Release Note for the Cisco ACE Web Application Firewall

July 9, 2010

Contents

This release note applies to software version 6.1(1) for the Cisco Application Control Engine (ACE) XML Gateway and the Cisco ACE Web Application Firewall.

For detailed information on product features, refer to the ACE XML Gateway and ACE Web Application Firewall documentation on http://www.cisco.com.

This release note contains the following sections:

- New Software Features in 6.1
- New Software Features in 6.1(1)
- Software Feature Changes in 6.1(1)
- Important Notes
- Software Version 6.1(1) Open Caveats and Resolved Caveats
- Software Version 6.1 Open Caveats and Resolved Caveats
- Related Documentation
New Software Features in 6.1

This section lists important new software features and feature enhancements in this 6.1 release, including:

- Java Upgrade
- Base Configuration
- Port Channeling
- Link Monitoring
- Whitelist for DOS Protection
- Client IP Logging
- Batch Import / Export
- Clearing the Policy History
- Policy Statistics Information
- Policy Component Search by ID
- Detailed LDAP Error Information
- Improvements in the Manager

Java Upgrade

The version of the Java runtime environment included in the product was upgraded from 1.4 to 1.6.13. Starting from software version 6.1, the ACE XML Gateway supports SDK extensions written in Java 6. All Java SDK extensions that are officially supported by Cisco will continue to work with the 6.1 release, but there is no such guarantee for custom Java SDK extensions. However, they should continue to work as long as the code and the set of used libraries are compatible with JDK 1.6. Please contact your support representative if you want to determine whether a specific extension is officially supported by Cisco or not.

Java SDK for Extensions

The 6.1 software release of the Cisco ACE XML Gateway comes with new version of the Java SDK for extensions version 2.0.0. There are no API changes between the previous version 1.4.0 and the new version 2.0.0. The only difference is that 2.0.0 SDK is compiled with Java 6. The change affects only creation of new custom extensions—you must use 6.1 release and SDK 2.0.0 if you create an extension that is compiled with Java 6. At the same time, 6.1 software release is compatible with extensions that are compiled using 1.x.x SDK and Java 1.4.

Base Configuration

A base configuration update is available for software release 6.1. The base configuration defines the built-in signatures, rules, and profiles available for configuring web application security. Base configuration updates can be applied to the system independently of software updates. New appliances that have software version 6.1 pre-installed will include the latest base configuration by default. However, if updating to 6.1 from a previous version, you will need to apply the base configuration update directly. A base configuration update file is in the form of a PPF (Portable Policy Format) file. To apply the base configuration update, upload the PPF file using the Update Base Configuration button in the Rules and Signatures page of the Manager web console.
The portable policy format is used for the files generated by exporting a policy from the Manager as well.

Base configuration update PPF files can be uploaded on the Rules & Signatures page. The version identifier for the base configuration update is 1.0(2)_2009100501. The base configuration identifier (2009100501) appears on the Rules & Signatures page of the Manager web console. This version of the base configuration cannot be applied to software versions prior to 6.1; it is not compatible with 6.0.x. You can acquire the base configuration update file from cisco.com.

In 6.1 release version the base configuration can be separately downloaded and imported into the Manager. After an import of a new base configuration, it is recommended that you:

- Switch all web applications into “monitor mode”;
- Deploy the policy;
- Allow it run for a while to identify any “false positives”.

Since there are rule and signature changes, this change may result in false positives.

**Port Channeling**

The ACE Web Application Firewall now supports port channeling at its physical network interfaces. Port channeling is designed to overcome issues such as bandwidth limitations and lack of redundancy at Ethernet ports. Port channeling allows you to aggregate multiple network ports/cables into a single logical channel, increasing the link speed or providing a failover mechanism for the physical interfaces.

The ACE Web Application Firewall can allocate traffic across aggregated links using the following methods:

- balance-rr
  This mode uses the round-robin policy for load balancing. It separates network packets between aggregated interfaces distributing bandwidth among them. Periodically the system polls network link statuses and excludes broken links from rotation.

- active-backup
  This mode uses the active-backup policy for load balancing. All traffic is sent via a single active (primary) network interface. If the primary network interface goes down, a new primary interface is selected from the rest of aggregated interfaces. It allows you to create a backup network route which normally should not be used (e.g. if the link is slow or traffic through that link is more expensive).

- balance-xor
  This mode selects link interface to transmit each packet based on the packet’s source and destination MAC addresses. With this mode packets from a particular client to a particular destination always are transmitted via the same link interface. It allows you increase network throughput by transmitting packets from different clients via different network interfaces.

Port channeling can be configured from the Network Configuration menu of the appliance console interface.
Link Monitoring

The Link Monitoring feature has been made to send SNMP traps if one of the links (including link aggregations and aggregated ones) changes its state, for example it goes down (if it was up before) or up (if it was down before). It is useful to enable these notifications especially together with the port channeling feature. For example, when one of the aggregated links goes down, it might not trigger a network malfunction, but it can decrease network bandwidth.

Changes in the state of the network interfaces are also reflected in the Event Log:

- When a link goes down, the event is indicated in the event log at the error level.
- When a link goes up, the event is indicated in the event log at the notice level.

Whitelist for DOS Protection

A new feature is added for configuration of DOS protection. It allows you to specify zero or more IP addresses/IP ranges that are excluded from attack detection. Clients with the specified IP address or whose address is included in the specified IP address range are exempt from blocking even if the rate of their requests exceeds one of the configured thresholds.

Client IP Logging

The client IP option, which appears under the Global Policy Settings menu item, allows for an IP address indicated in an HTTP request header to be treated as the source client IP for purposes of logging and reporting. This option can be used when the ACE Web Application Firewall is deployed behind a load balancer that is configured to send a real client IP in an HTTP header, for example in “X-Forwarded-For”. When the option is enabled, event logs will contain the IP address extracted from the HTTP header, in addition to the IP address of the load balancer.

Batch Import / Export

The “Batch import/export” feature is introduced in the 6.1 software release of the ACE Web Application Firewall. It allows you to import/export the contents of several selected subpolicies in the PPF using one operation.

Clearing the Policy History

The “Clearing the Policy History” feature has been introduced in the ACE XML Manager under the “Policy Manager” menu item.

With the course of time the total policy size and number of entries in the policy history increases, it can eventually cause resource-related issues. The feature allows you to remove the old saved and hidden policies from history and all policy components related to them in order to free the disk space.

The Clean History page contains information about the policy history (the number of entries per subpolicy) and the disk space occupied by the cluster.

The clean history option can be customized by two options:
- **Trim history to**: The number of recently saved policy history entries that you want to retain. Other policy history entries are deleted, and related files are removed from the disk.

- **mode**: This option lets you specify whether to clear history entries for the current subpolicy only or for all subpolicies.

### Policy Statistics Information

This new option in the Policy Manager provides you with information about policy statistics. It shows the total number of subpolicies, total number of components in every subpolicy and in the whole policy, number of records in the policy history, and the cluster size. If one of the values exceeds the recommended maximum, a warning message appears.

### Policy Component Search by ID

This feature allows you to locate a policy component based on its ID, irrespective of the subpolicy where the component is located. The component ID is usually mentioned in the Exception Notification email, which is sent when an exception occurs during the service request processing. This is useful, for example, to quickly find the virtual service or handler associated with the exception message. To perform the search, enter the 16-hexadecimal digit ID in the field on the Policy Manager page.

### Detailed LDAP Error Information

In the ACE XML Gateway product, a new option in the LDAP authenticator settings allows a client to get an extended error code received from a backend LDAP system. The option is introduced for the following types of authenticators:

- Active Directory LDAP Query
- LDAP Bind Success
- LDAP Query

The setting can be found on the credentials setup page for the corresponding authenticator under the “Result Processing” section.

### Improvements in the Manager

In the 6.1 software release of the Cisco ACE XML Gateway some important changes have been made to improve Manager performance, including the items described in the following sections.

#### Manager Locking

In prior releases the Manager had a global lock that prevented requests from influencing each other. All requests from users were queued up and executed one by one, so often end-users of the Manager in a multi-user environment had to wait while requests of other users complete. In 6.1 software version the locking strategy is changed, allowing simultaneous access for multiple users.
Signature Navigation Improvements

References to signatures and rules appear in the Event Log and the Web Application Firewall incident report; they are also present on the Web Application Firewall Profile Inspection Rules page and the Web Application Firewall Rule details. The UI is enhanced to make it easier to track these references for detailed description:

- For references to a rule, its details are shown;
- For signature groups, contents are displayed in the pop-up windows;
- For a link to the specific signature, its definition is highlighted in a pop-up window.

Manager Performance

Overall performance is improved as a result of code optimizations, Java upgrade, and increasing the amount of available memory for the Manager.

New Software Features in 6.1(1)

This section lists important new software features and feature enhancements in this 6.1(1) release, including:

- Certificate Renewal
- WSDL Transparency
- Client Certificate Verification

Certificate Renewal

The 6.1(1) software release of the Cisco ACE XML Gateway introduces the Certificate Renewal feature. It allows you create a new certificate signing request (CSR) for an existing private key.

Click the [CSR generation] link (every key has its own link) on the Public/Private Keypairs page in the right column of the table. The Generate Certificate Signing Request page appears. The options are similar to generating the CSR with a new key.

Once the CSR is signed by a trusted Certificate Authority (CA) it may be uploaded into the policy. The signed certificate replaces the old one, while preserving the existent Public/Private Keypair resource.

WSDL Transparency

This feature improves interoperability of WSDL import/generation. When the feature is enabled the ACE XML Gateway produces a WSDL file which is as much as possible close to the original file. Documentation, faults and custom extensibility elements are preserved during import/generation cycle.

This feature can be enabled/disabled per a handler group. By default, it is switched off and can be available if all of the following conditions are met:

- A handler group is WSDL-compatible
- A handler group is created by WSDL imported in the version 6.1(1) or higher
- All handlers within a handler group are routed to services created from the same WSDL or manually

If the handler group does not meet these requirements, the descriptive message will be shown. You can check which WSDL files were used to produce handler in the groups, examining table under “Members” section.
If you need to enable the feature for a handler group created by WSDL import in version before 6.1(1), the WSDL must be updated or re-imported.

**Client Certificate Verification**

The client certificate verification feature, introduced in software release 6.1(1), helps to enhance Manager security. With this feature, the Manager can be configured to verify the client certificate of users who access the Manager web interface. The certificates are verified against a particular certificate chain of trust that you configure in the Manager.

To enable this feature, perform the following steps:

**Step 1** Configure the truststore for the Manager. The truststore is a Java keystore containing certificates of trusted Certificate Authorities (CAs). The “/usr/local/reactivity/sbin/trustkeystore” script should be used to manage truststore. Run it without parameters to see usage instructions. The certificates provided to the script must be in the PEM format.

