you configure the maximum value as <b>equal-to-minimum</b> , the maximum value is automatically set to 0. When the allocation maximum value is 0, no additional resource units are available beyond the allocation minimum value to each context.

**Table 3-3** *Field Descriptions for the show resource usage Command Output (continued)*

Field	Description
Denied	Number of denied resources because of oversubscription or resource depletion.
Actual Min	Minimum ACL, regexp, sticky, or syslog buffer resources that you can allocate to the context if the resource-class minimum cannot be met.



**Note**

The **show resource usage** command 100 percent Allocation Min and Allocation Max values for conc-connections, proxy-connections, and other parameters display the bidirectional connections (inbound leg and outbound leg) for both IXP processors in the ACE. For example, the maximum number of concurrent connections that the ACE supports is 4,000,000, but the **show resource usage** command displays a maximum conc-connections value of 8000000, which is equal to 4,000,000 unidirectional connection records for each network processor times two network processors.

## Displaying User Roles

You can display the roles (predefined and user-configured) by using the **show role** command. The syntax of this command is as follows:

```
show role [name]
```

For the optional *name* argument, enter the unique identifier of the role as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. This parameter displays only the named role that you specify. To display all roles, enter the command without a name.

For example, to display all roles, enter:

```
host1/C1# show role
```

Table 3-4 describes the fields in the **show role** command output.

**Table 3-4** Field Descriptions for the **show role** Command Output

Field	Description
Role	Name of the role (for example, Admin).
Description	Text that describes the role (for example, Administrator).
Number of Rules	Number of rules associated with the role.
Rule	Sequence number of the rule.
Type	Type of rule. Possible values are Permit or Deny.
Permission	Permission level of the rule. The possible permission values ranked from highest to lowest are Create, Modify, Debug, and Monitor.
Feature	Software feature associated with the rule (for example, access-list).

## Displaying Domains

You can display information about the configured domains in the ACE by using the **show domain** command. The syntax of this command is as follows:

```
show domain [name]
```

For the optional *name* argument, enter the unique identifier of an existing domain as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/C1# show domain D1
```

Table 3-5 describes the fields in the **show domain** command output.

**Table 3-5** *Field Descriptions for the show domain Command Output*

Field	Description
Name	Unique identifier of the domain.
Object Type	List of objects associated with the domain (for example, Class-map).
Object Name	Configured identifier of the object.

## Displaying User Information

You can display information for users who are currently logged in to the ACE by using the **show users** command. The syntax of this command is as follows:

```
show users [name]
```

For the optional *name* argument, enter the unique identifier of a user as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/Admin# show users admin
```

Table 3-6 describes the fields in the **show users name** command output.

**Table 3-6** *Field Descriptions for the show users name Command Output*

Field	Description
User	Name of user.
Context	Name of the context associated with the user.
Line	Port through which the user connected to the ACE (for example, pts/1).
Login Time	Month, day, and time that the user logged in to the ACE (for example, Dec 7 20:11).

**Table 3-6** *Field Descriptions for the show users name Command Output (continued)*

Field	Description
Location	Location of the user expressed as an IP address.
Role	Role assigned to the user (for example, Admin).
Domain(s)	Domain associated with the user (for example, default-domain).

To display user account information, use the **show user-account** command in Exec mode. The syntax of this command is as follows:

**show user-account** *name*

For the optional *name* argument, enter the unique identifier of a user as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/Admin# show user-account admin
```

[Table 3-7](#) describes the fields in the **show user-account** command output.

**Table 3-7** *Field Descriptions for the show user-account Command Output*

Field	Description
User	Name of the user.
Account Expiry	Date, if any, that the user account expires.
Roles	Role assigned to the user (for example, Admin).
Domain	Domain associated with the user (for example, default-domain).
Context	Name of the context associated with the user (for example, Admin).

## Logging Out a User

You can force a user to log out (clear the user session) by using the **clear user** command in Exec mode. The syntax of this command is as follows:

