CNS Security Enhancement

First Published: June 19, 2006
Last Updated: June 19, 2006

The CNS Security Enhancement feature improves the security of Cisco Networking Services (CNS) messages by authenticating sender credentials through the use of the Service-Oriented Access Protocol (SOAP) message format.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for CNS Security Enhancement" section on page 16.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Restrictions for CNS Security Enhancement

- CNS must be enabled.

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

Information About CNS Security Enhancement

To configure the CNS Security Enhancement feature, you should understand the following concepts:

CNS

CNS is a foundation technology for linking users to networking services and provides the infrastructure for the automated configuration of large numbers of network devices. Many IP networks are quite complex, having many devices, and currently each device must be configured individually. When standard configurations do not exist or have been modified, the time involved in initial installation and subsequent upgrading is considerable. Also, the volume of smaller, more standardized, customer networks is increasing faster than the number of available network engineers. Internet service providers (ISPs) now need a method for sending out partial configurations to introduce new services.

To address all these issues, CNS has been designed to provide “plug-and-play” network services using a central directory service and distributed agents. CNS features include CNS configuration and event agents and a flow-through provisioning structure. The configuration and event agents use a CNS configuration engine to provide methods for automating initial Cisco IOS device configurations, incremental configurations, and synchronized configuration updates, and the configuration engine reports the status of the configuration load as an event to which a network monitoring or workflow application can subscribe. The CNS flow-through provisioning uses the CNS configuration and event agents to provide an automated workflow, eliminating the need for an on-site technician.

CNS Security

Before the introduction of the CNS Security Enhancement feature, the CNS message format did not support security. Using the new CNS SOAP message structure, the username and password are authenticated.

If Authentication, Authorization, and Accounting (AAA) is configured, then CNS SOAP messages will be authenticated with AAA. If AAA is not configured, there will be no authentication. For backward compatibility, CNS will support the existing non-SOAP message format and will respond accordingly without security.

The **cns aaa authentication** command is required to turn on CNS Security Enhancement. This command determines whether the CNS messages are using AAA security or not. If the **cns aaa authentication** command is configured, then all incoming SOAP messages into the device are authenticated by AAA.

CNS Message Formats

SOAP Message Format

Using the SOAP protocol provides a way to format the layout of CNS messages in a consistent manner. SOAP is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. SOAP uses extensible markup language (XML) technologies to define an extensible messaging framework that provides a message format that can be exchanged over a variety of underlying protocols.

Within the SOAP message structure, there is a security header that enables CNS notification messages to authenticate user credentials.

CNS messages are classified into three message types: request, response and notification. The formats of these three message types are defined below.

Request Message

The following is the format of a CNS request message to the Cisco IOS device:

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://www.w3.org/2003/05/soap-envelope">
 <SOAP:Header>
  <wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext" >
    <wsse:usernameToken SOAP:mustUnderstand="0">
     <wsse:Username>john</wsse:Username>
     <wsse:Password>cisco</wsse:Password>
    </wsse:usernameToken>
   </wsse:Security>
   <cns:cnsHeader version="1.0" xmlns:cns="http://www.cisco.com/management/cns/envelope">
    <cns:Agent>CNS_CONFIG</cns:Agent>
    <cns:Request>
     <cns:correlationID>IDENTIFIER</cns:correlationID>
     <cns:ReplyTo>
        <cns:URL>http://10.1.36.9:80/cns/ResToServer</cns:URL>
     </cns:ReplyTo>
    </cns:Request>
    <cns:Time>2003-04-23T20:27:19.847Z</cns:Time>
   </cns:cnsHeader>
  </SOAP:Header>
  <SOAP:Body xmlns="http://www.cisco.com/management/cns/config">
   <config-event config-action="read" no-syntax-check="TRUE">
    <config-data>
     <config-id>AAA</config-id>
     <cli>access-list 1 permit any</cli>
   </config-data>
  </config-event>
 </SOAP:Body>
</SOAP:Envelope>
```

Note The ReplyTo field is optional. In the absence of the ReplyTo field, the response to the request will be sent to the destination where the request originated. The body portion of this message contains the payload and is processed by the CNS agent mentioned in the Agent field.

Response Message

The following is the format of a CNS response message from the Cisco IOS device as a response to a request:

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://www.w3.org/2003/05/soap-envelope">
 <SOAP:Header>
  <wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
SOAP:mustUnderstand="true">
   <wsse:UsernameToken>
    <wsse:Username>infysj-7204-8</wsse:Username>
    <wsse:Password>NTM3NTg2NzIzOTg2MTk2MjgzNQ==</wsse:Password>
   </wsse:UsernameToken></wsse:Security>
   <CNS:cnsHeader Version="2.0" xmlns:CNS="http://www.cisco.com/management/cns/envelope">
```

```
   <CNS:Agent>CNS_CONFIG</CNS:Agent>
   <CNS:Response>
     <CNS:correlationID>IDENTIFIER</CNS:correlationID>
   </CNS:Response>
   <CNS:Time>2005-06-23T16:27:36.185Z</CNS:Time>
  </CNS:cnsHeader>
 </SOAP:Header>
 <SOAP:Body xmlns="http://www.cisco.com/management/cns/config">
   <config-success><config-id>AAA</config-id></config-success>
 </SOAP:Body>
</SOAP:Envelope>
```