In order for the client certificate to be approved, the certificate chain must be established. This chain must meet the following rules:

- each certificate of the chain must be present in truststore
- client certificate must be signed by the CA that comes first in the chain
- each certificate in the chain must be signed by the CA that follows next in the chain
- the last certificate in the chain must be self signed (so called “root CA”).

**Step 2** Enable the feature by setting the “webapp.client.cert.auth” property in the “/usr/local/reactivity/config/webapp.properties” file to “true”.

**Step 3** If you want to use the CRL (Certificate Revocation List) during certificate verification, set the “webapp.client.cert.auth.crl” property in the “/usr/local/reactivity/config/webapp.properties” file to “true”. Currently the Manager can read CRL file from the disk only, so place it in the predefined location. The CRL file must be named as “truststore.crl” and placed under the “/var/lib/reactivity/truststore” directory. Make sure that CRL file is readable by every user.

**Note** The “/var/lib/reactivity/truststore” directory is created by the truststore management script, so you should configure truststore before placing CRL file.

**Software Feature Changes in 6.1(1)**

This section lists important features changes and enhancements in this 6.1(1) release, including:

- **Platform Updates**

**Platform Updates**

This release incorporates the following platform updates:

- The version of Sendmail has been upgraded from 8.12.11 to 8.14.4.
Important Notes

The version of Apache Tomcat on the platform has been upgraded from 5.0 to 6.0. This upgrade incorporates numerous security enhancements to Tomcat. The upgrade does not affect any aspects of the product behavior.

Important Notes

This section describes behavior changes, supplemental documentation, and other information for this release. It includes the following sections:

- nCipher
- About the Product Documentation

nCipher

The Manager uses SSL acceleration only if a security world is created and initialized. In the previous releases it always used SSL acceleration if the hardware was available.

About the Product Documentation

Other than this release note and the ACE XML Gateway Quick Start Guide included in the box, each product has its own documentation set. While every effort was made to target the Cisco ACE Web Application Firewall documentation exclusively to Cisco ACE Web Application Firewall features, the documents may contain references to features that are available only with the Cisco ACE XML Gateway product.

The Cisco ACE Web Application Firewall documentation set includes the Cisco ACE Web Application Firewall Getting Started Guide, a tutorial-style guide that takes you step-by-step through the process for setting up web application security with the Cisco ACE Web Application Firewall features. The guide applies to using the web application security features with an Cisco ACE XML Gateway license as well.

The Cisco ACE Web Application Firewall Getting Started Guide includes instructions for setting up a web application security policy to protect a specific sample backend application, the Poison Oak Insurance web application. Note that the sample application is not currently publicly available.

Software Version 6.1(1) Open Caveats and Resolved Caveats

The following sections contain the open and resolved caveats in software version 6.1(1):

- Software Version 6.1(1) Open Caveats
- Software Version 6.1(1) Resolved Caveats

Software Version 6.1(1) Open Caveats

The following table lists open caveats
The following table lists resolved caveats.

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCsv14517</td>
<td>The error message saying “The resource is in use by Service” appears while deleting XSD resource. However, the Service settings contain no visible references to that resource. This issue occurs when a policy contains XSD resource and SOAP-document Virtual Service. Originally the message validation was selected to schema-based validation against a specific XSD. Later the mode was changed to well-formed validation. The attempt to remove the XSD resource fails with the error message reporting that the resource is still in use by the Service. Workaround: In the Service Request/Response Message Specification page, switch the SOAP Message Validation drop-down to “Content...” option, then deselect reference to XSD resource in the “Import additional XML schemas” list. After this the SOAP Message Validation can be switched back to the Well-formed option and changes are saved.</td>
</tr>
<tr>
<td>CSCtb31575</td>
<td>Custom Java-based extensions for the ACE Web Application Firewall may be vulnerable to Common Vulnerabilities and Exposures (CVE) identifier CVE-2009-2625. The vulnerability is found inside XML parser in JDK and allows remote attackers to cause a denial of service (infinite loop and application hang) via malformed XML. None of the certified Cisco-created extensions are affected by this issue. Workaround: N/A</td>
</tr>
<tr>
<td>CSCtb75870</td>
<td>The Cisco ACE XML Gateway leverages Apache Xerces-C, which is vulnerable to CVE-2009-1885. However, there is no way for this particular vulnerability to be exploited outside of the product. This Cisco bug ID exists to ensure that Apache Xerces-C library is patched with the appropriate fixes. Workaround: N/A</td>
</tr>
<tr>
<td>CSCtc03893</td>
<td>When using an authenticator that parses the client certificate and verifies it against an LDAP server, the filter input allows copying the certificate credentials using %d. However, if the client certificate includes parentheses anywhere in the subject, the authenticator fails with a message in the logs saying that the filter is invalid. Workaround: N/A</td>
</tr>
<tr>
<td>CSCtc16963</td>
<td>The ACE Web Application Firewall reports “500, Validation Error” on the HTTP DELETE request because of missing attributes even if all required attributes are set. Or the ACE Web Application Firewall sends the HTTP DELETE request without attributes to a backend server even if it is configured to send attributes. This issue occurs when a route from the HTTP DELETE handler to the HTTP DELETE service descriptor is configured to map or pass through handler attributes to service descriptor attributes. Workaround: N/A</td>
</tr>
<tr>
<td>Issue ID</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| CSCtc40822   | Valid SOAP messages fail schema validation. This issue happens when:  
  • Validation is performed against schema that contains element B, which extends element A of a complex type.  
  • The sent message contains an element of type B.  
  • The message is processed by the Flex Path handler.  
  There are two possible workarounds:  
  1. Change the schema declarations to avoid “complex extensions”.  
  2. Change the handler settings, to make messages going through the Reactor. |
| CSCtc56926   | An XML request with large number of XML entities is rejected by the ACE Web Application Firewall as malformed. The Event Log contains the following message: “Exception while checking SOAP Envelope: Could not parse XML document: Entity; line 1: parser error : Detected an entity reference loop”. This issue occurs when the policy contains the XML-based virtual service that runs on the Flex Path. The message is in XML format and contains 500000 or more XML entities.  
  There are two possible workarounds:  
  1. The issue appears on the Flex Path only. It can be avoided by making the service subject to the Reactor processing instead of the Flex Path processing, if possible.  
  2. This issue does not affect numeric entities. To workaround the issue, transform the message and replace all entity references with numeric. |
| CSCtc76288   | Importing of a WSDL file into the Manager fails with the “ACE XML Gateway Manager Internal Error”. The internal log contains messages related to the problem in URI parsing: “java.lang.IllegalArgumentException: URI is not absolute”. This issue occurs when the WSDL contains definition of SOAP via an HTTP web service. The service interface URI is malformed.  
  Workaround: The service interface URI should be declared in the <soap:address> tag and in the “location” attribute. |
| CSCtc81781   | The ACE Web Application Firewall is restarted by watchdog when it was processing a certain XML message for security validity. This issue occurs when the ACE Web Application Firewall handler has options to decrypt and check a signature of the incoming SOAP 1.2 request and has the advanced SOAP header processing feature “Process WS-Security header for validity, but do not alter the message” turned on. It is terminated while processing of the incoming SOAP message that was properly encrypted and signed.  
  Workaround: Turn off the “Process WS-Security header for validity, but do not alter the message” in the Advanced SOAP Header Processing page. |
| CSCtc81819   | The ACE Web Application Firewall rejects SOAP messages containing elements that are declared to be empty by XML schema attribute ‘xsi:nil= “1”’. The attribute value “1” is valid for XML schema boolean type, however, the Gateway accepts only value “true”.  
  Workaround: The message needs to be processed by the XSL transformation, which changes the value of xsi:nil attribute from “1” to “true”. The transformation must be applied in pre-processing, before validation. |
An industry-wide vulnerability exists in the Transport Layer Security (TLS) protocol that could impact any Cisco product that uses any version of TLS and SSL. The vulnerability exists in how the protocol handles session renegotiation and exposes users to a potential man-in-the-middle attack. This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20091109-tls.shtml.

The ACE Web Application Firewall responds with a 500, “Transformation error” and the following warning level entry is observed in the Event Log: "Exception during processing of message HTTP POST request for / from <ip address>; problem type ‘Message transformation failed’, problem message ‘com.reactivity.sdk.api.SDKException: Null message body specified from transform’". This issue occurs when the request is sent to the HTTP POST Arguments handler which is configured to perform transformation with extension. The extension does not change the body of the request.

Workaround: N/A

Approuter process is killed by watchdog because of high memory usage. The Event Log contains corresponding error message. This issue occurs when XML validation was extensively used with significant amount of different XSD schemes.

Workaround: N/A

WSDL generation for a particular handler group takes several minutes to be completed. The slowness is also observed during policy compilation, when WSDL publishing was switched on. This issue occurs when the policy contains a handler group, which consists of a large number (hundreds) of virtual services.

There are two possible workarounds:

1. The policy compilation can be sped up by disabling the WSDL publishing option.
2. Upgrade a system from the previous software version to 6.1, since 6.1 is much faster than an earlier version.

SSL connection to the backend server fails with the following error message: “Error while verifying server certificate: server certificate was not signed by any of permitted CAs”. This issue occurs when the policy contains the necessary trusted Certificate Authority (CA) in the Shared. Some subpolicy also contains duplicates of these CAs. The Server is set to verify server certificate against some trusted CA.

Workaround: The policy must contain only one instance of the trusted Certificate Authorities. All other instances must be deleted.

