Cisco IOS Web Services Management Agent Command Reference

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

CONTENTS

A through W Commands

acl (WSMA)

To enable access control lists (ACLs) for restricting addresses that can connect to a Web Services Management Agent (WSMA) profile, use the **acl** command in WSMA listener configuration mode. To disable the access control lists, use the **no** form of this command.

acl *acl-number*

no acl

Syntax Description

acl-number	Access control list number that can connect to the WSMA profile. Valid values are from 1 to 2799.

Command Default

ACLs are disabled.

Command Modes

WSMA listener configuration (config-wsma-listen)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

You can use the **acl** command to enable ACLs for restricting access to WSMA profiles. Use this command in WSMA listener configuration mode. To enter this mode, use the **wsma profile listener** command in global configuration mode.

Examples

The following example shows how to enable ACL 34 for a WSMA profile named prof1:

```
Router(config)# wsma profile listener prof1
Router(config-wsma-listen)# acl 34
```

Related Commands

Command	Description
encap	Configures an encapsulation for a WSMA profile.
idle-timeout	Sets a time for the WSMA profile to disconnect the session when there is no network traffic.
max-message	Sets the maximum size limit for incoming messages.
stealth	Disables WSMA from sending SOAP faults.
transport	Defines a transport configuration for a WSMA profile.
wsma profile listener	Enables a WSMA listener profile and enters WSMA listener configuration mode.
wsse	Enables the WSSE for a WSMA profile.

backup excluded

To set the time that the Web Services Management Agent (WSMA) profile must wait after a connection is lost before attempting to connect to the backup transport configuration, use the **backup excluded** command in WSMA initiator configuration mode. To disable the configured backup excluded time, use the **no** form of this command.

backup excluded *seconds*

no backup excluded

Syntax Description

seconds	The time, in seconds, that the WSMA profile waits before attempting to connect to the backup transport configuration. The range is from 1 to 2000000. The default is 0.

Command Default

The time is set to 0 seconds.

Command Modes

WSMA initiator configuration (config-wsma-init)

Command History

Release	Modification
15.1(1)T	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

If the primary transport connection is lost and a backup transport configuration has been set up, the WSMA profile will connect to the backup transport connection.

This setting is ignored if the WSMA profile has no primary transport configuration.

Examples

The following example shows how to set the backup excluded time to 60 seconds for a WSMA initiator profile named prof1:

```
Router(config)# wsma profile initiator prof1
Router(config-wsma-init)# backup excluded 60
```

Related Commands

Command	Description
backup hold	Sets the time that the WSMA profile remains connected to the backup transport configuration.
encap	Configures an encapsulation for a WSMA profile.
idle-timeout	Sets a time for the WSMA profile to keep the session alive in the absence of any data traffic.
keepalive	Enables keepalive messages and configures interval and retry values for a WSMA profile.
max-message	Sets the maximum size limit for incoming messages.
reconnect	Specifies the time for the WSMA initiator profile to wait before attempting to reconnect a session.
stealth	Disables WSMA from sending SOAP faults.
transport	Defines a transport configuration for a WSMA profile.
wsma profile initiator	Enables a WSMA initiator profile and enters WSMA initiator configuration mode.
wsse	Enables the WSSE for a WSMA profile.

backup hold

To set the time that the Web Services Management Agent (WSMA) profile remains connected to the backup transport configuration, use the **backup hold** command in WSMA initiator configuration mode. To disable the backup hold time, use the **no** form of this command.

backup hold *minutes*

no backup hold

Syntax Description

minutes	The time, in minutes, to remain connected to the backup transport connection. The range is from 1 to 35000. By default, the connection is set to never disconnect.

Command Default

The backup hold time is set to never disconnect.

Command Modes

WSMA initiator configuration (config-wsma-init)

Command History

Release	Modification
15.1(1)T	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

If both primary and backup transport connections are configured, the hold time indicates how long the WSMA profile remains connected to the backup transport before the connection to the backup is closed and a new connection to the primary transport is attempted.

If the primary transport connection is lost and a backup transport configuration has been set up, the WSMA profile will connect to the backup transport connection.

This command can be used when you need to disconnect from the primary transport for a specific time. For example, use this command if you want to perform maintenance on the primary transport and want to automatically switch back from the backup to the primary transport after a known period.

This setting is ignored if the WSMA profile has no primary transport configuration.

Examples

The following example shows how to set the backup hold time to 120 minutes for a WSMA initiator profile named prof1:

```
Router(config)# wsma profile initiator prof1
Router(config-wsma-init)# backup hold 120
```

Related Commands

Command	Description
backup excluded	Sets the time that the WSMA profile must wait after a connection is lost before attempting to connect to the backup transport configuration.
encap	Configures an encapsulation for a WSMA profile.
idle-timeout	Sets a time for the WSMA profile to keep the session alive in the absence of any data traffic.
keepalive	Enables keepalive messages and configures interval and retry values for a WSMA profile.
max-message	Sets the maximum size limit for incoming messages.
reconnect	Specifies the time for the WSMA initiator profile to wait before attempting to reconnect a session.
stealth	Disables WSMA from sending SOAP faults.
transport	Defines a transport configuration for a WSMA profile.
wsma profile initiator	Enables a WSMA initiator profile and enters WSMA initiator configuration mode.
wsse	Enables the WSSE for a WSMA profile.

clear wsma agent

To clear Web Services Management Agent (WSMA) counters, use the **clear wsma agent** command in privileged EXEC mode.

clear wsma agent [**config**| **exec**| **filesys**| **notify**] **counters**

Syntax Description

config	(Optional) Clears the counters for a configuration agent.
exec	(Optional) Clears the counters for an executive agent.
filesys	(Optional) Clears the counters for a file system agent.
notify	(Optional) Clears the counters for a notify agent.
counters	Clears counters for the specified agents. If the **config**, **exec**, **filesys** or **notify** keywords are not specified, counters for all the agents are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

The following example shows how to clear the counters for a WSMA filesys agent:

```
Router# clear wsma agent filesys counters
```

Related Commands

Command	Description
clear wsma profile	Clears WSMA profiles.

clear wsma profile

To clear a configured Web Services Management Agent (WSMA) profile, use the **clear wsma profile** command in privileged EXEC mode.

clear wsma profile [**name** *profile-name*] {**connections**| **counters**}

Syntax Description

name *profile-name*	(Optional) Specifies the name of the profile to be cleared. If a profile name is not specified, all WSMA profiles are cleared.
connections	Closes all data connections for the listener and initiator profiles.
counters	Clears all counters for the listener and initiator profiles.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.1(1)T	This command was modified. Support was added for WSMA initiator configuration mode.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