Note The value of CorrelationId is echoed from the corresponding request message.

The body portion of this message contains the response from the Cisco IOS device to a request. If the request is successfully processed, the body portion contains the value of the response put in by the agent that processed the request. If the request cannot be successfully processed, then the body portion will contain an error response.

Notification Message

The following is the format of a CNS notification message sent from the Cisco IOS device:

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://www.w3.org/2003/05/soap-envelope">
 <SOAP:Header>
  <wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
SOAP:mustUnderstand="true">
   <wsse:UsernameToken>
    <wsse:Username>dvlpr-7200-2</wsse:Username>
    <wsse:Password></wsse:Password>
   </wsse:UsernameToken>
  </wsse:Security>
  <CNS:cnsHeader version="2.0" xmlns:CNS="http://www.cisco.com/management/cns/envelope">
   <CNS:Agent>CNS_CONFIG_CHANGE</CNS:Agent>
   <CNS:Notify></CNS:Notify>
   <CNS:Time>2006-01-09T18:57:08.441Z</CNS:Time>
  </CNS:cnsHeader>
 </SOAP:Header>
 <SOAP:Body xmlns="http://www.cisco.com/management/cns/config-change">
  <configChanged version="1.1" sessionData="complete">
   <sequence lastReset="2005-12-11T20:18:39.673Z">7</sequence>
   <changeInfo>
    <user></user>
    <async><port>con_0</port></async>
    <when>
     <absoluteTime>2006-01-09T18:57:07.973Z</absoluteTime>
    </when>
   </changeInfo>
   <changeData>
    <changeItem>
     <context></context>
     <enteredCommand>
      <cli>access-list 2 permit any</cli>
     </enteredCommand>
     <oldConfigState>
      <cli>access-list 1 permit any</cli>
     </oldConfigState>
     <newConfigState>
      <cli>access-list 1 permit any</cli>
      <cli>access-list 2 permit any</cli>
```

```
     </newConfigState>
    </changeItem>
   </changeData>
  </configChanged>
 </SOAP:Body>
</SOAP:Envelope>
```

A notification message is sent from the Cisco IOS device without a corresponding request message when a configuration change is made. The body of the message contains the payload of the notification and it may also contain error information. If the request message sent to the Cisco IOS device fails in XML parsing and the CorrelationId field cannot be parsed, then an error notification message will be sent instead of an error response.

Error Reporting

Error is reported in the body of the response or a notification message in the SOAP Fault element. The following is the format for reporting errors.

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://www.w3.org/2003/05/soap-envelope">
 <SOAP:Header>
  <wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/04/secext"
SOAP:mustUnderstand="true">
   <wsse:UsernameToken>
    <wsse:Username>dvlpr-7200-2</wsse:Username>
    <wsse:Password></wsse:Password>
   </wsse:UsernameToken>
  </wsse:Security>
  <CNS:cnsHeader version="2.0" xmlns:CNS="http://www.cisco.com/management/cns/envelope">
   <CNS:Agent>CNS_CONFIG</CNS:Agent>
   <CNS:Response>
    <CNS:correlationID>SOAP_IDENTIFIER</CNS:correlationID>
   </CNS:Response>
   <CNS:Time>2006-01-09T19:10:10.009Z</CNS:Time>
  </CNS:cnsHeader>
 </SOAP:Header>
 <SOAP:Body xmlns="http://www.cisco.com/management/cns/config">
   <SOAP:Detail>
    <config-failure>
     <config-id>AAA</config-id>
     <error-info>
      <line-number>1</line-number>
      <error-message>CNS_INVALID_CLI_CMD</error-message>
     </error-info>
    </config-failure>
   </SOAP:Detail>
  </SOAP:Fault>
 </SOAP:Body>
</SOAP:Envelope>
```