The ACE XML Gateway sends the SOAP message with MTOM attachment header and the backend service returns the HTTP Error 400, “Bad Request”. This issue affects SOAP Document and HTTP POST body handlers that are used to process requests with MTOM attachments. The affected versions are from 5.2 to 6.1. Workaround: N/A

The Flex Path encodes underscore characters in HTTP GET arguments, that may cause interoperability issues in communication with the backend server. Workaround: Modify handler settings to make it running on the Reactor. To find out the settings have been changed, click the “flex path report” icon for a corresponding handler.
<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCte12091</td>
<td>The ACE Web Application Firewall stops processing traffic due to an excessive number of open files while performing LDAP authentication. This issue can be identified by the “Too many open files” error message in the Event Log. Also, the lsof command shows that approuter process has more than 1000 file descriptors. This issue occurs when the policy has the LDAP authenticator that verifies using the LDAP Query, the LDAP bind is performed via many different users (%u in the User DN field). Workaround: 1. Access the shell menu on the Gateway appliance. 2. Execute the following commands:  • service reactivity-firewall stop  • su - agateway  • vi config/runtime.properties 3. Edit the “policy.cache.ldapbind.enable” parameter in the configuration file to the following: “policy.cache.ldapbind.enable=false”. 4. Save changes and exit from bash. 5. Restart the ACE XML Gateway.</td>
</tr>
<tr>
<td>CSCte38916</td>
<td>WSDL generation for a handler group fails with the following error message: “Handler: ‘&lt;handler name&gt;’, Schema to be included in WSDL has null or empty Target Namespace”. This issue occurs when the WSDL for a specified handler group imports the XML schema with null target namespace. Workaround: Change the XML schema. Specify some target namespace for it.</td>
</tr>
<tr>
<td>CSCte41124</td>
<td>The ACE Web Application Firewall returns “503 Error in firewall” if a request was sent to a SOAP Document handler. When the SOAP Document handler configured to send SAML token to the backend server, the gateway awaits WS-Addressing SOAP headers in a request. When the request does not contain such headers, the gateway returns “503 Error in firewall”. Workaround: Send requests with correct SOAP headers.</td>
</tr>
<tr>
<td>CSCte51198</td>
<td>The WSDL file generated by the ACE Web Application Firewall contains a reference to the internal ACE Web Application Firewall resource. This issue occurs when the handler group is constructed upon imported WSDL file, which contains nested XML schemes with “include” statement. Workaround: N/A</td>
</tr>
<tr>
<td>CSCte51572</td>
<td>The WSDL generated by the ACE Web Application Firewall misses some parts that are present in the original imported WSDL. The missing elements/ parts are actually ignored during the WSDL importing and they do not affect traffic processing. Workaround: N/A</td>
</tr>
<tr>
<td>CSCte52741</td>
<td>The Password Digest Authentication of a message on the ACE XML Gateway fails when the nonce of the message contains a byte equal to 0. Workaround: Make sure no a byte of the message nonce is equal to 0.</td>
</tr>
<tr>
<td>Issue ID</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCte55963</td>
<td>The ACE Web Application Firewall returns an HTTP error code 503 when processes a message containing a SAML token. The Event Log contains: “Dangling message—generating 503”. This issue occurs when the policy contains a virtual service and the service authentication is enabled and specified to send one SAML token to the backend server. The handler does not have authenticator, or authenticator is not SAML type. Workaround: The access control for the handler should have authenticator of the “SAML Token” type.</td>
</tr>
<tr>
<td>CSCte64217</td>
<td>The ACE Web Application Firewall is vulnerable to CVE-2004-0488. If all conditions are exist, remote attackers may use this to execute arbitrary code. This issue occurs when an attacker is able to craft the specific client TLS certificate with long subject DN and then sign it by a CA, which the gateway trusts. Workaround: N/A</td>
</tr>
<tr>
<td>CSCte64233</td>
<td>The ACE Web Application Firewall is vulnerable to CVE-2003-0020. The product does not perform special actions to filter some parts of incoming messages from log files. This may be used by attackers for inserting special byte sequences into log files. If the log file is viewed in the terminal emulator program, which is vulnerable to that special byte sequences, then the machine on which the log is viewed may be compromised. This issue occurs when log files from the gateway are viewed using vulnerable software and remote attackers send specifically crafted messages to the ACE Web Application Firewall. Messages must exploit the specific vulnerabilities in the terminal emulator software used to examine the logs. Workaround: Do not view log files in terminal emulators, use text editors.</td>
</tr>
<tr>
<td>CSCte64349</td>
<td>The Manager Web Console is a Java-based web application running on the Apache Tomcat application server. In order to increase overall system security, the Java Security Manager has been enabled for Tomcat. Now Tomcat may run only limited number of operations necessary for the Manager Web Console, while all other operations are restricted. Thus Manager Web Console has become less vulnerable to possible exploits in the Java Platform, Apache Tomcat or the Web Console itself. Workaround: N/A</td>
</tr>
</tbody>
</table>
## Software Version 6.1(1) Open Caveats and Resolved Caveats

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| CSCtf08639  | The Manager is not responding after attempt to login. This issue occurs if one of the gateways in the current cluster hung. The gateway accepts TCP connection, responds to ping, but does not send any data. Workaround: The hanging gateway must be removed from the cluster and the Manager should be restarted:  
1. Login into the Blue Screen and stop the ACE Web Application Firewall Manager process  
2. Acquire the list of the gateways in the cluster:  
   cat /var/lib/reactivity/console_documents/clusterXXXXX/cluster.properties  
3. Check every gateway in the cluster: try to ping it, try to connect via SSH, try to send data to gateway services. The hanging gateway responds to ping, accepts connection, but doesn't send any data.  
4. Remove the gateway from the cluster by manual editing the “/var/lib/reactivity/console_documents/clusterXXXXX/cluster.properties” file.  
5. Start the Manager process. |
| CSCtf25045  | After configuring an NTP server, the ACE Web Application Firewall indicates that communication to the NTP server failed. A tcpdump taken from the ACE Web Application Firewall shows that the NTP server is replying. However, the ACE Web Application Firewall sends an icmp reply destination port unreachable to the NTP server. Workaround:  
1. Connect to the appliance using a SSH client.  
2. From the shell menu, access the bash prompt.  
3. Execute the following: vi /usr/local/reactivity/config/lockdown.d/base  
4. Add the following to the file:  
   • # Allow NTP  
   • -p udp --sport ntp  
5. Save changes and exit the editor.  
6. Execute “service reactivity-iptables restart”.  
7. Execute “service ntpd restart”.  
8. Exit the bash. |
| CSCtf60288  | VIP import from the ACE fails with the following line: “ERROR: Load balancer <balancer_address> virtual server parse failed unsupported port name seen in ace-class map <address> has no VIPs, or all of its VIPs are already represented by HTTP server definitions in this policy”. This issue occurs when the XML configuration, obtained from the ACE, contains references to unsupportable protocols. The element “match_virtual-addr” contains “port-tcp-name” attribute (or “protocol-value” for early versions of the ACE) with value different from the following: “http”, “https”, “smtp”, “www”. Workaround: Create VIPs manually. |
### Issue ID | Description
--- | ---
CSCtf99191 | The ACE XML Gateway does not process HTTP requests if the URL ends with a query string such as “?WSDL” or “?wsdl”. The following error appears: “No handler was found matching the request”. This issue occurs when:
- URLs end with a query string without additional parameters or value
  - http://hostname/url>?wsdl
- any combination of upper and lower case letters after the “?”
  Workaround: Add an additional parameter or a value after the query string:
  - http://hostname/url>?WSDL=value
  - http://hostname/url>?wsdl=value

CSCtg47664 | Approuter process is killed by watchdog because of high memory usage. The Event Log contains corresponding error message. This issue occurs when XML validation was extensively used with significant amount of different XSD schemes.
  Workaround: N/A

CSCtg62959 | HTTP POST request sent to the backend server becomes malformed. The request-line and HTTP headers are not changed. While the ACE Web Application Firewall is sending the request to the backend server, the connection gets unexpectedly closed by the backend side. This issue affects requests with non-empty body (POST or PUT). Both GET and HEAD requests are processed successfully. The issue occurs on the Reactor only.
  Workaround: This issue is related to the Reactor reconnect feature. It could be disabled by setting the parameter “connection.attempts” to “0” in the “reactor.conf” file. However, if all conditions for the issue are met, ACE Web Application Firewall will reply with 500 HTTP error instead of reconnecting.

CSCtg78525 | While applying a change to the access control, the following error appears:
  "You do not have sufficient user privileges for this task. Please contact you administrator if you believe this is an error.”

  The user log shows: “May 12 18:43:45 mr0315-ace-xml-1
  Java_1.6.0_13[http8243-Processor19]: 1273689825996 [console /console/users console W] The current user “administrator” does not have permission to perform this action:
  “/edit.do”.”

  This issue occurs when the Authorization Group is in Shared, but you are in a subpolicy.
  Workaround: N/A
<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCsu26376</td>
<td>When WSSE pass through is enabled, the ACE Web Application Firewall removes namespace prefix from Id attribute of the UsernameToken. If schema validation is enabled for message processing, the request fails with the following message: “XML was not valid: Attribute ‘Id’ is not declared for element ‘UsernameToken’”. This issue occurs when the policy contains SOAP 1.1 Virtual Service with WSS Username pass through enabled. The request message has SOAP header UsernameToken: <code>&lt;a:UsernameToken b:Id=&quot;0123456789&quot;&gt;</code>, where namespaces are standard WSS schemas defined by OASIS: xmlns:a=&quot;<a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd</a>&quot;, xmlns:b=&quot;<a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd</a>&quot; During the ACE Web Application Firewall processing, the message looses namespace prefix for the Id attribute. This behavior is seen only if a tag and its attribute are declared in different namespaces. Workaround: The namespace prefix of the Id attribute is preserved if it is the same as for the UsernameToken tag. The request could be changed to the following: <code>&lt;a:UsernameToken a:Id=&quot;0123456789&quot;&gt;</code>. In the WSS schema declaration the ‘Id’ attribute is derived from the base XML schema and can be safely changed from one namespace to the other.</td>
</tr>
<tr>
<td>CSCsu51385</td>
<td>Large messages (10s MB) are failed to be processes by ACE Web Application Firewall extensions due to Java out of memory error. Workaround: The amount of memory for SDK host process should be increased (by default it is 128 Mb). The workaround must be applied to every gateway in the cluster. Edit: /usr/local/reactivity/io/init.d/sdk-host Replace default “javaoptions” declaration to javaoptions=&quot;-server -DNETE_TXM_ROOT=/usr/local/reactivity -Dnete.wa.root=/usr/local/reactivity -Xms128M -Xmx1024m&quot; (The value specified in -Xmx option controls the memory limit for SDK process)</td>
</tr>
<tr>
<td>CSCsu82121</td>
<td>If you disable a handler that is configured to receive messages from MQ server using built-in MQ support, the ACE Web Application Firewall continues to receive messages from the corresponding queue, but the handler does not participate in message classification anymore. As result, the Gateway reads messages from the MQ server, but all these messages are rejected by the Gateway with “No handler matched the request” error message. This issue happens if you disable the handler which is configured to receive messages from MQ server using built-in MQ support. There are two possible workarounds: 1. Delete disabled MQ handlers. 2. Use MQ extension. Currently MQ extension provides more functionality than build-in MQ support. This workaround requires policy reconfiguration because configurations for build-in MQ support and for MQ extension are not compatible. Please contact your support representative in order to obtain the latest version of MQ extension.</td>
</tr>
</tbody>
</table>
### Issue ID | Description
--- | ---
CSCsu88285 | Message traffic logging is enabled for at least one handler in the policy. The Message Traffic Log page shows list of messages, but the message body contents are not shown, and the error page appears: “ACE XML Gateway Manager Error. Cannot find message with specified guid:”

Workaround: Message contents can be viewed by entering the direct link in the web browser:

Where message-guid should be taken from the error page.