The following example shows how to clear the profile counters for the WSMA profile named prof1:

```
Router# clear wsma profile name prof1 counters
```

Related Commands

Command	Description
clear wsma agent	Clears WSMA counters.

encap

To configure an encapsulation for a Web Services Management Agent (WSMA) profile, use the **encap** command in WSMA initiator or listener configuration mode. To reset the encapsulation to its default value, use the **no** form of this command.

encap {**soap11**| **soap12**}

no encap

Syntax Description

soap11	Configures the Simple Object Access Protocol (SOAP) 1.1 encapsulation. Incoming messages that do not correspond to the SOAP 1.1 format are discarded. Outgoing messages are sent using the SOAP 1.1 format. SOAP 1.1 is the default encapsulation.
soap12	Configures the SOAP 1.2 encapsulation. Incoming messages that do not correspond to the SOAP 1.2 format are discarded. Outgoing messages are sent using the SOAP 1.2 format.

Command Default

SOAP 1.1 encapsulation is enabled for a WSMA profile.

Command Modes

WSMA initiator configuration (config-wsma-init)

WSMA listener configuration (config-wsma-listen)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.1(1)T	This command was modified. Support was added for WSMA initiator configuration mode.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use this command in WSMA listener configuration mode or WSMA initiator configuration mode. To enter WSMA listener configuration mode, use the **wsma profile listener** command in global configuration mode. To enter WSMA initiator configuration mode, use the **wsma profile initiator** command in global configuration mode.

Examples

The following example shows how to configure SOAP 1.2 encapsulation for a WSMA listener profile:

```
Router(config)# wsma profile listener prof1
Router(config-wsma-listen)# encap soap12
```

Related Commands

Command	Description
acl	Enables ACLs for restricting addresses that can connect to a WSMA profile.
idle-timeout	Sets a time for the WSMA profile to disconnect the session when there is no network traffic.
max-message	Sets the maximum size limit for incoming messages.
stealth	Disables WSMA from sending SOAP faults.
transport	Defines a transport configuration for a WSMA profile.
wsma profile listener	Enables a WSMA listener profile and enters WSMA listener configuration mode.
wsse	Enables the WSSE for a WSMA profile.

idle-timeout (WSMA)

To set a time for the Web Services Management Agent (WSMA) profile to keep the session alive in the absence of any data traffic, use the **idle-timeout** command in WSMA initiator or listener configuration mode. To disable the idle-timeout setting, use the **no** form of this command.

idle-timeout *minutes*

no idle-timeout

Syntax Description

minutes	The time, in minutes, until the WSMA profile disconnects the session if there is no network traffic. The range is from 1 to 35000. The default is infinite, which means the session is kept alive indefinitely in the absence of data traffic. If the connection is lost, WSMA reconnects.

Command Default

The idle-timeout value is set to infinite.

Command Modes

WSMA initiator configuration (config-wsma-init)

WSMA listener configuration (config-wsma-listen)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.1(1)T	This command was modified. Support was added for WSMA initiator configuration mode.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use this command in WSMA listener configuration mode or WSMA initiator configuration mode. To enter WSMA listener configuration mode, enter the **wsma profile listener** command in global configuration mode. To enter WSMA initiator configuration mode, use the **wsma profile initiator** command in global configuration mode.

Examples

The following example shows how to set the idle-timeout value to 345 minutes for a WSMA listener profile:

```
Router(config)# wsma profile listener prof1
Router(config-wsma-listen)# idle-timeout 345
```

Related Commands

Command	Description
acl	Enables ACLs for restricting addresses that can connect to a WSMA profile.
encap	Configures an encapsulation for WSMA profiles.
max-message	Sets the maximum size limit for incoming messages.
stealth	Disables WSMA from sending SOAP faults.
transport	Defines a transport configuration for a WSMA profile.
wsma profile listener	Enables a WSMA listener profile and enters WSMA listener configuration mode.
wsse	Enables the WSSE for a WSMA profile.

keepalive (WSMA)

To enable keepalive messages and configure interval and retry values for a Web Services Management Agent (WSMA) profile, use the **keepalive** command in WSMA initiator or listener configuration mode. To disable keepalive messages, use the **no** form of this command.

keepalive *seconds* [**retries** *number*]

no keepalive

Syntax Description

seconds	The time, in seconds, that the WSMA profile will allow before sending a keepalive message. After the configured time without traffic, a message is sent to determine whether the connection should be maintained. The range is from 10 to 2000000.
retries *number*	(Optional) Specifies the maximum number of times that the WSMA profile will continue to send keepalive messages without a response before closing the connection. The range of valid values is from 1 to 100. The default is infinite.

Command Default

Keepalive messages are not sent.

Command Modes

WSMA initiator configuration (config-wsma-init)

WSMA listener configuration (config-wsma-listen)

Command History

Release	Modification
15.1(1)T	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

WSMA initiator profiles using the HTTP or HTTPS protocol must be configured to send keepalive messages. This configuration ensures that the Cisco IOS device allows the remote WSMA application to send WSMA requests.

Keepalive messages are not sent from WSMA listener connections that use the HTTP or HTTPS protocol because of the directional nature of HTTP transactions. Only the HTTP client can send requests on an HTTP connection.

Note If the keepalive interval is configured, but the retries value is not configured, the retries value defaults to infinite, and the profile will send keepalive messages forever.

Examples

The following example shows how to enable keepalive messages and configure interval and retry values for a WSMA initiator profile:

```
Router(config)# wsma profile initiator prof1
Router(config-wsma-init)# keepalive 200 retries 20
```

Related Commands

Command	Description
acl	Enables ACLs for restricting addresses that can connect to a WSMA profile.
backup excluded	Sets the time that the WSMA profile must wait after a connection is lost before attempting to connect to the backup transport configuration.
backup hold	Sets the time that the WSMA profile remains connected to the backup transport configuration.
encap	Configures an encapsulation for a WSMA profile.
idle-timeout	Sets a time for the WSMA profile to keep the session alive in the absence of any data traffic.
max-message	Sets the maximum size limit for incoming messages.
reconnect	Specifies the time for the WSMA initiator profile to wait before attempting to reconnect a session.
stealth	Disables WSMA from sending SOAP faults.
transport	Defines a transport configuration for a WSMA profile.
wsma profile initiator	Enables a WSMA initiator profile and enters WSMA initiator configuration mode.
wsma profile listener	Enables a WSMA listener profile and enters WSMA listener configuration mode.
wsse	Enables the WSSE for a WSMA profile.

max-message

To set the maximum size limit for incoming messages, use the **max-message** command in WSMA initiator or listener configuration mode. To disable the maximum message size limit, use the **no** form of this command.

max-message *message-size*

no max-message

Syntax Description

message-size	Maximum size, in kilobytes (KB), for the incoming message. The range is from 1 to 2000. The default is 50.