```
clear user name
```

For the *name* argument, enter the name of an existing user as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, to log out the user named John, enter:

```
host1/Admin# clear user John
```

## Clearing All Statistics in a Context

You can clear all statistical information in a context by using the **clear stats all** command in Exec mode. The syntax of this command is as follows:

```
clear stats all
```

For example, to clear all statistical information for context C1, enter:

```
host1/Admin# clear statistics all
```



## INDEX

---

### A

#### Admin

- context [1-2](#)
- description [1-2, 1-6](#)
- permissions [1-6](#)

admin user [2-25](#)

---

### C

#### configurational examples

- virtualization [2-27](#)

#### context

- Admin [1-2](#)
- associating with a resource class [2-17](#)
- configuration, displaying [3-2](#)
- configuration file [1-2](#)
- configuring [2-1, 2-15](#)
- database [1-2](#)
- description [1-2, 1-4, 2-15](#)
- diagram [1-4](#)
- displaying information [3-3](#)
- domains [1-4, 1-5](#)
- moving from one to another [1-2, 2-18](#)

- overview [1-1](#)
- startup-config [1-2](#)
- user role [1-4, 2-19](#)
- users, configuring [2-25](#)
- VLANs, configuring [2-16](#)

---

### D

#### default user

- admin [2-25](#)
- www [2-25](#)

#### domain

- configuration, displaying [3-2](#)
- configuring [2-23](#)
- default [2-23](#)
- description [1-5](#)
- diagram [1-4](#)
- function within a context [1-4](#)
- information, displaying [3-9](#)
- name [1-5](#)

---

### L

- license for user contexts [1-1, 2-1](#)

logging

logging out a user [3-12](#)

---

## N

Network Admin

description [1-6](#)

permissions [1-6](#)

Network-Monitor

description [1-7](#)

permissions [1-7](#)

---

## O

object

association with contexts and domains [1-5](#),  
[2-23](#)

configuring [2-23](#)

description [1-5](#), [2-23](#)

---

## Q

quick start

virtualization configuration [2-2](#)

---

## R

RBAC

description [1-6](#)

predefined user roles [1-6](#)

resource class

associating a context [2-17](#)

configuration, displaying [3-2](#)

creating [2-4](#)

customized [1-9](#)

default [1-9](#), [2-4](#), [2-17](#)

description [1-9](#)

resources

allocation, displaying [3-4](#)

customizing for contexts [1-9](#)

list of managed [2-12](#)

managing [2-4](#)

usage, monitoring [3-5](#)

role

configuration, displaying [3-3](#)

displaying [3-8](#)

predefined [1-6](#)

rules, defining [2-20](#)

role-based access control

See RBAC [1-6](#)

rule, defining for a user role [2-20](#)

---

## S

Security-Admin

description [1-7](#)

permissions [1-7](#)

## Server-AppIn-Maintenance

description [1-8](#)

permissions [1-8](#)

## Server-Maintenance

description [1-8](#)

permissions [1-8](#)

## SLB-Admin

description [1-8](#)

permissions [1-8](#)

## SSL-Admin

description [1-9](#)

permissions [1-9](#)

## statistics

clearing [3-12](#)

displaying for virtualization [3-1](#)

within a context [1-4, 2-19](#)

---

## V

### virtualization

configuration quick start [2-2](#)

configuring [2-1](#)

diagram [1-3](#)

displaying configuration and statistics [3-1](#)

example configuration [2-27](#)

overview [1-1](#)

statistics, clearing [3-12](#)

### VLANs

configuring for a context [2-16](#)

---

## W

www user [2-25](#)

---

## U

### user

configuring [2-25](#)

displaying information [3-10](#)

session, clearing [3-12](#)

### user role

configuration, displaying [3-3](#)

configuring [2-19](#)

default [2-20, 2-25](#)

displaying [3-8](#)

predefined [1-6, 2-20](#)

rules, defining [2-20](#)