CSCsv97848 | The ACE Web Application Firewall reports validation error for a SOAP message containing an element with type restriction. The Event Log contains the following validation errors: “XML was not valid: Datatype error” and “XML was not valid: Type “restricted type” that is used in xsi:type is not derived from the type of element”. The validation error appears only for elements which definition is imported from an external schema.

This issue occurs when the policy contains a SOAP Document virtual service with XML schema-based validation switched on. The XML schema has elements with definitions imported from another schema. In requests, this element has type restriction specified. Handler is configured to use the Flex Path.

One of the following solutions is possible:
- Reconfigure handler to use the Reactor;
- Switch off the schema-based validation for SOAP request processing;
- Change requests by removing type restrictions for elements imported from a nested XML schema.

CSCsw42790 | The ACE Web Application Firewall accepts invalid SOAP messages that do not conform to an XML schema definition.

This issue happens when the policy contains Virtual Service or Handler and schema-based validation is switched on for requests passing through the Virtual Service / Handler. Message processing uses the Flex Path.

SOAP message body is formed by elements defined in schema declaration inside a WSDL file, and types of elements are defined in an external schema. The message does not conform XML schema, but the ACE Web Application Firewall accepts it as valid.

Two workarounds are possible:
1. Convert the virtual service or handler to run on the Reactor.
2. Move all schema definitions out of the WSDL file to separate XML schema files.
### Issue ID | Description
---|---
CSCsw72824 | The ACE XML Gateway does not reject a SOAP message that is invalid according to schema-based validation. This issue occurs when the policy contains Virtual Service that runs on the Flex Path. Schema-based validation is switched on for requests passing to this virtual service. An XML schema that defines a body of a SOAP message contains elements that have local namespace declaration.

**Workaround:** Move all namespace declarations from elements to the root `xs:schema` element. For example, if an original schema has the following element declaration:

```xml
<xs:element name="ElementName" type="myns:MyType"
xmlns:myns="MyNamespace"/>
```

Rewrite the schema by moving the namespace declaration “xmlns:myns="MyNamespace"” to the root `xs:schema` element.

CSCsx64191 | Clicking on the “Export as XML” button on the “Compliance Report” page results in the following error: “The Log Query resulted in too much data. Please choose a smaller time range and try again”.

This issue occurs when the compliance report XML export procedure exports three reports at once: message logs, event logs and audit logs. However, exporting reports with more than 5000 entries is not supported. So, if at least one of these reports is greater than 5000 entries, it will result in the “The Log Query resulted in too much data. Please choose a smaller time range and try again” error.

**Workaround:** Choose a smaller time range.

CSCsy07756 | The Exception Mapping for the HTTP POST Body service is configured to pass through all 500 error responses from a backed server to a client. Nevertheless, the backend returns an HTTP 500, “Internal Server Error” with XML/SOAP content type and SOAP body.

**Workaround:** The HTTP POST Body service should be replaced with the SOAP Document service, which allows you to configure SOAP-based errors.

CSCsy23168 | Many browsers provide an autocomplete feature for user input fields. This feature is useful in many situations but it is also a security concern. Browsers can store user information in plain text somewhere on the computer (in the registry, or elsewhere). This issue is possible when many forms in the Manager have password-type input fields.

**Workaround:** Disable autocomplete settings in your browser.
Software Version 6.1 Open Caveats and Resolved Caveats

The following sections contain the open and resolved caveats in software version 6.1:

- Software Version 6.1 Open Caveats
- Software Version 6.1 Resolved Caveats

Software Version 6.1 Open Caveats

The following table lists open caveats.

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCsz77013</td>
<td>The ACE Web Application Firewall does not send body of a response to an HTTP client. This issue occurs when a request goes through the Flex Path. The response from the backend server does not contain “Transfer-Encoding” and “Content-Length” headers (a backend server assumes the message length is determined by closing the server connection). Workaround: 1. Change the backend server settings to use other mechanism for message length specifying. 2. Use the Reactor handler (or the Virtual Web Application) as a proxy for the Flex Path handler.</td>
</tr>
<tr>
<td>CSCsz89814</td>
<td>The Manager stops responding during snapshot generation. This issue happens when data that being packed into the snapshot requires more disk space than currently exists. Workaround: More disk space should be freed on the appliance before snapshot creation starts. For more information contact your support representative.</td>
</tr>
</tbody>
</table>

Software Version 6.1 Open Caveats

- Custom Java-based extensions for the ACE XML Gateway may be vulnerable to CVE-2009-2625. From the RedHat security announcement provided (RHSA-2009:1200-01), the only vulnerability that impacts on the Cisco ACE XML Gateway is CVE-2009-2625 which may potentially allow remote attackers to cause a denial of service (infinite loop and application hang) via malformed XML in custom Java-based extensions. None of the certified Cisco-created extensions are affected by the XML parsing issue. Workaround: N/A

- When using an authenticator that parses the client certificate and verifies it against an LDAP server, the filter input allows copying the certificate credentials using %d. However, if the client certificate includes parentheses anywhere in the subject, the authenticator fails with a message in the logs saying that the filter is invalid. Workaround: N/A
<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCtc16963</td>
<td>The ACE XML Gateway reports “500, Validation Error” on the HTTP DELETE request because of missing attributes even if all required attributes are set. Or the ACE XML Gateway sends the HTTP DELETE request without attributes to a backend server even if it is configured to send attributes. This issue occurs when a route from the HTTP DELETE handler to the HTTP DELETE service descriptor is configured to map or pass through handler attributes to service descriptor attributes. Workaround: N/A</td>
</tr>
</tbody>
</table>
| CSCtc40822 | Valid SOAP messages fail schema validation. This issue happens when:  
- Validation is performed against schema that contains element B, which extends element A of a complex type.  
- The sent message contains an element of type B.  
- The message is processed by the Flex Path handler.  
There are two possible workarounds:  
1. Change the schema declarations to avoid “complex extensions”.  
2. Change the handler settings, to make messages going through the Reactor. |
| CSCsu82121 | If you disable a handler that is configured to receive messages from MQ server using built-in MQ support, the ACE XML Gateway continues to receive messages from the corresponding queue, but the handler does not participate in message classification anymore. As result, the Gateway reads messages from the MQ server, but all these messages are rejected by the Gateway with “No handler matched the request” error message. This issue happens if you disable the handler which is configured to receive messages from MQ server using built-in MQ support.  
There are two possible workarounds:  
1. Delete disabled MQ handlers.  
2. Use MQ extension. Currently MQ extension provides more functionality than build-in MQ support. This workaround requires policy reconfiguration because configurations for build-in MQ support and for MQ extension are not compatible. Please contact your support representative in order to obtain the latest version of MQ extension. |
| CSCsu88285 | Message traffic logging is enabled for at least one handler in the policy. The Message Traffic Log page shows list of messages, but the message body contents are not shown, and the error page appears: “ACE XML Gateway Manager Error. Cannot find message with specified guid:”  
Workaround: Message contents can be viewed by entering the direct link in the web browser:  
Where message-guid should be taken from the error page. |
<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCsv97848</td>
<td>The ACE XML Gateway reports validation error for a SOAP message containing an</td>
</tr>
<tr>
<td></td>
<td>element with type restriction. The Event Log contains the following validation</td>
</tr>
<tr>
<td></td>
<td>errors: &quot;XML was not valid: Datatype error&quot; and &quot;XML was not valid: Type &quot;</td>
</tr>
<tr>
<td></td>
<td>restricted type&quot; that is used in xsi:type is not derived from the type of</td>
</tr>
<tr>
<td></td>
<td>element&quot;. The validation error appears only for elements which definition is</td>
</tr>
<tr>
<td></td>
<td>imported from an external schema. This issue occurs when the policy contains</td>
</tr>
<tr>
<td></td>
<td>a SOAP Document virtual service with XML schema-based validation switched on.</td>
</tr>
<tr>
<td></td>
<td>The XML schema has elements with definitions imported from another schema. In</td>
</tr>
<tr>
<td></td>
<td>requests, this element has type restriction specified. Handler is configured</td>
</tr>
<tr>
<td></td>
<td>to use the Flex Path. One of the following solutions is possible:</td>
</tr>
<tr>
<td></td>
<td>• Reconfigure handler to use the Reactor;</td>
</tr>
<tr>
<td></td>
<td>• Switch off the schema-based validation for SOAP request processing;</td>
</tr>
<tr>
<td></td>
<td>• Change requests by removing type restrictions for elements imported from a</td>
</tr>
<tr>
<td></td>
<td>nested XML schema.</td>
</tr>
<tr>
<td>CSCsw42790</td>
<td>The ACE XML Gateway accepts invalid SOAP messages that do not conform to an</td>
</tr>
<tr>
<td></td>
<td>XML schema definition. This issue happens when the policy contains Virtual</td>
</tr>
<tr>
<td></td>
<td>Service or Handler and schema-based validation is switched on for requests</td>
</tr>
<tr>
<td></td>
<td>passing through the Virtual Service / Handler. Message processing uses the</td>
</tr>
<tr>
<td></td>
<td>Flex Path. SOAP message body is formed by elements defined in schema</td>
</tr>
<tr>
<td></td>
<td>declaration inside a WSDL file, and types of elements are defined in an</td>
</tr>
<tr>
<td></td>
<td>external schema. The message does not conform XML schema, but the ACE XML</td>
</tr>
<tr>
<td></td>
<td>Gateway accepts it as valid. Two workarounds are possible:</td>
</tr>
<tr>
<td></td>
<td>1. Convert the virtual service or handler to run on the Reactor.</td>
</tr>
<tr>
<td></td>
<td>2. Move all schema definitions out of the WSDL file to separate XML schema</td>
</tr>
<tr>
<td>CSCsw72824</td>
<td>The ACE XML Gateway does not reject a SOAP message that is invalid according</td>
</tr>
<tr>
<td></td>
<td>to schema-based validation. This issue occurs when the policy contains Virtual</td>
</tr>
<tr>
<td></td>
<td>Service that runs on the Flex Path. Schema-based validation is switched on for</td>
</tr>
<tr>
<td></td>
<td>requests passing to this virtual service. An XML schema that defines a body</td>
</tr>
<tr>
<td></td>
<td>of a SOAP message contains elements that have local namespace declaration.</td>
</tr>
<tr>
<td></td>
<td>Workaround: Move all namespace declarations from elements to the root xs:schema</td>
</tr>
<tr>
<td></td>
<td>element. For example, if an original schema has the following element</td>
</tr>
<tr>
<td></td>
<td>declaration: &lt;xs:element name=&quot;ElementName&quot; type=&quot;myns:MyType&quot; xmlns:myns=&quot;</td>
</tr>
<tr>
<td></td>
<td>MyNamespace&quot;/&gt; Rewrite the schema by moving the namespace declaration</td>
</tr>
<tr>
<td></td>
<td>&quot;xmlns:myns=&quot;MyNamespace&quot;&quot; to the root xs:schema element.</td>
</tr>
<tr>
<td>CSCsy07756</td>
<td>The Exception Mapping for the HTTP POST Body service is configured to pass</td>
</tr>
<tr>
<td></td>
<td>through all 500 error responses from a backed server to a client. Neverthe-</td>
</tr>
<tr>
<td></td>
<td>less, the backend returns an HTTP 500, “Internal Server Error” with XML/SOA</td>
</tr>
<tr>
<td></td>
<td>P content type and SOAP body. Workaround: The HTTP POST Body service should</td>
</tr>
<tr>
<td></td>
<td>be replaced with the SOAP Document service, which allows you to configure</td>
</tr>
<tr>
<td></td>
<td>SOAP-based errors.</td>
</tr>
<tr>
<td>Issue ID</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCsy10533</td>
<td>The ACE XML Gateway stops accepting SSL traffic. Event Log contains the following warning messages: “OpenSSL Error: hwcrhk engine: HWCRHK_RSA_MOD_EXP: request failed” and “SSL handshake failed”. This issue occurs when the Gateway is configured to use hardware SSL acceleration. Hardware-protected keypairs are used by the Virtual Services of the Gateway. Workaround: To temporary resolve the issue SSL acceleration hardware needs to be restarted: 1. Connect to the appliance using a SSH client. 2. From the shell menu, access the bash prompt and execute “/opt/n/sbin/init.d-nfast restart”. 3. Return to the main menu. 4. Go to “Manage ACE XML Gateway Processes” and choose “Restart All Configured Processes”.</td>
</tr>
<tr>
<td>CSCsz77013</td>
<td>The ACE XML Gateway does not send body of a response to an HTTP client. This issue occurs when a request goes through the Flex Path. The response from the backend server does not contain “Transfer-Encoding” and “Content-Length” headers (a backend server assumes the message length is determined by closing the server connection). Workaround: 1. Change the backend server settings to use other mechanism for message length specifying. 2. Use the Reactor handler (or the Virtual Web Application) as a proxy for the Flex Path handler.</td>
</tr>
<tr>
<td>CSCsz89814</td>
<td>The Manager stops responding during snapshot generation. This issue happens when data that being packed into the snapshot requires more disk space than currently exists. Workaround: More disk space should be freed on the appliance before snapshot creation starts. For more information contact your support representative.</td>
</tr>
</tbody>
</table>
# Software Version 6.1 Resolved Caveats