Command Default

The maximum message size is set to 50 KB.

Command Modes

WSMA initiator configuration (config-wsma-init)

WSMA listener configuration (config-wsma-listen)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.1(1)T	This command was modified. Support was added for WSMA initiator configuration mode.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use this command in WSMA listener configuration mode or in WSMA initiator configuration mode. To enter WSMA listener configuration mode, use the **wsma profile listener** command in global configuration mode. To enter WSMA initiator configuration mode, use the **wsma profile initiator** command in global configuration mode.

Any incoming message that exceeds the maximum message size, it is considered to be oversized and is dropped. An error message is sent to indicate that the message is dropped.

Examples

The following example shows how to set the maximum message size for an incoming message to 290 KB:

```
Router(config)# wsma profile listener prof1
Router(config-wsma-listen)# max-message 290
```

Related Commands

Command	Description
acl	Enables ACLs for restricting addresses that can connect to a WSMA profile.
encap	Configures an encapsulation for a WSMA profile.
idle-timeout	Sets a time for the WSMA profile to disconnect the session when there is no network traffic.
stealth	Disables WSMA from sending SOAP faults.
transport	Defines a transport configuration for a WSMA profile.
wsma profile listener	Enables a WSMA listener profile and enters WSMA listener configuration mode.
wsse	Enables the WSSE for a WSMA profile.

reconnect

To specify the time for the Web Services Management Agent (WSMA) initiator profile to wait before attempting to reconnect a session, use the **reconnect** command in WSMA initiator configuration mode. To disable the configured reconnect time and revert to the default value, use the **no** form of this command.

reconnect [*pause-time* | [*exponential-backoff-factor* | [**random**]]]

no reconnect

Syntax Description

pause-time	(Optional) Time to wait, in seconds, before attempting to reconnect after a connection is lost. The range is from 1 to 2000000. The default is 60.
exponential-backoff-factor	(Optional) Exponential backoff factor that triggers the reconnect attempt exponentially. The range is from 2 to 9.
random	(Optional) Specifies the random backoff fraction that triggers the reconnect attempt based on a random factor.

Command Default

The reconnect wait value is set to 60 seconds.

Command Modes

WSMA initiator configuration (config-wsma-init)

Command History

Release	Modification
15.1(1)T	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.4(1)T	This command was modified. The *exponential-backoff-factor* argument and the **random** keyword were added.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use the *exponential-backoff-factor* to trigger a reconnect attempt exponentially.

For example, if you configure **reconnect** *120 3* the following behavior occurs:

- The first reconnect attempt is after 120 seconds.

- The second reconnect attempt is after 360 (120 x 3) seconds.
- The third reconnect attempt is after 1080 (120 x 3 x 3) seconds, and so on.

Use the **random** keyword to trigger a reconnect attempt based on a randomly generated factor.

For example, if you configure **reconnect** *120 2* **random** the following behavior occurs:

- The first reconnect attempt is after 120 seconds.
- The second reconnect attempt is after 240 seconds (120 x 2.aaa, where aaa is the first positive random factor that is generated).
- The third reconnect attempt is after 480 seconds (120x2.aaa x 2.bbb, where bbb is the first positive random factor that is generated), and so on.

Examples

The following example shows how to configure a reconnect wait time of 120 seconds and an exponential factor of 3.

```
Device(config)# wsma profile initiator smartgrid
Device(config-wsma-init)# reconnect 120 3
```

Related Commands

Command	Description
backup excluded	Sets the time that the WSMA profile must wait after a connection is lost before attempting to connect to the backup transport configuration.
backup hold	Sets the time that the WSMA profile remains connected to the backup transport configuration.
encap	Configures an encapsulation for a WSMA profile.
idle-timeout	Sets a time for the WSMA profile to keep the session alive in the absence of any data traffic.
keepalive	Enables keepalive messages and configures interval and retry values for a WSMA profile.
max-message	Sets the maximum size limit for incoming messages.
stealth	Disables WSMA from sending SOAP faults.
transport	Defines a transport configuration for a WSMA profile.
wsma profile initiator	Enables a WSMA initiator profile and enters WSMA initiator configuration mode.
wsse	Enables the WSSE for a WSMA profile.

show wsma agent

To display the Web Services Management Agent (WSMAs) configured, use the **show wsma agent** command in user EXEC mode.

show wsma agent [**config**| **exec**| **filesys**| **notify**] {**counters**| **profiles**| **schema**}

Syntax Description

config	(Optional) Displays the WSMA configuration agent.
exec	(Optional) Displays the WSMA executive agent.
filesys	(Optional) Displays the WSMA file system agent.
notify	(Optional) Displays the WSMA notify agent.
counters	Displays the WSMA counters.
profiles	Displays the WSMA profiles.
schema	Displays the WSMA schema.

Command Modes

User EXEC (>)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.1(1)T	This command was modified. Information was added to the counters output.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.2(2)T	This command was modified. The **profiles** keyword was added.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.1(1)SY	This command was modified. The **profiles** keyword was added.

Usage Guidelines

You can use the **show wsma agent** command to display the WSMAs.

Examples

The following example shows how to display the WSMA configuration agent counters:

```
Router> show wsma agent config counters

messages received 53, replies sent 53, faults 0
```

The following example shows how to display all WSMA counters information:

```
Router> show wsma agent counters

WSMA Exec Agent Statistics:
messages received 0, replies sent 0, faults 0
WSMA Config Agent Statistics:
messages received 4, replies sent 4, faults 0
WSMA Filesys Agent Statistics:
messages received 1, replies sent 1, faults 0
WSMA Notification Agent Statistics:
config silent
messages received 0, replies sent 0, notifications sent 0, faults 0
```

The table below describes the significant fields shown in the display when the **counters** keyword is used.

Table 1: show wsma agent Field Descriptions

Field	Description
messages received	Total number of messages that were passed from the profile into the WSMA. The number of messages sent and the number of fault messages together form the total number of messages received.
replies sent	Total number of reply messages sent to the profile.
faults	Total number of faults that prevented a message from producing a reply. Faults are not a count of bad requests sent to the WSMA. The faults value counts the cases where the WSMA agent could not send a response for reasons out of its control. (For example, the WSMA agent could not send a response because no memory is available.)

