

# Cisco ACE Application Control Engine Module Software Release 2.3.0

PB458841

The Cisco® ACE Application Control Engine Module for the Cisco Catalyst® 6500 Series Switches and Cisco 7600 Series Routers represents the next-generation of application switches for increasing the availability, accelerating the performance, and enhancing the security of data center applications. The Cisco ACE Module allows enterprises and service providers to accomplish four primary IT objectives for application delivery:

- Increase application availability
- Accelerate application performance
- Secure the data center and critical business applications
- Facilitate data center consolidation through the use of fewer servers and load balancers

## New Features

Cisco ACE Module Software Release 2.3.0 includes the following features, summarized in Table 1:

- New management and reporting capabilities
  - Secure backup and restore of Cisco ACE Module files
  - Enhanced Simple Network Management Protocol (SNMP) MIB support
  - Bulk copy for SSL certificate and key files
  - Granular reporting of HTTP URL hits on a virtual IP address<sup>1</sup>
  - New syslog messages for Network Address Translation (NAT)<sup>1</sup>

### Comprehensive suite of SSL offload features

- HTTP header insert for SSL information
- HTTP redirect on client authentication failure
- Lightweight Directory Access Protocol (LDAP)-based certificate revocation list (CRL) retrieval<sup>1</sup>
- CRL checking of SSL server certificates<sup>1</sup>
- Sample SSL key and certificate
- Scalability, load-balancing, and networking enhancements
  - Enhanced scalability for global server load balancing (GSLB) with Cisco Global Site Selector (GSS) Software<sup>1</sup>
  - Persistence rebalance for HTTP GET requests on the same TCP connection
  - Support for secondary IP addresses on an interface VLAN

<sup>1</sup> This feature was first introduced in Cisco ACE Module Software Release 2.2.0.

**Table 1.** New Features in Cisco ACE Module Software Release 2.3.0

| Feature   | Description   | Benefit  |
|---|---|--|
| <b>Secure backup and restore of Cisco ACE Module files</b>                | The Cisco ACE Module can securely back up and restore the startup configuration, running configuration, checkpoints, license files, and SSL keys and certificate files across multiple virtual devices with a single command, both in administrator and user contexts. An option allows encryption of the backup archive to securely store the SSL keys and certificates.   | Provides efficient and administrator-friendly user interface, especially in an environment with multiple contexts, freeing administrators to do more with reduced IT operating budgets |
| <b>Enhanced SNMP MIB support</b>  | The Cisco ACE Module supports additional SNMP MIBs, leading to parity with the MIBs supported on the Cisco ACE 4710.  | Enables centralized management of the load balancing infrastructure, improving agility in IT operations  |
| <b>Bulk copy command for SSL certificates and key pairs</b>               | The bulk copy command for SSL certificates and key pairs enables the import of multiple SSL certificates and key-pair files at the same time.   | Increases productivity by reducing time needed to copy SSL files   |
| <b>Granular reporting of HTTP URL hits on a virtual IP address</b>        | The Layer 7 match HTTP URL statement hit count feature allows you to display the number of times that a connection is established (hit count) based on match HTTP URL statements for a class map in a Layer 7 HTTP policy map.  | Provides reporting capability for multiple web applications under the same virtual IP address  |
| <b>Syslog reporting for NAT</b>   | New syslog messages track the NAT function.   | Complies with regulations for service providers to log NAT maps  |
| <b>HTTP header insert for SSL information</b>                             | The Cisco ACE Module can offload SSL processing from the real server in the web application server farm. In some cases, the web application still requires SSL-related information such as the SSL session parameters, SSL server certificate, and SSL client certificate. With this new feature, the information is provided to the web application through user-defined HTTP protocol headers that are inserted by the Cisco ACE Module during HTTP communication with the real server running the web application. | Efficiently uses expensive real server cycles to process application data and provide a secure single point of management for SSL server certificates on the Cisco ACE Module          |
| <b>HTTP redirect on client authentication failure</b>                     | The Cisco ACE Module can redirect users in the event of failed client authentication, providing more information such as the reason for the client authentication failure and recommended next steps to restore access to the application.  | Efficiently handles client authentication failures, reducing calls to application support and improving the user experience, while providing the benefits of SSL offload               |
| <b>LDAP-based CRL retrieval for SSL offload</b>                           | The Cisco ACE Module can query the CRL distribution point (CDP) server using the LDAP protocol, both in SSL termination and end-to-end SSL deployment modes.  | Enables transparent migration to Cisco ACE SSL offload for environments currently providing access to CDP servers using LDAP   |
| <b>CRL checking of SSL server certificates</b>                            | The Cisco ACE Module can query the CDP server to verify that an SSL termination point's certificate has not been revoked.   | Enables transparent migration to Cisco ACE SSL offload for environments currently verifying SSL server certificates using CRLs   |
| <b>Sample SSL key and certificate</b>                                     | The Cisco ACE Module software image has a sample SSL key and certificate pair to get the user started with SSL offload function testing and integration prior to requesting a third-party-generated SSL key and certificate pair for use in real-world production environments.   | Facilitates demonstration and testing of the SSL offload feature   |
| <b>Enhanced scalability for GSLB with Cisco GSS</b>                       | Cisco ACE Module integration with Cisco GSS now supports up to 4000 virtual IP addresses per Domain Name System (DNS) domain, which scales the Cisco ACE load-balancing solution for large enterprises and service providers.   | Scales capacity for a GSLB solution with the Cisco ACE Module and Cisco GSS, leading to investment protection and reduced capital expenditures (CapEx)                                 |
| <b>Persistence rebalance for HTTP requests on the same TCP connection</b> | The Cisco ACE Module can be configured to load balance each HTTP request on the same TCP connection from a client IP address.   | Uniformly distributes HTTP traffic if a significant share of the HTTP requests are from the same client, leading to better resource utilization  |
| <b>Support for secondary IP addresses on an interface VLAN</b>            | The Cisco ACE Module supports secondary IP addresses on an interface VLAN in addition to the primary IP address.  | Enables transparent migration from load-balancing products that support secondary IP addresses on a VLAN   |