The following table lists resolved caveats.

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCta06364</td>
<td>A malicious client can enforce a cipher suite not supported by the server to be used for a session between the client and the server. It can result in disclosure of sensitive information. This issue is applicable to all ports for which SSL encryption is used. Workaround: N/A</td>
</tr>
<tr>
<td>CSCta18303</td>
<td>The ACE Web Application Firewall shows low performance numbers in HTTP requests processing. The HTTP transaction rate is about several hundreds per second or less. CPU usage is high and close to 100%. This happens when an HTTP client sends long HTTP requests (GET or POST) with many parameters. The length of the requests is more than 4 KB. The number of parameters is about several thousands. Workaround: N/A</td>
</tr>
</tbody>
</table>
| CSCta33239  | After processing a specific XML request the Flex Path stops accepting traffic. All subsequent requests to the Flex Path result in “503 Service Temporarily Unavailable” response. Approuter process consumes a lot of memory (2GB). The traffic processing can be restored only by restarting the Gateway. To workaround this issue the XML processing should be reconfigured and the following property changed:  
  1. Connect to the Gateway using a SSH client.  
  2. Stop the ACE XML Gateway process.  
  3. From the shell menu, access the bash prompt.  
  4. Edit the file /usr/local/reactivity/config/runtime.properties.  
  5. Set property “xml.allocatorcutoff=0”.  
  6. Save changes and exit from bash.  
  7. Restart the ACE XML Gateway process. |
<p>| CSCta47414  | When a handler is tested using the “Test Handler” option in the Manager, the following error appears “Couldn't make HTTP request: Operation timed out after 10 seconds with 0 bytes received”. This issue occurs if you test a handler with time of response more than 10 seconds. Workaround: Do not use the “Test handler” option for testing handlers with time of response more than 10 seconds. |</p>
<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCta48867</td>
<td>A client receives the response with the status code 401, “Unauthorized” during TCP connection, which was previously used to authenticate this client using NTLM; or a client did not perform NTLM authentication for the connection and succeeds request, which the client is not authorized to make. This issue occurs when several handlers (and service descriptors) routing to the same backend that uses NTLM authentication. Some clients sending requests to those handlers successfully perform NTLM authentication. This issue exists on the Flex Path handlers only. Workaround: Switch handlers from the Flex to the Reactor, if it is possible. <strong>Note</strong> The ACE XML Gateway handlers processed by the Reactor by default and by the Flex Path if it was specifically configured in port settings or if the handler configuration could not be deployed for the Reactor.</td>
</tr>
<tr>
<td>CSCta53171</td>
<td>The ACE XML Gateway Manager is unable to process several requests in the web console simultaneously. This issue is known to occur for product versions 6.0 through 6.0(3). Workaround: N/A</td>
</tr>
<tr>
<td>CSCta54359</td>
<td>Constant growth of memory utilization by reactor processes when the PCI compliance is turned on, excessive memory usage and abnormal termination of reactor worker processes. This issue occurs only under high load. Workaround: Set the “worker.requests” parameter to smaller value (e.g. 10000; default is 100000) to prevent excessive memory usage.</td>
</tr>
<tr>
<td>CSCta66043</td>
<td>The Manager reports “com.reactivity.policy.PolicyGenerationException: Error constructing Ephemeral resources for Endpoint: 320d87cd868c8e3d” during a policy compilation. This error appears when the policy contains SOAP RPC Handlers with empty SOAP Method namespace. Workaround: Provide the valid SOAP Method namespace for the Handler.</td>
</tr>
<tr>
<td>CSCta79944</td>
<td>During policy compilation the following message appears: “Please wait while the policy is compiled... Compile failed. com.reactivity.policy.PolicyGenerationException: Error constructing Ephemeral resources for Endpoint: 3e3b037aadb157bd”. This issue occurs when there is a SOAP Document handler, service descriptor or virtual service (later “object”). The objects’s “SOAP Message Validation” is set to “passive XML schema-based content validation (allow invalid messages)”. In XML schema which is used to validate message the element <a href="">xs:schema</a> lacks the attribute “targetNamespace”. Workaround: Specify “targetNamespace” attribute in the <a href="">xs:schema</a> element. Note it can not be empty, since it is forbidden by the specs.</td>
</tr>
<tr>
<td>CSCta80163</td>
<td>Exception Mapping for handlers is configured to pass through 3xx error codes from a backend server to a client. However, when the backend returns such code, the Service Health treats this request as an error. Workaround: N/A</td>
</tr>
</tbody>
</table>

**Release Note for the Cisco ACE Web Application Firewall**
<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| CSCta80681   | The ACE XML Gateway responds with “500, Unable to connect” error code when the request is POST and contains multipart data without “Content-Type” headers in each part.  
Workaround: N/A                                                                                     |
| CSCtb06407   | The following error message is displayed by the ACE XML Gateway Manager during import of a PPF file:  
“ACE XML Gateway Manager Error  
ACE XML Gateway Manager ran out of memory and cannot complete current operation.  
Manager must be restarted.  
To restart Manager:  
Login into appliance console menu.  
From Manage Gateway Processes menu, choose Stop Manager.  
After Manager stops, choose Start Manager.  
To report this error to Cisco, please submit a diagnostic snapshot to Cisco Support.”  
This issue occurs during a policy import when a large PPF file is being imported.  
Workaround: N/A                                                                                     |
| CSCtb37130   | The Cisco ACE XML Gateway is vulnerable to Libxml2 issues CVE-2009-2414 and CVE-2009-2416.  
Workaround: N/A                                                                                     |
| CSCtb39109   | Growing amount of reactor worker processes. When the amount of reactor worker processes exceeds twice as much as configured in the “reactor.conf” file, traffic stops running through the appliance, because the reactor workers do not accept and process it.  
This issue occurs when the backend server sends a bad response to HEAD-request. For instance, the backend server may close connection without sending any data to a client.  
Workaround: Forbid HEAD-requests in the web application configuration.                                 |
| CSCtb52443   | A request contains one SOAPAction header, but a backend server receives two SOAPAction headers. This issue happens if:  
• There is the “POST Body” handler and the request is processed by this handler.  
• There is the “SOAP Document” handler on the same port (even if this handler is disabled).  
• The “POST Body” handler uses authorizer BasicAuthNoVerifierAuthorizer.  
To resolve this issue the following two steps should be performed:  
1. Remove SOAP handlers.  
2. Change the request processing option for the “POST Body” handler (Virtual Services > Handler: Handler Name [HTTP POST Body], section ROUTES, column “Req. Processing”, press “edit” link): remove all headers mapping and add:  
   • Header Name: *  
   • Action: pass through |
<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| CSCtb65035 | Under certain circumstances, the response from the Reactor is truncated, that is, the length of a response is less than the value provided in the Content-Length header. Both Virtual Services and Virtual Applications are affected by the issue. The issue doesn’t occur when the port is handled by Flex Path. There are two possible workarounds:  
1. For the ACE XML Gateway handler, enable “Always use FlexPath” for the port.  
2. For the Web Application Firewall handler, disable message rewrite rules. |
| CSCtb82159 | If an appropriate error handler is not found during generating a “Message-handling Errors” message, the response discloses the ACE XML Gateway and the ACE Web Application Firewall client internal IP address. This vulnerability affects all product versions of the ACE XML Gateway and the ACE Web Application Firewall earlier 6.1. Though the response by itself does not provide any way to compromise the device, this behavior discloses potentially valuable information about the internal network structure. The disclosed address is not the address of the ACE XML Gateway or the Web Application Firewall, it is an address of its client, which in many cases is a load balancer. The Internal IP address is included in the message-handling errors response if the ACE XML Gateway or the Web Application Firewall was not able to find a matching handler for the request. Workaround: N/A |
| CSCtc12440 | The exemption for a particular rule for cookies has no effect on traffic. The attack is detected in spite of the exemption existence. This issue occurs when the policy contains the Virtual Web Application that has a modifier with the exemption, that should disable some inspection rule for cookies. The traffic contains cookie data that triggers the rule that was disabled by the modifier. The exemption is created via click-to-rule UI. Workaround: N/A |
| CSCtc14500 | The message with an attack vector is not blocked. This issue occurs when:  
1. There are both case-sensitive and case-insensitive signatures.  
2. The case-sensitive signature match partially with the attack vector.  
To resolve this issue all signatures should have the same settings for a nocase parameter. It means that all signatures should be case sensitive or all of them should be case insensitive. |
<p>| CSCsm93017 | In the Performance Monitor page the values of the “Service Latency” for the handler linked with SDK Output Extension are shown in the “Response Processing” column. This issue occurs with the handlers which are linked to SDK Output Extensions, not to standard ACE XML Gateway service descriptors. Workaround: N/A |</p>
<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| CSCsq25244 | It is impossible to reach high TCP connection rates (like 30K connections per second) for more than several seconds. At some point the ACE XML Gateway stops accepting connections during up to two minutes. This issue happens when the ACE XML Gateway is loaded with high TCP connection rate (more than 10K connections per seconds).  
Workaround: Edit the /usr/local/reactivity/scripts/lockdown file. Replace the line “$sudo /sbin/iptables -A $newchain -m state --state NEW -j REJECT” with the “$sudo /sbin/iptables -A $newchain -j REJECT” line. |
| CSCsr61858 | A policy compilation and deployment from the ACE XML Gateway Manager take several minutes. This issue occurs if there are many ACE XML Gateway policies, especially policies containing multiple imported WSDL files, large numbers of service proxies, and/or large resources.  
Workaround: This is a known performance characteristic of the ACE XML Gateway. There is no workaround for this issue. |
| CSCsu63509 | Email notifications from the ACE XML Gateway indicating message processing errors contain insufficient information to determine which subpolicy contains the handler experiencing the error. The email message contains identifiers for the handler and message that produced the error, but these do not produce search results unless are already logged into the relevant subpolicy. This issue affects all versions of the ACE XML Gateway where multiple subpolicies are in use with handlers configured to send email notifications of message processing errors.  
Workaround: Manually switch to every subpolicy in turn and search for the relevant identifiers in each subpolicy independently. |
| CSCsu72318 | If the backup script was run with the parameters –all or –traffic, the script fails with the following error message: “System backup failed: Unable to cpio the system wide files”.  
Workaround: Run the backup script with the following parameters:  
sbin/backup -filestore -userlog -auditlog <tarfilename>  
In this case backup will not contain message traffic statistics. |
The Cisco ACE Web Application Firewall accepts HTTP requests with multiple Content-Length headers. While the product will strip additional Content-Length headers before they reach the backend service, some web application scanning products expect that instead the Web Application Firewall will reject the request with the “400, Bad Request” HTTP response code. The condition occurs when the incoming HTTP request contains more than one Content-Length header. The behavior of WAF does not depend on the chosen web application profile, therefore, in particular it also applies to the built-in “PCI Compliance” profile.