Related Commands

Command	Description
show wsma id	Displays the WSMA ID configured on Cisco networking devices.
show wsma profile	Displays information about WSMA profiles.

show wsma id

To display the Web Services Management Agent (WSMA) ID configured on Cisco networking devices, use the **show wsma id** command in user EXEC mode.

show wsma id

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

The following example shows how to display the WSMA ID:

```
Device1> show wsma id
Device1
Device1>
```

Related Commands

Command	Description
show wsma agent	Displays all WSMAs configured.
show wsma profile	Displays information about WSMA profiles.
wsma id	Assign unique WSMA IDs to Cisco networking devices.

show wsma profile

To display information about Web Services Management Agent (WSMA) profiles, use the **show wsma profile** command in user EXEC mode.

show wsma profile [**name** *profile-name*] {**connections**| **counters**| **schema**}

Syntax Description

name *profile-name*	(Optional) Displays profile information about the profile name specified.
connections	Displays information about the connections for all listener and initiator profiles configured.
counters	Displays various statistics about the listener and initiator profiles.
schema	Displays information about the WSMA profile schema configured.

Command Modes

User EXEC (>)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.1(1)T	This command was modified. Additional information was added to the output for counter statistics. The output for connection information was reformatted.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

If you do not specify a profile name, information for all profiles is displayed.

Specifying the **connection** keyword provides details about the connections to all the listener and initiator profiles.

Specifying the **counters** keyword provides various statistics about the listeners and initiators.

Examples

The following example shows how to display information about WSMA profile connections:

```
Router> show wsma profile connections

Listener Profile http: 0 open connections: 0 closing connections
Encap: soap11
WSSE header is required
Max message (RX) is 50 Kbytes
SOAP Faults are sent
Idle timeout infinite
Keepalive not configured
Listening via http
Listening to path /wsma.  Max Idle 0 ms.  Accepting post on plain text connections.
Established at 01:11:04.207 UTC Tue Jan 12 2010
Tx 493475 bytes (90 msg), Tx 0 errors,
Last message sent at 05:18:08.539 UTC Sat Feb 20 2010
Rx 59457 bytes (90 msg), 0 empty msg
Last message received at 05:18:08.295 UTC Sat Feb 20 2010
Listener Profile ssh: 2 open connections: 0 closing connections
Encap: soap11
WSSE header is required
Max message (RX) is 50 Kbytes
SOAP Faults are sent
Idle timeout infinite
Keepalive not configured
Listening via ssh
SSH listener, 10 sessions accepted, 0 sessions rejected
Connected sessions...
Remote connection via SSH by user(cisco) from 172.16.29.134:44457, state connect
Established at 01:14:03.184 UTC Thu Mar 11 2010
Tx 1183 bytes (2 msg), Tx 0 errors,
Last message sent at 01:14:48.565 UTC Thu Mar 11 2010
Rx 10 bytes (1 msg), 0 empty msg
Last message received at 01:14:48.565 UTC Thu Mar 11 2010
Remote connection via SSH by user(cisco) from 172.16.154.90:45404, state connect
Established at 01:14:28.041 UTC Thu Mar 11 2010
Tx 1183 bytes (2 msg), Tx 0 errors,
Last message sent at 01:14:54.437 UTC Thu Mar 11 2010
Rx 7 bytes (1 msg), 1 empty msg
Last message received at 01:14:54.437 UTC Thu Mar 11 2010
Initiator Profile ssh-init: 0 open connections: 0 closing connections
Encap: soap11
WSSE header is required
Max message (RX) is 50 Kbytes
SOAP Faults are sent
Idle timeout infinite
Keepalive not configured
Reconnect time 60 seconds
No transport configured
```

The table below describes the significant fields shown in the display.

Table 2: show wsma profile Field Descriptions

Field	Description
open connections	The number of connections into the profile.
closing connections	The number of connections that have initiated a close but for which the close is not complete yet.
sessions accepted	The total number of sessions accepted (including closed ones) since the profile was configured or the counters were last cleared.

Field	Description
sessions rejected	The total number of sessions rejected since the profile was configured or the counters were last cleared. Rejections may be due to the access control lists (ACLs) or internal errors such as malloc failures).

The following example shows how to display information about WSMA profile counters:

```
Router> show wsma profile counters

Statistics for profile http
incoming total 90, bad XML 0, authentication errors 0, oversized 0
outgoing total 90, absorbed 0
message internal errors 0
Connection Accepts 90, local hangup 0, remote hangup 90, keepalive hangup 0
session internal errors 0
Statistics for profile ssh
incoming total 9, bad XML 2, authentication errors 0, oversized 0
outgoing total 20, absorbed 0
message internal errors 0
Connection Accepts 8, local hangup 0, remote hangup 8, keepalive hangup 0
session internal errors 0
```

The table below describes the significant fields shown in the display.

Table 3: show wsma profile counters Field Descriptions

Field	Description
incoming total	Total number of messages received.
bad XML	Total number of incoming messages that could not be parsed by the XML parser.
oversized	Total number of messages exceeding the maximum message size configured.
outgoing total	Total number of messages sent.
absorbed	Total number of messages that were absorbed by specifying the **stealth** command.
message internal errors	Total number of internal errors that prevented the message from getting processed completely.
authentication errors	Total number of messages with Simple Object Access Protocol (SOAP) Web Services Security (WSSE) headers that contained incorrect credentials resulting in authentication errors.
Connection Accepts	Total number of connections that have been accepted.
local hangup	Total number of connections that have had the hangup initiated from the Cisco networking device.

Field	Description
remote hangup	Total number of connections that have had the hangup initiated from the remote end.
keepalive hangup	Total number of connections that have had the hangup initiated after the configured number of keepalive retries is reached.
session internal errors	Total number of internal errors preventing a connection from continuing.