## System Requirements

Table 2 lists the system requirements for the Cisco ACE Module.

**Table 2.** Cisco Catalyst 6500 and Cisco 7600 Series System Requirements for Cisco ACE Module

| Requirement                 | Description  |
|-----------------------------|--|
| <b>Chassis</b>              | All Cisco Catalyst 6500 Series and Cisco 7600 Series chassis   |
| <b>Supervisor engines</b>   | <ul style="list-style-type: none"> <li>• Cisco Catalyst 6500 Series Supervisor Engine 720 and Virtual Switching Supervisor Engine 720 with 10GE Uplinks</li> <li>• Cisco 7600 Series Supervisor Engine 720 with Multilayer Switch Feature Card and Route Switch Processor 720 with Multilayer Switch Feature Card</li> </ul>   |
| <b>Chassis OS</b>           | <ul style="list-style-type: none"> <li>• Cisco Catalyst 6500 Series running Cisco IOS® Software Release 12.2(18)SXF4 or later for Supervisor Engine 720, and Release 12.2(33)SXH or later for Supervisor Engine 720 with 10GE</li> <li>• Cisco 7600 Series running Cisco IOS Software Release 12.2(18)SXF4 or later and Release 12.2(33)SRB or later for Supervisor Engine 720, and 12.2(33)SRC or later for Route Switch Processor 720</li> </ul> |
| <b>Chassis connectivity</b> | Functions as a fabric-enabled line card  |
| <b>Chassis slots</b>        | Occupies 1 slot in the chassis   |

## Ordering Information

Table 3 provides ordering information for the Cisco ACE Module.