This issue can be worked around by creating a custom rule which places a limit on the number of “Content-length” headers which can be contained in a request. The process for creating custom rules is documented in Chapter 6 of the Cisco ACE Web Application Firewall User’s Guide, “Developing Rules and Signatures”.

Once the custom rule is created, it can be added to an existing or new profile and applied to existing virtual applications.

A sample custom rule file is below:

```plaintext
# Cisco Rule File v. 1.0
# Group declarations
GROUP X-HeaderLimit: Limits on numbers of particular headers
# rule declarations
X-HeaderLimit.ContentLength:REQUEST_HEADER['content-length'].count() gt 1
    name: No more than one content-length header
    sev: 0
```

While running the ACE XML Gateway backup script, the Manager or Gateway process may be shut down. If the available disk space drops below 500 MB while running the backup tool, the Manager and Gateway will be shut down by their respective watchdog processes. The Manager shut down occurs only on the product version 5.2 or later. The Gateway shut down occurs on all supported versions of the product.

However, only processes running on the same appliance as the backup tool will be shut down. Therefore, if backing up a standalone Manager appliance, there is no chance that low disk situation on the Manager will cause any standalone Gateways associated with the Manager to be shut down.

To work around this issue, ensure you have sufficient disk space before executing the backup. To determine the disk space required for the backup, run the backup tool with the desired options and check the size of the resulting file. During the backup process, the backup tool will use up to three times the size of the output file. Delete unneeded files to ensure that there is at least three times the archive size plus 500 MB free before starting a backup.

Also ensure that the backup contains no unnecessary data by specifying the minimal necessary set of flags. For many cases, the most important option is `-f (-filestore)`. 

HTTP header processing works incorrectly when configured for regular expression-based processing. When the action for the HTTP header processing configuration is set to “use regular expression match”, instead of being processed as configured, the header is passed through.

Workaround: N/A

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCsu74152</td>
<td>The Cisco ACE Web Application Firewall accepts HTTP requests with multiple Content-Length headers. While the product will strip additional Content-Length headers before they reach the backend service, some web application scanning products expect that instead the Web Application Firewall will reject the request with the “400, Bad Request” HTTP response code. The condition occurs when the incoming HTTP request contains more than one Content-Length header. The behavior of WAF does not depend on the chosen web application profile, therefore, in particular it also applies to the built-in “PCI Compliance” profile. This issue can be worked around by creating a custom rule which places a limit on the number of “Content-length” headers which can be contained in a request. The process for creating custom rules is documented in Chapter 6 of the Cisco ACE Web Application Firewall User’s Guide, “Developing Rules and Signatures”. Once the custom rule is created, it can be added to an existing or new profile and applied to existing virtual applications. A sample custom rule file is below: # Cisco Rule File v. 1.0 # Group declarations GROUP X-HeaderLimit: Limits on numbers of particular headers # rule declarations X-HeaderLimit.ContentLength:REQUEST_HEADER['content-length'].count() gt 1 name: No more than one content-length header sev: 0</td>
</tr>
<tr>
<td>CSCsu95398</td>
<td>While running the ACE XML Gateway backup script, the Manager or Gateway process may be shut down. If the available disk space drops below 500 MB while running the backup tool, the Manager and Gateway will be shut down by their respective watchdog processes. The Manager shut down occurs only on the product version 5.2 or later. The Gateway shut down occurs on all supported versions of the product. However, only processes running on the same appliance as the backup tool will be shut down. Therefore, if backing up a standalone Manager appliance, there is no chance that low disk situation on the Manager will cause any standalone Gateways associated with the Manager to be shut down. To work around this issue, ensure you have sufficient disk space before executing the backup. To determine the disk space required for the backup, run the backup tool with the desired options and check the size of the resulting file. During the backup process, the backup tool will use up to three times the size of the output file. Delete unneeded files to ensure that there is at least three times the archive size plus 500 MB free before starting a backup. Also ensure that the backup contains no unnecessary data by specifying the minimal necessary set of flags. For many cases, the most important option is <code>-f (-filestore)</code>.</td>
</tr>
<tr>
<td>CSCsv85586</td>
<td>HTTP header processing works incorrectly when configured for regular expression-based processing. When the action for the HTTP header processing configuration is set to “use regular expression match”, instead of being processed as configured, the header is passed through. Workaround: N/A</td>
</tr>
</tbody>
</table>
### Issue ID | Description
--- | ---
CSCsv21241 | SSL warning messages appear in the Event Log. It occurs if the client has a SSL session with the ACE XML Gateway and the client suddenly terminates SSL session.  
Workaround: N/A

CSCsv94979 | The ACE XML Gateway is vulnerable to CVE-2008-4225 and to CVE-2008-4226. This issue occurs when using a large XML document, CVE-2008-4225 allows attackers to cause a denial of service (infinite loop) and CVE-2008-4226 allows attackers to cause a denial of service (memory corruption) or possibly to execute arbitrary code.  
Workaround: N/A

CSCsv98114 | The ACE Web Application Firewall responds with an HTTP Error 400, “Bad Request” on valid HTTP requests. The requests include HTTP headers with a name containing the characters, allowed by RFC 2616 and disallowed by the ACE Web Application Firewall. You must not use the following non-letter characters for header names in the HTTP requests:
- 0-8, 11-31, 127-255!
- “# $ % & ' ( ) * + , ; < = > ? @ [ \ ] ^ ` { | } ~

**Note** However, you can use . / _

Workaround: N/A

CSCsw20411 | While importing an XML schema resource bundle the following error message is displayed: “Could not retrieve the resource from the URL. Target namespace for imported xsd () does not match declared target namespace in import element (custom-element-name)”. This issue occurs when the XML schema resource bundle contains several schema files. One of the files imports another via xsd:include command. A target namespace is declared in the root schema and child schemes have no namespace declared. By specification xsd:include does not require the target namespace to be defined, also it is restricted to be the same as in the parent schema.  
Workaround: The target namespace should be specified in the child schema. The value must be the same as in the parent schema.

CSCsw28573 | When the ACE XML Gateway publishes the WSDL file, it is available only for GET requests containing the “?”WSDL” written in upper case. This may cause interoperability issues with some systems that attempt to download WSDL with a GET request ending with the “?”wsdl” written in lower case.  
Workaround: Two workarounds are possible for this issue:  
1. Set “Always Use Flex Path” mode for the port which is used for WSDL Export feature.  
Modify the third party system to request WSDL using GET requests ending with the “?”WSDL” written in upper case, if it is possible.
**CSCsw40323**  The policy compilation fails and the Manager reports that overlapping operations exist. The issue occurs if the policy contains a multi-operation virtual service and one of its overridden operations was deleted.

To correct the issue the overridden operation needs to be restored and than removed:

1. Go to the virtual service which contains the overridden operation.
2. Click **manage** in the operations section.
3. Check off the overridden operation that needs to be removed.
4. Click Restore Defaults.
5. Remove the operation.
6. Deploy the Policy.

For more information see the *ACE XML Gateway User Guide*, “Working with Multiple Operation Virtual Services”.

**CSCsw45428**  Under certain circumstances, it’s possible for audit log data to become corrupted, resulting in these symptoms:

1. The ACE XML Manager reports that all gateways are unreachable.
2. It’s impossible to create a diagnostic snapshot from the manager (“An error occurred while generating the diagnostic snapshot which prevented it from finishing. Please contact Cisco Support for additional assistance.”).
3. The Policy Changes page cannot be opened, and instead results in an internal error (“ACE XML Gateway Manager Internal Error”).
4. The policy cannot be deployed, with an “ACE XML Gateway Manager Internal Error” reported.

This issue has been observed to occur as a side-effect of disk memory exhaustion on the appliance.