The following example shows how to display information about the WSMA profile schema:

```
Router> show wsma profile schema

Schema myschema
New Name Space ''
<VirtualRootTag> [0, 1] required
  New Name Space 'http://schemas.xmlsoap.org/soap/envelope/'
  <Envelope> 1+ required
    <Header> any subtree is allowed
    <Body> 1 required
      <Fault> [0, 1] required
        <faultcode> 1 required
        <faultstring> 1 required
        <faultactor> [0, 1] required
        <detail> any subtree is allowed
      New Name Space 'urn:cisco:exec'
        <request> [0, 1] required
          <execCLI> 1+ required
            <cmd> 1 required
            <dialogue> 0+ required
              <expect> 1 required
              <reply> 1 required
      New Name Space 'urn:cisco:wsma-config'
        <request> [0, 1] required
<config-data> 1 required
            <cli-config-data> [0, 1] required
              <cmd> 1+ required
            <cli-config-data-block> [0, 1] required
            <xml-config-data> [0, 1] required
              <Device-Configuration> [0, 1] required
                <> any subtree is allowed
      New Name Space 'urn:cisco:wsma-filesystem'
        <request> [0, 1] required
          <fileList> [0, 1] required
          <fileDelete> [0, 1] required
            <deleteFileList> 1 required
              <filename> 1+ required
          <fileCopy> [0, 1] required
            <srcURL> 1 required
            <dstURL> 1 required
            <validationInfo> [0, 1] required
              <md5CheckSum> 1 required
            <deleteFileList> [0, 1] required
              <filename> 1+ required
      New Name Space 'urn:cisco:wsma-notify'
 <request> [0, 1] required
Schema dog1
New Name Space ''
<VirtualRootTag> [0, 1] required
  New Name Space 'http://schemas.xmlsoap.org/soap/envelope/'
  <Envelope> 1+ required
    <Header> any subtree is allowed
```

```
<Body> 1 required
  <Fault> [0, 1] required
    <faultcode> 1 required
    <faultstring> 1 required
    <faultactor> [0, 1] required
    <detail> any subtree is allowed
```

Related Commands

Command	Description
show wsma agent	Displays all the WSMAs configured.
show wsma id	Displays the WSMA ID configured on Cisco IOS networking devices.

stealth

To disable the Web Services Management Agent (WSMA) profile from sending Simple Object Access Protocol (SOAP) faults, use the **stealth** command in WSMA initiator or listener configuration mode. To enable WSMA to send the SOAP faults, use the **no** form of this command.

stealth

no stealth

Syntax Description

This command has no arguments or keywords.

Command Default

Stealth is disabled; that is, SOAP faults are sent.

Command Modes

WSMA initiator configuration (config-wsma-init)

WSMA listener configuration (config-wsma-listen)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.1(1)T	This command was modified. Support was added for WSMA initiator configuration mode.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use this command in WSMA listener configuration mode. To enter this mode, use the **wsma profile listener** command in global configuration mode.

Examples

The following example shows how to enable the **stealth** command to stop sending SOAP faults:

```
Router(config)# wsma profile listener prof1
Router(config-wsma-listen)# stealth
```

Related Commands

Command	Description
acl	Enables ACLs for restricting addresses that can connect to a WSMA profile.
idle-timeout	Sets a time for the WSMA profile to disconnect the session when there is no network traffic.
max-message	Sets the maximum size limit for incoming messages.
transport	Defines a transport configuration for a WSMA profile.
wsma profile listener	Enables a WSMA listener profile and enters WSMA listener configuration mode.
wsse	Enables the WSSE for a WSMA profile.

transport (WSMA)

To define a transport configuration for a Web Services Management Agent (WSMA) profile, use the **transport** command in WSMA listener configuration mode. To disable the transport configuration, use the **no** form of this command.

transport {**ssh subsys** *subsys-name*{**http| https**}**path** *pathname*}

no transport

Syntax Description

ssh	Enables the WSMA profile to listen on the Secure Shell Version 2 (SSHv2) port.
subsys	Specifies the SSH subsystem to use.
subsys-name	Name of the SSH subsystem. By default, **wsma** is used as the subsystem name.
http	Enables the WSMA profile to listen on the HTTP port.
path	Specifies the HTTP path to use.
pathname	Pathname for the HTTP or Secure HTTP (HTTPS) path. The pathname must begin with a forward slash (/). By default, **/wsma** is used as the pathname.
https	Enables the WSMA profile to listen on the HTTPS port.

Command Default

The transport is not configured.

Command Modes

WSMA listener configuration (config-wsma-listen)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Release	Modification
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

You can use the **transport** command to define the transport termination points for a WSMA profile. Defining the transport configuration opens a listening socket for listeners on the device or connecting sockets for clients on the router. Opening the listening sockets enables the WSMA to start listening to messages.

You can define SSHv2, HTTP, or HTTPS as the transport configuration for a WSMA profile.

Use this command in WSMA listener configuration mode. To enter this mode, use the **wsma profile listener** command in global configuration mode.

Examples

The following example shows how to use the SSHv2 protocol to enable the listener profile:

```
Router(config)# wsma profile listener prof1
Router(config-wsma-listen)# transport ssh subsys wsma
```

Related Commands

Command	Description
acl	Enables ACLs for restricting addresses that can connect to a WSMA profile.
encap	Configures an encapsulation for a WSMA profile.
idle-timeout	Sets a time for the WSMA profile to disconnect the session when there is no network traffic.
max-message	Sets the maximum size limit for incoming messages.
stealth	Disables WSMA from sending SOAP faults.
wsma profile listener	Enables a WSMA listener profile and enters WSMA listener configuration mode.
wsse	Enables the WSSE for a WSMA profile.

transport (WSMA initiator)

To define a transport configuration for a Web Services Management Agent (WSMA) initiator profile, use the **transport** command in WSMA initiator configuration mode. To disable the transport configuration, use the **no** form of this command.

[backup] transport {**http**| **https**| **ssh** *remote-host* [*initiator-port-number*] **path** *pathname* [**user** *username*[**0**| **6**]*password*]| **tls** *remote-host* [*initiator-port-number*] [**localcert** *trustpoint-name*] [**remotecert** *trustpoint-name*] [**source** *source-interface*]}

no [backup] transport

Syntax Description

backup	(Optional) Configures a backup transport connection. The backup connection is used only if the primary connection becomes unresponsive or is not configured.
http	Specifies HTTP (plain text) as the transport method for the WSMA profile and enables the profile to initiate connections from the device to the HTTP port on the remote HTTP server.
https	Specifies Secure HTTP (HTTPS) (encrypted) as the transport method for the WSMA profile and enables the profile to initiate connections from the device to the HTTPS port on the remote HTTP server.
ssh	Specifies Secure Shell (SSH) as the transport method for the WSMA profile and enables the profile to initiate connections from the device to the SSH port on the remote SSH server.
remote-host	The name or IP address of the WSMA application host.
initiator-port-number	(Optional) The port number that the remote WSMA application host is listening on. By default, the client attempts to connect to the port for the transport protocol being used (port 13000 for Transport Layer Security [TLS]). This value should be set to the same value as the WSMA application listener port.
path	When the transport method selected is HTTP or HTTPS, this keyword specifies the path to the HTTP server. When the transport method selected is SSH, this keyword specifies the path to the remote command to be invoked.

