Cisco Networking Services Security Enhancement

The Cisco Networking Services Security Enhancement feature improves the security of Cisco Networking Services messages by authenticating sender credentials through the use of the SOAP message format.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Information About Cisco Networking Services Security Enhancement

Cisco Networking Services Security Enhancement

Cisco Networking Services messages can be configured to use the Cisco Networking Services SOAP message structure, in which the username and password are authenticated.

If authentication, authorization, and accounting (AAA) is configured, then Cisco Networking Services SOAP messages will be authenticated with AAA. If AAA is not configured, there will be no authentication. For backward compatibility, Cisco Networking Services will support the existing non-SOAP message format and will respond accordingly without security.

The **cns aaa authentication** command is required to turn on Cisco Networking Services Security Enhancement. This command determines whether the Cisco Networking Services 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.

Cisco Networking Services Trusted Servers

Use the **cns trusted-server** command to specify a trusted server for an individual Cisco Networking Services agent or for all the Cisco Networking Services agents. To avoid security violations, you can build a list of trusted servers from which Cisco Networking Services agents can receive messages. An attempt to connect to a server not on the list will result in an error message being displayed.

Configure a Cisco Networking Services trusted server when a Cisco Networking Services agent will redirect its response to a server address that is not explicitly configured on the command line for the specific Cisco Networking Services agent. For example, the Cisco Networking Services EXEC agent may have one server configured but receive a message from the Cisco Networking Services event bus that overrides the configured server. The new server address has not been explicitly configured, so the new server address is not a trusted server. An error will be generated when the Cisco Networking Services exec agent tries to respond to this new server address unless the **cns trusted-server** command has been configured for the new server address.

How to Configure Cisco Networking Services Security Enhancement

Configuring Cisco Networking Services Trusted Servers

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cns trusted-server** {**all-agents** | **config** | **event** | **exec** | **image**} *name*
4. **cns message format notification** {**version 1** | **version 2**}
5. **cns aaa authentication** *authentication-method*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**cns trusted-server** {**all-agents** | **config** | **event** | **exec** | **image**} *name* **Example:** `Device(config)# cns trusted-server event 10.19.2.5`	Configures a Cisco Networking Services trusted server for the specified hostname or IP address.
Step 4	**cns message format notification** {**version 1** | **version 2**} **Example:** `Device(config)# cns message format notification version 1`	Configures the message format for notification messages from a Cisco Networking Services 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 5	**cns aaa authentication** *authentication-method* **Example:** `Device(config)# cns aaa authentication method1`	Enables Cisco Networking Services AAA options. **Note** The authentication methods must be configured within AAA.

Configuration Examples for Cisco Networking Services Security Enhancement

Example: Configuring Cisco Networking Services Trusted Servers

```
enable
 configure terminal
   cns trusted-server event 10.19.2.5
   cns message format notification version 2
   cns aaa authentication method1
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco Networking Services commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Cisco Networking Services Command Reference
Cisco Networking Services Configuration Engine	Cisco CNS Configuration Engine Administrator Guide, 1.3

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco Networking Services Security Enhancement

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1: Feature Information for Cisco Networking Services Security Enhancement

Feature Name	Releases	Feature Information
Cisco Networking Services Security Enhancement	12.4(9)T 12.2(33)SRA	The Cisco Networking Services Security Enhancement feature improves the security of Cisco Networking Services messages by authenticating sender credentials through the use of the SOAP message format. The following commands were introduced or modified: **cns aaa authentication**, **cns message format notification**.