Workaround: Contact your support representative.
<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCsw72558</td>
<td>The ACE XML Gateway doesn't reject SOAP messages that are invalid according to the XML schema applied in the policy. This issue affects SOAP messages that contain elements that use type inheritance. That is, the element is defined by a type inherited from the base type defined in the schema (by xsi:type attribute). The issue appears on Flex Path only. Workaround: This issue occurs due to optimizations used during message validation. These optimizations can be switched off as follows: 1. Access the shell menu on each Gateway appliance in the cluster. 2. Choose “Manage ACE XML Gateway Processes” and then “Stop ACE XML Gateway”. 3. Return to the main menu and choose “Advanced Options” and then “Bash”. 4. Edit the file “/usr/local/reactivity/config/runtime.properties”. 5. Add the following line into the file: xmlschema.validation.simple.maxdocs=0 6. Save changes and exit from bash. 7. Restart Gateway processes using “Manage ACE XML Gateway Processes” &gt; “Start ACE XML Gateway”.</td>
</tr>
<tr>
<td>CSCsw72869</td>
<td>The ACE XML Gateway doesn't reject an invalid SOAP messages that do not conform to an XML schema. The policy is created by importing a WSDL file that contains two schemas. Elements from the first schema refer to types defined in the second. Restrictions applied to types in the nested schema have no effect on message validation. Workaround: Two workarounds for this issue are possible: 1. Configure the virtual service or handler for Reactor processing rather than Flex Path processing. 2. Move all schema definitions from the WSDL file to separate XML schema files.</td>
</tr>
<tr>
<td>CSCsw78346</td>
<td>A URL contains UTF-8 symbols which consist of 5 or 6 bytes passes to a backend server without normalization. This issue occurs since the ACE XML Gateway does not support normalization neither 5 nor 6 bytes UTF-encoded symbols. Workaround: N/A</td>
</tr>
<tr>
<td>CSCsw77349</td>
<td>If you want to remove the Public/Private Keypair component, the error message appears “cannot be deleted because it is in use by another sub-policy”. Such message is shown when the shared policy contains the Public/Private Keypair component that is used as a SSL keypair by one or several components in some subpolicies (for example by the HTTP Server). In this case it is impossible to understand from message, in which subpolicy this component is located. Workaround: N/A</td>
</tr>
<tr>
<td>Issue ID</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| CSCsw78416  | The Event Log contains a warning messages stating about XML validation errors for requests sent to the virtual web application. This issue occurs if the requests sent to the virtual web application contains the following strings:  
  - text/xml  
  - application/xml  
  - application/soap+xml  
  **Note**  
  “123text/xml345” is affected too, since it contains the “text/xml” content type.  
  Workaround: N/A                                                                                     |
| CSCsw78835  | Appliance disk space on the ACE XML Gateway or Manager can be exhausted by policy history data. This issue may occur if a large policy is deployed many times (hundreds). Currently there is no rotating mechanism for the policy history data.  
  Workaround: Contact your support representative.                                                   |
| CSCsw96962  | The ACE XML Gateway is vulnerable to CVE-2008-5077. This issue occurs when an attacker in control of a malicious server, or able to effect a “man in the middle” attack, could present a malformed SSL/TLS signature from a certificate chain to a vulnerable client and bypass validation.  
  Workaround: N/A                                                                                     |
| CSCsx17741  | Response processing configuration is not available in SOAP Document handler when response validation is set to “must be empty”.  
  Workaround: If response processing is required on empty responses, POST body handler may be used to partially emulate the SOAP Document handler.  
  When POST Body handler is used instead of the SOAP Document handler, request header processing must be configured to send appropriate SOAPAction header to a backend server. |
| CSCsx19437  | The ACE XML Gateway appliance, acting as an SSL server, sends out only the “leaf” or “end entity” server certificate, despite the attempts to get it to send out a certificate chain by uploading the intermediate and/or root CAs as Trusted Certificate Resources.  
  Normally the ACE XML Gateway includes CA certificates from the Trusted CA Resource list that chain up from the SSL server certificate and include them into the outgoing chain. This behavior is suppressed by setting the SSLVerifyClient to “none”.  
  Workaround: Set SSLVerifyClient back to the default value “optional_no_ca”.                           |
<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
</table>
| CSCsx26223 | When the ACE Web Application Firewall is used under high load, while accessing a website through the firewall, it can take about a minute to open a page. Memory usage statistics shows that all swap memory space is used. This issue occurs when in the “reactor.conf” file the property ‘worker.processes’ is set to 16 or higher. To correct this issue:  
   1. Connect to the appliance using a SSH client.  
   2. From the shell menu, access the bash prompt.  
   3. Edit /usr/local/reactivity/io/conf/reactor/conf file using vi:  
      - set worker.processes configuration value to 8;  
      - uncomment “worker.openfiles” (if it was commented);  
      - set worker.openfiles configuration value to 4096;  
      - save changes and exit from vi;  
   4. Exit from bash.  
   5. Restart the Gateway. |
| CSCsx26510 | The overall Manager performance is low. Some pages are slow and processed in several seconds or minutes. If there are several active users in the Manager it can take some minutes to process even a relatively fast page. This issue occurs when you try to access one of potentially slow pages and/or other users work in the Manager at the same time. Potentially slow pages are those that require much data processing or heavy communication with gateways. Such pages include: Message Traffic Log, Event Log, Performance Monitor and Dashboard. Workaround: N/A |
| CSCsx47192 | The rollback process starts but fails with:  
   “WARNING: rollback had problems, please contact Reactivity support  
   END - Rolling back to ACE XML Gateway release 4.4.2-937 FAILED with RESULT 177  
   Halting Installation”.  
   The issue occurs when free disk space is less than 1GB.  
   Workaround: Before starting rollback operation, clean the disk to provide sufficient amount of free disk space. |
| CSCsx58933 | The ACE XML Gateway responds with “500, Unable to connect” error code and the following message appears in the Event Log “generic error in HTTP library (internal error: (65) necessary data rewind wasn't possible)”. This issue occurs when the ACE XML Gateway handler is configured on the backend server with NTLM authentication and the sent message is larger than approximately 16 KB. Workaround: N/A |
| CSCsx72789 | The following warning message appears in the Event Log:  
   “WARNING: regular expression execution returned an error (-10)”. The issue may happen when the string (specifically, header values) that matched by some signature's DFA contains some unicode characters. |
### Issue ID Description

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCsx73068</td>
<td>The ACE XML Gateway responds with a “503, Service unavailable”, an error message “Dangling message” appears in the Event Log. This issue occurs when: 1. The content-screening rule is enabled on response HTTP headers on the Flex Path. 2. An HTTP response message contains more than one header with the same name and all of them match with content screening. Workaround: N/A</td>
</tr>
<tr>
<td>CSCsx73427</td>
<td>The content screening rules do not change the matched value of HTTP headers. This issue happens when the ACE XML Gateway is configured to perform content screening rules on response and HTTP headers are on the Flex Path. The content screening rule specifies that processing of the matched message should be continued and the matched value should be replaced with other specified value.</td>
</tr>
<tr>
<td>CSCsy04750</td>
<td>The ACE XML Gateway fails to send a SOAP request with an attachment to a backend server. The event log contains the following warning messages: “Unable to make request: send error while sending to “XXX” (internal error: curl(55) Unhandled HTTP result code 0)” and “Request failed for message: Generic error”. This issue occurs when the ACE XML Gateway uses uppercase spelling of “Content-Length” header (“CONTENT-LENGTH”) for SOAP requests with an attachment. According to the RFC 2616, headers in requests should be regarded in a case-insensitive manner. However, there are backend servers that do not accept the content-length header unless it is capitalized as “Content-Length”. Workaround: N/A</td>
</tr>
<tr>
<td>Issue ID</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| CSCsy10769 | A custom error message is not shown for authentication failure for the SOAP handler with multiple routes. Instead of it a default text is shown: “Forbidden. You are not allowed to access that resource.” This issue occurs when a policy has a virtual service constructed from a handler and multiple routes to services. The Exception Mapping for “Authentication or authorization failure” is configured on every route. The default route for the handler is not specified. Workaround: The Exception Mapping settings for a non-default route has no influence on processing of authentication failure. There are two workarounds possible. 1. Specify the default Exception Mapping for authenticator or authorization failure. To configure the default Exception Mapping:  
   • Choose “Exception Mapping Defaults” in the Shared policy;  
   • Select the SOAP option for “Mappings for handlers of type”;  
   • Configure the request exceptions for the “Authentication or authorization failure” type.  
   2. Add the default route to the fixed response service and change its Exception Mapping. If the incoming request cannot be classified, the ACE XML Gateway returns generic SOAP response with information that there’s no a handler matching the request. To emulate this behavior default route should go to the fixed response service returning “not-found” message.  
   • Create the fixed response server and set it to return HTTP code 404, or more sophisticated response e.g. a SOAP message with specific Fault string.  
   • Create the SOAP service to the server from 1.  
   • In the virtual service add default route to the service from 2.  
   • Configure the Exception Mapping for the default route. |
| CSCsy23176 | The ACE XML Gateway Manager application is vulnerable to some cross-site scripting (XSS) attacks. Workaround: N/A |
| CSCsy54602 | In some cases the chained update from the version 5.2 to 6.0(3) fails while updating to 6.0(2). The updater fails with the following message: 
“./doUpdate.sh: line 843: cd: /var/lib/reactivity/console_documents/cluster/stats: No such file or directory”. Workaround: Remove the “/var/lib/reactivity/console_documents/cluster” directory and restart the chained updater. |
<p>| CSCsy76596 | The Manager stops accepting new requests. A browser is waiting for the page to load, until an error is displayed. It occurs when the Manager processes a request for a long time and fails with internal error. The issue appears on the pages that show message traffic log and message details. Workaround: Restart the Manager process. |</p>
<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCsy76651</td>
<td>After deploying a policy, the HTTP service does not start. The event logs contain the following warnings: “Syntax error on line... of... httpd.conf”. The issue occurs after the policy compilation and deployment. It happens rarely, but the longer compilation the more probable this issue. Workaround: Compile and deploy the policy once again.</td>
</tr>
<tr>
<td>CSCsy84529</td>
<td>The Message Traffic Log with all default settings shows just a small number of messages. However, if the filter is selected for a specific handler the list contains all messages. This issue appears if the manager policy contains several subpolicies and handlers with message traffic log enabled in these subpolicies. Traffic is sent to different handlers. Simple search on the Message Traffic Log page is used to view a list of messages. Workaround: N/A</td>
</tr>
<tr>
<td>CSCsy87207</td>
<td>There is a message in the event log: Exception while receiving data from back end: “Malformed RFC822 Header caused by premature end of input”. This issue occurs when a backend server uses LF as a header delimiter and a virtual service uses the Flex Path. Workaround: Disable all features that cause the virtual service to use the Flex Path.</td>
</tr>
<tr>
<td>CSCsy93647</td>
<td>The snmp process does not stay running when multiple ethernet interfaces are bonded to work as a single interface. snmp.log-messages: error on subcontainer “ ” insert (-1) error on subcontainer “ia_addr” insert (-1) error on subcontainer “ia_index” insert (-1) error on subcontainer “ia_addr” insert (-1) ... arch ipaddress copy failed This issue occurs when a bonding device exists in the system. Snmpd process starts but fails in several minutes. Workaround: Bonding must not be used, since it is not supported. SNMP works without bonding.</td>
</tr>
</tbody>
</table>
| CSCsz16342 | Acunetix scanner shows XSS vulnerabilities in the Manager. This problem takes place when one of the following types of the extensions is installed:  
  - Service  
  - Authenticator  
  - Transformer  

| CSCsz16549 | Low number of processed requests per second. The “Top” command shows high CPU usage. This issue occurs when HTTP requests contain “Cookie” headers with length more than 2 KB. The cookie header contains large number of attributes. Workaround: N/A                                                                 |
| CSCsz21388 | A request consisting of attack vector may be passed through, if the attack vector is located in the second or consequent cookie headers. Workaround: N/A                                                                                                               |
**Issue ID** | **Description**
--- | ---
CSCsz25031 | The ACE XML Gateway is not able to import VIPS from the ACE starting from version 2(1.3). This issue occurs when the class-map uses “eq” operator in matching rule like “match virtual-address 1.1.1.1 tcp eq www”.