pathname	When the transport method selected is HTTP or HTTPS, this value is the pathname for the HTTP or HTTPS path. When the transport method selected is SSH Version 2 (SSHv2), this value is the path to the remote command to be invoked.
user	(Optional) Specifies the username for the remote application.
username	(Optional) The username to connect to the remote application.
0	(Optional) Specifies that the password is unencrypted.
6	(Optional) Specifies that the password is encrypted.
password	(Optional) The password for the specified user.
tls	(Optional) Specifies the TLS protocol as the transport method for the WSMA profile, and enables the profile to initiate connections from the device to the TLS port on the remote TLS server.
localcert	(Optional) Specifies the trustpoint used for client-side authentication during the TLS handshake. The Cisco IOS device presents the certificate supplied by this trustpoint to the WSMA host on the remote side. By default, the primary crypto trustpoint in the global configuration is used. **Note** This configuration is needed only if the WSMA application is configured for TLS client authentication.
trustpoint-name	(Optional) The name of the client or server trustpoint.
remotecert	(Optional) Specifies the trustpoint used for server certificate validation. This trustpoint specifies the certificate authority (CA) server that validates the certificates presented by the remote WSMA application host. By default, all trustpoints in the global configuration are used to validate the remote WSMA application host certificate.
source	(Optional) Specifies the source interface for the outgoing connection.
source-interface	(Optional) The source interface to use for the outgoing connection.

Command Default The transport is not configured.

Command Modes WSMA initiator configuration (config-wsma-init)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines You can use the **transport** command to define the transport termination points for a WSMA profile.

Defining the transport configuration in WSMA initiator mode enables the Cisco IOS device to initiate connections to the remote management application over trusted and untrusted networks.

To enter WSMA initiator configuration mode, use the **wsma profile listener** command in global configuration mode.

Examples The following example shows how to define a transport configuration for an initiator profile using the TLS protocol:

```
Router(config)# wsma profile initiator prof2
Router(config-wsma-init)# transport tls 10.23.23.2
```

Related Commands

Command	Description
acl	Enables ACLs for restricting addresses that can connect to a WSMA profile.
backup excluded	Sets the time that the WSMA profile must wait after a connection is lost before attempting to connect to the backup transport configuration.
backup hold	Sets the time that the WSMA profile remains connected to the backup transport configuration.
encap	Configures an encapsulation for a WSMA profile.

Command	Description
idle-timeout	Sets a time for the WSMA profile to keep the session alive in the absence of any data traffic.
keepalive	Enables keepalive messages and configures interval and retry values for a WSMA profile.
max-message	Sets the maximum size limit for incoming messages.
reconnect	Specifies the time to wait before attempting to reconnect after a connection is lost.
stealth	Disables WSMA from sending SOAP faults.
wsma profile initiator	Enables a WSMA initiator profile and enters WSMA initiator configuration mode.
wsma profile listener	Enables a WSMA listener profile and enters WSMA listener configuration mode.
wsse	Enables the WSSE for a WSMA profile.

transport (WSMA listener)

To define a transport configuration for a Web Services Management Agent (WSMA) listener profile, use the **transport** command in WSMA listener configuration mode. To disable the transport configuration, use the **no** form of this command.

transport {**http**| **https** [**path** *pathname*]| **ssh** [**subsys** *subsys-name*]| **tls** [*listener-port-number*] [**localcert** *trustpoint-name*] [**disable-remotecert-validation**| **remotecert** *trustpoint-name*]}

no transport

Syntax Description

http	Specifies HTTP (plain text) as the transport method for the WSMA profile and enables the profile to listen on the HTTP port (port 80 or the port configured by the **ip http port** command).
https	Specifies Secure HTTP (HTTPS) (encrypted) as the transport method for the WSMA profile and enables the profile to listen on the HTTPS port (port 443 or the port configured by the **ip http secure-port** command).
path	(Optional) Specifies the HTTP or HTTPS path to use.
pathname	(Optional) The pathname for the HTTP or HTTPS path. The pathname must begin with a forward slash (/). By default, **/wsma** is used as the pathname.
ssh	Specifies Secure Shell (SSH) Version 2 as the transport method for the WSMA profile and enables the profile to listen on the SSHv2 port (port 22 or the port configured by the **ip ssh port** command).
subsys	Specifies the SSH subsystem to use.
subsys-name	(Optional) The name for the SSH subsystem. By default, **wsma** is used as the subsystem name.
tls	Specifies the Transport Layer Service (TLS) protocol as the transport method for the WSMA profile, and enables the profile to listen on the TLS port. By default the TLS port is set to 13000. This value can be changed using the **transport** command.
listener-port-number	(Optional) The port number for the TLS listener. By default, the TLS listener uses port 13000. The port number can be set to any unused port from 1025 to 65535.

localcert	(Optional) In WSMA listener mode, this keyword specifies the trustpoint used for server-side authentication during the TLS handshake process. The Cisco IOS device presents the certificate supplied by this trustpoint to the remote side. By default, the primary crypto trustpoint in the global configuration is used.
trustpoint-name	(Optional) The name of the localcert or remotecert trustpoint.
disable-remotecert-validation	(Optional) Disables the validation of the remote application host's certificate. This keyword is used when the Cisco IOS device that acts as the TLS server needs to disable the validation of the remote applications host's certificate. By default, TLS remote host certificate validation is enabled.
remotecert	(Optional) Specifies the trustpoint used for client certificate validation. This trustpoint specifies the certificate authority (CA) server that validates the certificates presented by the remote WSMA application host. By default, all trustpoints in the global configuration are used to validate the remote WSMA application host certificate.

Command Default The transport is not configured.

Command Modes WSMA listener configuration (config-wsma-listen)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.1(1)T	This command was modified. Support was added for the **tls** keyword.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

You can use the **transport** command to define the transport termination points for a WSMA profile.

Defining the transport configuration in WSMA listener configuration mode opens a listening socket for listeners on the router. Opening the listening sockets enables the WSMA to start listening to messages.

You can use Secure Shell Version 2 (SSHv2), HTTP, HTTPS, or Transport Layer Service (TLS) as the transport protocol for a WSMA profile.

To enter WSMA listener configuration mode, use the **wsma profile listener** command in global configuration mode.