**Table 3.** Ordering Information

| Part Number                 | Description  |
|-----------------------------|--|
| <b>C6509E-ACE20-8-K9**</b>  | Cisco ACE20 6509E SUP720-10G Bundle with 8Gbps Throughput License  |
| <b>WS-C6509E-ACE20-K9**</b> | Cisco ACE20 6509 Bundle with 8 Gbps Throughput License   |
| <b>WS-C6504E-ACE20-K9**</b> | Cisco ACE20 6504 Bundle with 4 Gbps Throughput License   |
| <b>WS-C6509-E-ACE-K9**</b>  | Cisco ACE10 6509 Bundle with 8 Gbps Throughput License   |
| <b>WS-C6504-E-ACE-K9**</b>  | Cisco ACE10 6504 Bundle with 4 Gbps Throughput License   |
| <b>ACE20-MOD-K9</b>         | Cisco ACE20 Service Module for Cisco Catalyst 6500 Series and Cisco 7600 Series: Includes 1000 SSL TPS and 5 Virtual Devices         |
| <b>ACE20-MOD-K9=</b>        | Cisco ACE20 Service Module for Cisco Catalyst 6500 Series and Cisco 7600 Series: Includes 1000 SSL TPS and 5 Virtual Devices (spare) |
| <b>ACE10-6500-K9</b>        | Cisco ACE10 Service Module for Cisco Catalyst 6500 Series and Cisco 7600 Series, Includes 1000 SSL TPS and 5 Virtual Devices         |
| <b>ACE10-6500-K9=</b>       | Cisco ACE10 Service Module for Cisco Catalyst 6500 Series and Cisco 7600 Series, Includes 1000 SSL TPS and 5 Virtual Devices (spare) |
| <b>ACE-16G-LIC</b>          | 16Gbps Throughput License for Cisco ACE20  |
| <b>ACE-08G-LIC</b>          | 8-Gbps Throughput License for Cisco ACE 10 and Cisco ACE20   |
| <b>ACE-04G-LIC</b>          | 4-Gbps Throughput License for Cisco ACE10 and Cisco ACE20  |
| <b>ACE-UPG2-LIC=</b>        | Upgrade License from 8 Gbps to 16 Gbps for Cisco ACE20   |
| <b>ACE-UPG1-LIC=</b>        | Upgrade License from 4 Gbps to 8 Gbps for Cisco ACE10 and Cisco ACE20  |
| <b>ACE-SSL-15K-K9</b>       | 15,000 SSL Transactions per Second License for Cisco ACE10 and Cisco ACE20   |
| <b>ACE-SSL-10K-K9</b>       | 10,000 SSL Transactions per Second License for Cisco ACE10 and Cisco ACE20   |
| <b>ACE-SSL-05K-K9</b>       | 5,000 SSL Transactions per Second License for Cisco ACE10 and Cisco ACE20  |
| <b>ACE-SSL-UP2-K9=</b>      | Upgrade license from 10,000 to 15,000 SSL Transactions per Second License for Cisco ACE10 and Cisco ACE20                            |
| <b>ACE-SSL-UP1-K9=</b>      | Upgrade license from 5,000 to 10,000 SSL Transactions per Second License for Cisco ACE10 and Cisco ACE20                             |
| <b>ACE-VIRT-250</b>         | 250 Virtual Contexts License for Cisco ACE10 and Cisco ACE20   |
| <b>ACE-VIRT-100</b>         | 100 Virtual Contexts License for Cisco ACE10 and Cisco ACE20   |
| <b>ACE-VIRT-050</b>         | 50 Virtual Contexts License for Cisco ACE10 and Cisco ACE20  |
| <b>ACE-VIRT-020</b>         | 20 Virtual Contexts License for Cisco ACE10 and Cisco ACE20  |

| Part Number         | Description  |
|---------------------|--|
| <b>ACE-VIRT-UP3</b> | Upgrade License from 100 to 250 Virtual Contexts for Cisco ACE10 and Cisco ACE20 |
| <b>ACE-VIRT-UP2</b> | Upgrade License from 50 to 100 Virtual Contexts for Cisco ACE10 and Cisco ACE20  |
| <b>ACE-VIRT-UP1</b> | Upgrade License from 20 to 50 Virtual Contexts for Cisco ACE10 and Cisco ACE20   |

\*\* Cisco ACE bundles do not include I/O modules so that customers can order the I/O modules of their choice.

## For More Information

For more information about the Cisco ACE Module, visit <http://www.cisco.com/go/ace> or contact your local Cisco account representative.



Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

Asia Pacific Headquarters  
Cisco Systems (USA) Pte. Ltd.  
Singapore

Europe Headquarters  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

CCDE, CCENT, CCSE, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumina, Cisco Nexus, Cisco Nitro Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mini, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), CiscoFinanced (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Register, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CDR, CCNA, CCNP, CCSP, CCVP, 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, Community, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, ILYN, Internet Quotient, IOS, IPPhone, iQuickStudy, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanel, PowerTV, PowerTV (Design), PowerVu, Prime, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TiersPath, 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. (0908R)