How to Configure CNS Security Enhancements

This section contains the following tasks:

- Configuring the CNS Configuration Agent, page 6 (required)
- Configuring the CNS Event Agent, page 7 (required)

- Configuring the CNS Image Agent Using the CLI, page 8 (optional)
- Configuring the Authentication of End-User Credentials in Incoming CNS Messages, page 11 (optional)

Configuring the CNS Configuration Agent

Use the following commands to configure the CNS configuration agent:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cns config initial**
4. **cns event**
5. **cns config partial**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cns config initial** **Example:** `Router(config)# cns config initial`	Downloads an initial configuration to the router when it boots up.
Step 4	**cns event** **Example:** `Router(config)# cns event`	Establishes a TCP connection with the Event Gateway. This connection is required for the router to request or receive incremental updates.
Step 5	**cns config partial** **Example:** `Router(config)# cns config partial`	Enables the partial Configuration Agent. The partial Configuration Agent is required for the router to request or receive updates.

Configuring the CNS Event Agent

Use the following commands to configure the CNS Event Agent:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cns event**
4. **exit**
5. **show cns event**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cns event** **Example:** `Router(config)# cns event`	Configures the Event Gateway for CNS.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 5	**show cns event** **Example:** `Router# show cns event`	(Optional) Displays information about the CNS event agent.

Configuring the CNS Image Agent Using the CLI

Use the following commands to configure the CNS image agent using the CLI:

CNS Image Agent ID

CNS uses a unique identifier to identify an image agent associated with that Cisco IOS device. Using the same process as CNS event and configuration agents, the configuration of the **cns id** command determines whether an IP address or MAC address of a specified interface, the hardware serial hardware number of the device, an arbitrary text string, or the hostname of the device is used as the image ID. By default, the system uses the hostname of the device.

The CNS image ID is sent in the content of the messages sent by the image agent and allows an application to know the unique image ID of the Cisco IOS device that generated the message. A password can be configured and associated with the image ID in the image agent messages.

Prerequisites

- To configure the CNS image agent to use HTTP or HTTP over Secure Socket Layer (HTTPS) to communicate with an image server, you need to know the URL for the image server and the URL to which status messages can be sent.
- If you are using HTTPS to communicate with the image server, you must set up security certificates to allow the server to be authenticated by the image agent when the connection is established.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cns id** *type number* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**]
   or
   cns id {**hardware-serial** | **hostname** | **string** *text*} [**event**] [**image**]
4. **cns image** [**server** *server-url* [**status** *status-url*]]
5. **cns image password** *image-password*
6. **cns image retry** *seconds*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**cns id** *type number* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**]
	
	or
	
	cns id {**hardware-serial** | **hostname** | **string** *text*} [**event**] [**image**]
	
	Example:
	`Router(config)# cns id fastethernet 0/1 ipaddress image`
	
	or
	
	Example:
	`Router(config)# cns id hardware-serial image`
		Specifies a unique CNS ID and interface type and number from which to retrieve the unique ID.
		or
		Specifies a unique CNS ID assigned from the hardware serial number, device hostname, or an arbitrary text string.
		The following information applies to either version of the syntax.
		• Use the **event** keyword to specify an event agent ID.
		• Use the **image** keyword to specify an image agent ID.
		• If no keywords are used, the configuration agent ID is configured.

Step 4	**cns image** [**server** *server-url* [**status** *status-url*]] **Example:** `Router(config)# cns image server https://10.21.2.3/cns/imgsvr status https://10.21.2.3/cns/status/`	Enables CNS image agent services and specifies the URL of the image distribution server. • Use the optional **status** keyword and *status-url* argument to specify the URL of a web server to which error messages are written. • If the **status** keyword and *status-url* argument are not specified, status messages are sent as events on the CNS Event Bus. To view the status messages on the CNS Event Bus, the CNS event agent must be configured.
Step 5	**cns image password** *image-password* **Example:** `Router(config)# cns image password abctext`	(Optional) Specifies a password for CNS image agent services. • If a password is configured, the password is included with the image ID in CNS image agent messages sent out by the image agent. The receiver of these messages can use this information to authenticate the sending device.