There are two workarounds are possible:

1. Use “range” operator in matching, like “match virtual-address 1.1.1.1 tcp range 80 81”.
2. Do not import VIPS, just add Virtual Server manually.

CSCsz28969 | Policy deployment fails with the message “Policy deployment failed due to a communication error: Policy was not successfully sent to the following host(s): <hostnames>”. This issue may occur when the policy is large.

Workaround:

1. Access the shell menu on each Gateway appliance in the cluster.
2. From the shell menu choose “Advanced Options” and then “Bash”.
3. Open the /usr/local/reactivity/config/runtime.properties file.
4. Change the “byte.array.reload.to.memo ry.fail.limit” parameter from 10240000 to 20240000 (It will allow approuter to accept policies of larger size).
5. Return to the console interface and restart the Gateway: choose “Manage ACE XML Gateway Processes” > “Stop ACE XML Gateway” > “Manage ACE XML Gateway Processes” > “Start ACE XML Gateway”.

CSCsz43132 | Reactor does not accept new connections. Static content on the port does not respond. An attempt to test the handler from the Manager fails with the error “ACE XML Gateway has encountered a problem and was unable to complete the request. Couldn't make HTTP request: SSL connection timeout.”. This issue occurs if an appliance in the network (e.g. load-balancer) constantly sends TCP or HTTP probes to the ACE XML Gateway.

To workaround this issue:

1. To avoid encountering the issue, the Reactor process can be periodically restarted.
2. If TCP or HTTP probes are not related to the network functionality, they can be blocked on the ACE XML Gateway appliances by IP tables configuration.
3. Increase allowed file handlers for workers and decrease the worker life time. To apply the workaround edit the “/usr/local/reactivity/io/conf/reactor.conf” file, set “worker.openfiles=16384” and “worker.requests=8000”, restart reactor IO process from the gateway manager.

**Note** This change can decrease performance of the gateway.
Software Release 6.1(1) Update Notes

To upgrade a system from the previous software version 6.1, you should use the 6.1(1) updater. To update from an earlier version, you can use the chained updater. The chained updater applies multiple updates sequentially, and can be used to update your system from version 5.2 or later.

Step-by-step procedures for applying the update are documented in the Administration Guide.

Applying the Software Update

This section describes how to update your ACE XML Gateway or ACE Web Application Firewall appliance to the latest software version. You can apply updates to the appliance using either the chained updater or the non-chained updater. A chained updater upgrades the appliance by more than one version; a non-chained updater applies a single incremental version update. The steps for using each are similar, however, as described here.

Before performing the update, carefully read the Release Note document for the software source and target versions you are applying. If using a chained updater, be sure to read the individual release notes for each version applied by the updater, not just the release note applicable to the final version.

An ACE XML Gateway or ACE Web Application Firewall deployment consists of one or more gateway or firewall appliances and at least one Manager, the administrative server for the system. If updating a live deployment with multiple appliances, the order in which you update the appliances is important. You should update the Manager first, then any gateways or firewalls in the Manager’s control. If there is more than one gateway or firewall in the Manager’s control, use a rolling upgrade procedure to avoid service downtime. The following steps provide an example upgrade procedure. This example assumes that a load balancer exists upstream from a cluster of gateways or firewalls.

1. Apply the update to the Manager. When finished, make sure you can access the Manager web console.

2. Once you have confirmed the update on the Manager, disable or take out the first gateway or firewall from the server farm group configuration of the upstream load balancer.

3. Apply the update to the first gateway or firewall.

4. When finished, deploy the policy selectively from the Manager to the updated gateway or firewall.

### Issue ID Description

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCsz48115</td>
<td>Several pages in the Manager are vulnerable for XSS attacks. The Manager was tested by the Acunetix security scanner. A number of pages are found to be vulnerable for the XSS attacks. Workaround: N/A</td>
</tr>
<tr>
<td>CSCsz70421</td>
<td>After a system update from version 5.2 or earlier to 6.0 or any 6.0(x) versions the following rules disappear from the “Content Screening” page: com.reactivity.privacy.Financial.1 com.reactivity.privacy.Medical.1 com.reactivity.privacy.Personal.1 If they were configured for a handler/service descriptor or globally before update, they are still active and can not be disabled. Workaround: Contact your support representative.</td>
</tr>
</tbody>
</table>
5. Re-enable the updated gateway or firewall in the server farm of the upstream load balancer.
6. Remove the second gateway or firewall from the server farm.
7. Apply the update to the second gateway or firewall.
8. Deploy the policy to the second gateway or firewall, and put it back in the server farm.
9. Repeat steps 6 through 8 for each gateway or firewall in the server farm.

The updater script is intended to be run on an appliance that has received at least one policy deployment from the Manager. That is, you should not attempt to run the updater script on an appliance that is in its initial, factory-default state. If necessary, deploy from the Manager to all appliances at least once before running the updater. (The policy that is deployed does not need to include any special configuration—a default policy will work.)

If an update fails for any reason, please contact your Cisco support representative.

Obtaining the Updater

To acquire the version 6.1(1) software updater, perform these steps:

**Step 1** At www.cisco.com, from the **Support** menu, click **Download Software**.

**Step 2** Choose **Application Networking Software** in the software product category list.

**Step 3** Log in, if prompted.

**Step 4** From the product list, click on **Cisco ACE XML Gateway**.

**Step 5** Click on the link for the major release version you are attempting to update.

**Step 6** From the file list, download the version 6.1(1) distribution archive for either the chained or non-chained updater. Chained updater starts from the version 5.2 and later; non-chained updater starts from the version 6.1 only.

**Step 7** After downloading the archive, transfer it to a directory location on the target appliance, such as to the /tmp directory.

**Note** In general, the /tmp directory on the appliance should be used for storing temporary files, such as the updater archive. The contents of this directory are purged automatically after they have been on the appliance for 10 days.

**Step 8** Verify the distribution as follows:

a. Change to the directory in which you have put the distribution archive:
   
   cd /tmp

b. Check the validity of the archive by issuing the md5sum command against it, as follows:
   
   md5sum axg-update-<target_build>-from-<source_build>.tar.gz

Once the distribution has been validated, you can run the updater script, as described next.
Running the Updater

Once you’ve acquired the update archive, follow these steps to update the software on the appliance:

**Step 1** Unpack the distribution archive, as follows:
```
tar xzf axg-update-<target_build>-from-<source_build>.tar.gz
```

**Step 2** Change the current directory to the newly created directory:
```
cd axg-update-<target_build>-from-<source_build>
```

**Step 3** Run the update script from the extracted update distribution directory, as follows:
```
./doUpdate.sh
```

The updater first looks for conditions that may prevent it from successfully applying the update. If it finds such conditions, the update is cancelled. If this occurs, contact your support representative.

The updater also warns you if it detects other types of unusual conditions, such as changes to non-configuration files. The script offers you the opportunity to interrupt the update to save the files or make any other changes before proceeding.

After the initial system validity check, the updater presents the following prompt:

The statistics databases need to be checked for consistency before the update can begin.
That required shutting down the ACE XML Manager for about one minute.
Do you want to continue at this time?

Enter “no” (or “n”) if you want to cancel the update or enter “y” to continue.

If you enter “y”, the script shuts down the system to perform the performance data consistency. If the database is found to be valid, the update proceeds as normal. If the database is found to be invalid, text such as the following appears:

```
Error: status database cluster62064/status is corrupted (code 1).
At least one cluster has a corrupted database. They must be repaired in order for the update to proceed.
NOTE: if the database cannot be repaired, it will be deleted.
Do you want to repair the databases during update?
```

Enter “y” to have the database repaired if possible. As noted, performance data may be lost if the database cannot be repaired. If you enter “n”, the update is cancelled.

**Note**
Updater will not proceed if any hotfix is installed. It is not possible to update some appliances with old nCipher firmware version, since the nCipher drivers have been changed to be compatible with Java 1.6. The updater can be cancelled while in progress at certain times. Those times are indicated by onscreen instructions (which read in part “C to abort”). Only cancel the updater (by pressing Ctrl-C) if the onscreen instructions indicate it is possible to do so.

When a version update is completed, the appliance is rebooted. This occurs once for the non-chained updater and multiple times for the chained updater, once for each version update in the chain.

If you are performing the update from an SSH client, keep in mind that you will be disconnected at the first reboot, and informational messages will no longer appear. When the update is finished, you can view the information message in the updater log file located in the following directory: /var/log/reactivity/
You can verify that the chained updater has completed by logging into the Manager Console and examining the event log. If the update is still in progress, the connection from the browser to the web console will be refused. When it is finished, a Notice-level item will appear in the event log indicating the identifier of the new version running on the appliance, such as: “Running release 6.1-2009-10-20T15”. After the chained update, each version will appear in the event log.

Note Do not proceed to the next step until a message indicating that the target version is running appears in the Event Log.

Step 4 The policy and general state of the console policy should not appear substantially different from the pre-updated version. Inspect it to be sure. Contact your support representative if you find anything in the policy that looks unusual or unexpected.

After all other appliances have been updated, recompile and deploy the policy from Manager. When finished, your system is updated to the latest software version and ready for use.

Rolling Back an Update

It’s possible to roll back a successful update. The rollback script included in the update distribution (doRollback.sh) restores an appliance to its state before the update was applied.

A rollback should NOT be attempted unless you are certain that the original update has completed successfully. After a chained update, you must use the same, extracted updater that was used to perform the original update. You cannot use an updater that has not been run, including an updater newly extracted from the original distribution archive.

Caution In general, it is strongly recommended that you contact Cisco support BEFORE attempting a rollback.

Related Documentation

The following documents provide information on the ACE XML Gateway product:

- ACE XML Gateway User Guide
- ACE XML Gateway Quick Start Guide
- ACE XML Gateway Administration Guide

The ACE Web Application Firewall product documents are:

- ACE Web Application Firewall User Guide
- ACE Web Application Administration Guide
- ACE Web Application Getting Started Guide
- ACE XML Gateway Quick Start Guide (included in the appliance packaging)