Examples

The following example shows how to define a transport configuration for a WSMA listener profile using the SSHv2 protocol:

```
Router(config)# wsma profile listener prof1
Router(config-wsma-listen)# transport ssh subsys wsma
```

The following example shows how to define a transport configuration for a WSMA listener profile using the TLS protocol:

```
Router(config)# wsma profile listener prof2
Router(config-wsma-listen)# transport tls 65534
```

Related Commands

Command	Description
acl	Enables ACLs for restricting addresses that can connect to a WSMA profile.
backup excluded	Sets the time that the WSMA profile must wait after a connection is lost before attempting to connect to the backup transport configuration.
backup hold	Sets the time that the WSMA profile remains connected to the backup transport configuration.
encap	Configures an encapsulation for a WSMA profile.
idle-timeout	Sets a time for the WSMA profile to keep the session alive in the absence of any data traffic.
keepalive	Enables keepalive messages and configures interval and retry values for a WSMA profile.
max-message	Sets the maximum size limit for incoming messages.
reconnect	Specifies the time to wait before attempting to reconnect after a connection is lost.
stealth	Disables WSMA from sending SOAP faults.

Command	Description
wsma profile initiator	Enables a WSMA initiator profile and enters WSMA initiator configuration mode.
wsma profile listener	Enables a WSMA listener profile and enters WSMA listener configuration mode.
wsse	Enables the WSSE for a WSMA profile.

wsma agent

To start a specific Web Services Management Agent (WSMA) and associate it with a profile, use the **wsma agent** command in global configuration mode. To disable the WSMA agent and its associations with a profile, use the **no** form of this command.

wsma agent {**config**| **exec**| **filesys**| **notify**} **profile** *profile-name*

no wsma agent {**config**| **exec**| **filesys**| **notify**}

Syntax Description

config	Starts the WSMA configuration agent.
exec	Starts the WSMA exec agent.
filesys	Starts the WSMA file system agent.
notify	Starts the WSMA notify agent.
profile *profile-name*	Specifies the profile name to use.

Command Default

WSMA agents are disabled and are not associated with profiles.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.2(2)T	This command was modified. Support for associating more than one profile with the same WSMA agent was added.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

The following example shows how to start a WSMA agent and associate it with a profile:

```
Router(config)# wsma agent config profile wsma1
```

Related Commands

Command	Description
wsma id	Assigns unique WSMA IDs to Cisco IOS devices.
wsma profile listener	Enables a WSMA listener profile and enters WSMA listener configuration mode.

wsma dhcp

To enable a Web Services Management Agent (WSMA) with permission to process and enable the incoming DHCP Option 43 message, use the **wsma dhcp** command in global configuration mode. To disable this permission, use the **no** form of this command.

wsma dhcp

no wsma dhcp

Syntax Description

This command has no arguments or keywords.

Command Default

The permission to process the incoming DHCP Option 43 message is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release XE3.8S	This command was integrated into Cisco IOS XE Release 3.8S.
Cisco IOS XE Release 3.3SE	This command was integrated into Cisco IOS XE Release 3.3SE

Usage Guidelines

Use the **wsma dhcp** command to enable the DHCP Option 43 message that the WSMA processes.

Examples

The following example shows how configure a WSMA agent to process the incoming DHCP Option 43 message:

```
Router(config)# wsma dhcp
```

Related Commands

Command	Description
cns dhcp	Enables a Cisco Networking Service with permission to process the incoming DHCP Option 43 message.

wsma id

To assign unique Web Services Management Agent (WSMA) IDs to Cisco devices, use the **wsma id** command in global configuration mode. To disable the WSMA IDs assigned to Cisco IOS devices, use the **no** form of this command.

wsma id {**hardware-serial**| **hostname**| {**ip-address**| **mac-address**} *interface*/*type*| **string** *value*}

no wsma id

Syntax Description

hardware-serial	Assigns the hardware serial number as a unique ID.
hostname	Assigns the hostname as a unique ID.
ip-address	Assigns the IP address of the specified interface as a unique ID.
interface/*type*	Specifies the interface type.
mac-address	Assigns the IP address of the specified interface as a unique ID.
string *value*	Assigns a string value as a unique ID.

Command Default

Unique WSMA IDs are not assigned to Cisco networking devices.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use this command to assign unique IDs to Cisco IOS devices. Unique IDs can also be configured by specifying required parameters.

Whenever the WSMA ID changes, all WSMA sessions are terminated. WSMA sessions are terminated in order to protect the management applications from not having to manage synchronizing states dynamically.

Examples

The following example shows how to assign WSMA IDs:

```
Router(config)# wsma id ip-address fastethernet 0/1
```

Related Commands

Command	Description
show wsma id	Displays the WSMA ID configured on Cisco networking devices.
wsma agent	Enables a specific WSMA and associates it with a profile.
wsma profile listener	Enables a WSMA listener profile and enters WSMA listener configuration mode.

wsma profile initiator

To enable a Web Services Management Agent (WSMA) initiator profile and to enter WSMA initiator configuration mode, use the **wsma profile initiator** command in global configuration mode. To disable a WSMA initiator profile, use the **no** form of this command.

wsma profile initiator *profile-name*

no wsma profile initiator *profile-name*

Syntax Description

profile-name	Name of the initiator profile to be enabled.

Command Default

No WSMA profiles are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

You can use the **wsma profile initiator** command to enable a WSMA profile. A WSMA profile associated with a specific WSMA constitutes an operational embedded agent.

WSMA profiles work as a transport termination point and allow transport and XML encapsulation parameters to be configured:

- The configurable encapsulations for WSMA are Simple Object Access Protocol (SOAP) 1.1 and SOAP 1.2.
- The transportation mechanisms for WSMA are Secure Shell (SSH), HTTP, Secure HTTP (HTTPS), and Transport Layer Security (TLS).

The WSMA initiator mode allows Cisco IOS devices to initiate connections to management applications over trusted and untrusted networks. You can configure various parameters for a WSMA profile in WSMA initiator configuration mode.

Examples

The following example shows how to enable a WSMA initiator profile:

```
Router(config)# wsma profile initiator prof1
Router(config-wsma-init)#
```

Related Commands

Command	Description
backup excluded	Sets the time that the WSMA profile must wait after a connection is lost before attempting to connect to the backup transport configuration.
backup hold	Sets the time that the WSMA profile remains connected to the backup transport configuration.
encap	Configures an encapsulation for a WSMA profile.
idle-timeout	Sets a time for the WSMA profile to keep the session alive in the absence of any data traffic.
keepalive	Enables keepalive messages and configures interval and retry values for a WSMA profile.
max-message	Sets the maximum size limit for incoming messages.
reconnect	Specifies the time for the WSMA initiator profile to wait before attempting to reconnect a session.
stealth	Disables WSMA profiles from sending SOAP faults.
transport	Defines a transport configuration for a WSMA profile.
wsma agent	Enables a specific WSMA and associates it with a profile.
wsma dhcp	Enables a WSMA with permission to process and enable an incoming Dynamic Host Control Protocol (DHCP) Option 43 message.
wsma id	Assigns unique WSMA IDs to Cisco IOS networking devices.
wsma profile listener	Configures and enables a WSMA listener profile and enters WSMA listener configuration mode.
wsse	Enables the WSSE for a WSMA profile.

wsma profile listener

To enable a Web Services Management Agent (WSMA) listener profile and to enter WSMA listener configuration mode, use the **wsma profile listener** command in global configuration mode. To disable a WSMA listener profile, use the **no** form of this command.

wsma profile listener *profile-name*

no wsma profile listener *profile-name*

Syntax Description

profile-name	Name of the listener profile to be enabled.