	Command or Action	Purpose
Step 6	**cns image retry** *seconds* **Example:** `Router(config)# cns image retry 240`	(Optional) Specifies an image upgrade retry interval in seconds. • The default interval is 60 seconds.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode, and returns the router to privileged EXEC mode.

Configuring the Authentication of End-User Credentials in Incoming CNS Messages

Use the following commands to configure the authentication of end-user credentials in incoming CNS notification message.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cns message format notification** [**version 1** | **version 2**]
4. **cns aaa authentication** *authentication-method*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cns message format notification** [**version 1** | **version 2**] **Example:** `Router(config)# cns message format notification 1`	Configures the message format for notification messages from a CNS device. Received messages which do not conform to the configured message format are rejected. Use version 1 to configure the non-SOAP message format. Use version 2 for SOAP message format.
Step 4	**cns aaa authentication** *authentication-method* **Example:** `Router(config)# cns aaa authentication method1`	Enables CNS AAA options. **Note** The authentication methods must be configured within AAA.

Additional References

The following sections provide references related to CNS.

Related Documents

Related Topic	Document Title
CNS Configuration Agent	*CNS Configuration Agent*
CNS Event Agent	*CNS Event Agent*
CNS Image Agent	*CNS Image Agent*
CNS commands	*Cisco IOS Network Management Command Reference,* Release 12.4

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support and Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new commands only.

- **cns aaa authentication**
- **cns message format notification**

cns aaa authentication

To enable Cisco Networking Services (CNS) Authentication, Authorization, and Accounting (AAA) options, use the **cns aaa authentication** command in global configuration mode. To explicitly disable CNS AAA options, use the **no** form of this command.

cns aaa authentication *authentication-method*

no cns aaa authentication *authentication-method*

Syntax Description

authentication-method	Specifies the AAA authentication method to be used.

Command Default

AAA is enabled when using CNS by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

Use the **cns aaa authentication** command to enable AAA when using CNS. When the **cns aaa authentication** command is configured, CNS notification messages sent to the device are rejected if they do not have sender credentials. By default, no authentication is enabled. This command must be enabled to configure AAA authentication for CNS messages. Use the **no cns aaa authentication** command to explicitly disable AAA support when using CNS.

For more information about AAA authentication methods, see the "AAA Authentication Methods Configuration Task List" section in the "Configuring Authentication" chapter of the *Cisco IOS Security Configuration Guide,* Release 12.4.

Examples

The following example shows how to enable AAA authentication when using CNS:

```
cns aaa authentication method1
```

Related Commands

Command	Description
cns message format notification	Configures the message format for notification messages from a CNS device.

cns message format notification

To configure the message format for notification messages from a Cisco Networking Services (CNS) device, use the **cns message format notification** command in global configuration mode. To unconfigure a configured message format for notification messages from a CNS device, use the **no** form of this command.

cns message format notification {**version 1** | **version 2**}

no cns message format notification {**version 1** | **version 2**}

Syntax Description

version 1	Configures CNS notification messages to use the non- Service-Oriented Access Protocol (SOAP) format.
version 2	Configures CNS notification messages to use the SOAP format.

Command Default

Non-SOAP notification messages are used by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

Use this command to configure a CNS agent to use the SOAP format for CNS notification messages. SOAP message formats are supported by default. If the Cisco IOS device receives a request in the non-SOAP message format, the response will be sent in the non-SOAP format. If the Cisco IOS device receives a request in the SOAP format, the response will be sent in the SOAP format. By default, notification messages that are sent without any corresponding request messages will be sent in both SOAP and non-SOAP formats.

When this command is configured, received CNS notification messages that do not conform to the configured message format are rejected.

If the **cns aaa authentication notification** command is already configured, then the sender's credentials will be authenticated. If the **cns message format notification** command is configured, then the notification messages will be sent as per the configured version number. The default configuration is the legacy non-SOAP format.

Examples

The following example shows how to configure CNS notification messages to use the SOAP format:

```
cns message format notification version 2
```

Related Commands	Command	Description
	cns aaa authentication	Enables CNS AAA options.

Feature Information for CNS Security Enhancement

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for CNS Security Enhancement

Feature Name	Releases	Feature Information
CNS Security Enhancement	12.4(9)T, 12.2(33)SRA	The Cisco Networking Services (CNS) Security Enhancement feature improves the security of CNS messages by authenticating sender credentials through the use of the Service-Oriented Access Protocol (SOAP) message format. In 12.4(9)T, this feature was introduced.