Command Default

No WSMA profiles are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

You can use the **wsma profile listener** command to enable a WSMA profile. A WSMA profile associated with a specific WSMA constitutes an operational embedded agent.

WSMA profiles work as transport termination points and allow transport and XML encapsulation parameters to be configured:

- The configurable encapsulations for WSMA are Simple Object Access Protocol (SOAP) 1.1 and SOAP 1.2.
- The transportation mechanisms for WSMA are Secure Shell Version (SSH), HTTP, Secure HTTP (HTTPS), and Transport Layer Security (TLS). The transport mechanisms open listening sockets for listeners on the router.

The **wsma profile listener** command creates a passive listening socket on the Cisco IOS device. The profile receives incoming messages provided they match the configured ACL requirements. You can configure various parameters for a WSMA profile in WSMA listener configuration mode.

Examples

The following example shows how to enable a WSMA listener profile:

```
Router(config)# wsma profile listener prof1
Router(config-wsma-listen)#
```

Related Commands

Command	Description
acl	Enables ACLs for restricting addresses that can connect to a WSMA profile.
encap	Configures an encapsulation for a WSMA profile.
idle-timeout	Sets a time for the WSMA profile to keep the session alive in the absence of any data traffic.
keepalive	Enables keepalive messages and configures interval and retry values for a WSMA profile.
max-message	Sets the maximum size limit for incoming messages.
stealth	Disables WSMA from sending SOAP faults.
transport	Defines a transport configuration for a WSMA profile.
wsma agent	Enables a specific WSMA and associates it with a profile.
wsma dhcp	Enables a WSMA with permission to process and enable an incoming Dynamic Host Control Protocol (DHCP) Option 43 message.
wsma id	Assigns unique WSMA IDs to Cisco IOS networking devices.
wsma profile initiator	Enables a WSMA initiator profile and enters WSMA initiator configuration mode.
wsse	Enables the WSSE for a WSMA profile.

wsse

To enable the Web Services Security (WSSE) Header for a Web Services Management Agent (WSMA), use the **wsse** command in WSMA initiator or listener configuration mode. To disable the security header, use the **no** form of this command.

wsse

no wsse [**authorization level** *level*]

Syntax Description

authorization level *level*	(Optional) Specifies the authorization level parameters to use when WSSE is disabled. The range is from 1 to 15. The default is 1.

Command Default

WSSE is enabled. When WSSE is disabled the default authorization level is set to 1 (the lowest level).

Command Modes

WSMA initiator configuration (config-wsma-init)

WSMA listener configuration (config-wsma-listen)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.1(1)T	This command was modified. Support was added for the **authorization level** keyword and for WSMA initiator configuration mode.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

You can use the **wsse** command to enable the WSSE for a WSMA profile. When enabled, the WSSE username and password are required in the Simple Object Access Protocol (SOAP) header. By default, this command is enabled and the nonvolatile generation (NVGEN) operation does not take place. Specifying the **no wsse** command enables the NVGEN operation.

The username in the WSSE header is authenticated and authorized using the authentication method set in the global configuration. If authentication, authorization, and accounting (AAA) is enabled on the router then the AAA settings are used. If AAA is disabled, the username and password in the WSSE header is compared to the username and password configured on the router.

When the WSSE SOAP header is disabled for a WSMA listener or initiator profile, the **authorization level** keyword can be used to select an authorization level for commands executed using the profile.

When the WSSE SOAP header is disabled for a WSMA profile, the authorization level assigned to requests over the configured connections is determined as follows:

- For HTTP, Secure HTTP (HTTPS), or Secure Shell (SSH) listener connections, the user details are extracted from the transport user's credentials. The authorization level used for the request is the lesser of the authenticated user's privilege level and the level configured using the **no wsse authorization level** *level* command.
- For the Transport Layer Security (TLS) listener connections, no user is associated with the connection because the protocol does not require user and password based authentication. Authentication is performed using certificates. The authorization level used for the request is the lesser of privilege 15 and the level configured using the **no wsse authorization level** *level* command.
- For HTTP, HTTPS, SSH, or TLS initiator connections, no user is associated with the connection because these are outgoing connections. If no user information is available, the authorization level set using the **no wsse authorization level** *level* command is used for all agents associated with the profile.
- If no authorization level is set, the default privilege level is used. The default privilege level is set to 1 (the minimum level).

Use this command in WSMA listener configuration mode or WSMA initiator configuration mode. To enter WSMA listener configuration mode, use the **wsma profile listener** command in global configuration mode. To enter WSMA initiator configuration mode, use the **wsma profile initiator** command in global configuration mode.

Examples

The following example shows how to enable WSSE on a WSMA listener profile:

```
Router(config)# wsma profile listener prof1
Router(config-wsma-listen)# wsse
```

The following example shows how to specify the authorization level parameters to use when WSSE is disabled on a WSMA initiator profile:

```
Router(config)# wsma profile initiator prof2
Router(config-wsma-init)# no wsse authorization level 3
```

Related Commands

Command	Description
acl	Enables ACLs for restricting addresses that can connect to a WSMA profile.
backup excluded	Sets the time that the WSMA profile must wait after a connection is lost before attempting to connect to the backup transport configuration.
backup hold	Sets the time that the WSMA profile remains connected to the backup transport configuration.
encap	Configures an encapsulation for a WSMA profile.
idle-timeout	Sets a time for the WSMA profile to keep the session alive in the absence of any data traffic.

Command	Description
keepalive	Enables keepalive messages and configures interval and retry values for a WSMA profile.
max-message	Sets the maximum size limit for incoming messages.
reconnect	Specifies the time for the WSMA initiator profile to wait before attempting to reconnect a session.
stealth	Disables WSMA from sending SOAP faults.
transport	Defines a transport configuration for a WSMA profile.
wsma profile initiator	Enables a WSMA initiator profile and enters WSMA initiator configuration mode.
wsma profile listener	Enables a WSMA listener profile and enters WSMA listener configuration mode.