



Web Services Management Agent

First Published: February 27, 2009

Last Updated: February 27, 2009

The Web Services Management Agent (WSMA) defines a mechanism through which a network device can be managed, configuration data information can be retrieved, and new configuration data can be uploaded and manipulated. WSMA uses Extensible Markup Language (XML)-based data encoding, that is transported by the Simple Object Access Protocol (SOAP), for the configuration data and protocol messages.

You can use WSMA over Secure Shell Version 2 (SSHv2), HTTP, or HTTPS to access the entire Cisco command-line interface (CLI). Multiple WSMA clients can connect to the WSMA server running on Cisco IOS software. WSMA accesses SSH and HTTP by configuring service listener, which defines how SSH or HTTP is used.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for WSMA” section on page 27](#).

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

- [Prerequisites for WSMA, page 2](#)
- [Restrictions for WSMA, page 2](#)
- [Information about WSMA, page 2](#)
- [How to Configure WSMA, page 6](#)



Americas Headquarters:

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

- [Configuration Examples for WSMA, page 22](#)
- [Additional References, page 25](#)
- [Feature Information for WSMA, page 27](#)
- [Glossary, page 28](#)

Prerequisites for WSMA

- Every WSMA agent must be associated with a WSMA profile to perform any operations. If WSMA agents are not properly associated with profiles, the WSMA agents cannot send or receive any messages.
- WSMA over SSHv2 requires that a vty line be available for each WSMA session.

Restrictions for WSMA

- Only SSHv2 is supported.
- You must be running a crypto image in order to configure HTTP or HTTPS.

Information about WSMA

Before configuring WSMA, you should understand the following concepts:

- [WSMA Overview, page 2](#)
- [WSMA Profiles, page 3](#)
- [Service Listener, page 3](#)
- [SOAP, page 3](#)
- [WSMA over SSHv2, page 3](#)
- [WSMA over HTTP, page 4](#)
- [WSMA ID, page 5](#)
- [WSMA Security, page 5](#)
- [WSMA Schema, page 6](#)

WSMA Overview

Web Services Management Agent (WSMA) is a family of embedded agents, used by the point-to-point management application to fully manage a device.

The current set of WSMA is as follows:

- Config WSMA—Validates and applies a set of configuration commands to Cisco IOS software.
- Exec WSMA—Handles the EXEC-mode command-line operations on Cisco IOS software.
- Filesys WSMA—Copies and validates files between local and remote file systems.

- Notification WSMA—Collects configuration-change events and forwards the details to the management application, which is configured to get the notifications.

WSMA Profiles

WSMA profiles abstract away the working of the transport layer from the WSMA. The transport protocol and an encapsulation together form a WSMA profile. Any WSMA agent must be associated with a specific WSMA profile to perform valid operations. WSMA profiles demultiplex requests to the appropriate WSMA.

WSMA profiles work as a transport termination point, and allows transport and XML encapsulation parameters to be configured.

- The configurable encapsulations for WSMA are SOAP 1.1 and SOAP 1.2.
- The transportation mechanism for WSMA include SSH, HTTP, and HTTPS. This mechanism opens listening sockets for listeners on the router or connecting sockets for clients on the router.

Service Listener

The service listener is a type of WSMA profile that listens for incoming connections and accepts devices from allowed addresses or accepted user IDs. The accepted addresses are configured by defining an access list.

Accepted user IDs are configured by defining the transport method that the service listener listens for. The transport method (SSH or HTTP) enforces the specific user ID that is accepted.

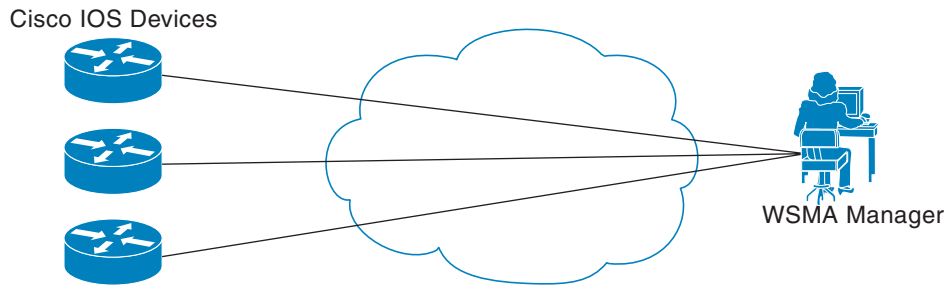
SOAP

SOAP is an industry-standard protocol to exchange XML data between applications. It defines a common mechanism to handle corrupted XML messages. It has a header mechanism to collate metadata associated with a transaction.

SOAP 1.1 and SOAP 1.2 have different schema definitions. They can co-exist with no impact on the other. Cisco IOS software has both SOAP 1.1 and SOAP 1.2 libraries. SOAP has mechanisms to handle XML framing and operational errors in a generic manner allowing greater interoperability of XML-based applications.

WSMA over SSHv2

To run the WSMA over SSHv2 feature, the WSMA agent needs to be configured to use a service profile that is using SSH as a transport method. [Figure 1](#) shows a basic WSMA over SSHv2 network configuration. The client and server exchange keys for security and password encryption. The user ID and password of the SSHv2 session running WSMA are used for authorization and authentication purposes. The user privilege level is enforced and the client session may not have full access to the WSMA operations if the privilege level is not high enough. If authentication, authorization, and accounting (AAA) is configured, the AAA service is used as if a user had established an SSH session directly to the device. Using the existing security configuration makes the transition to WSMA almost seamless. Once the client has been successfully authenticated, the client invokes the SSH connection protocol and the SSH session is established. After the SSH session is established, the user or application invokes WSMA as an SSH subsystem. The default name for the subsystem is “wsma.”

Figure 1 WSMA over SSHv2**SSHv2**

SSHv2 runs on top of a reliable transport layer and provides strong authentication and encryption capabilities. SSHv2 provides a means to securely access and securely execute commands on another computer over a network.

Service listeners do not support SSHv1. The configuration for the SSHv2 server is similar to the configuration for SSHv1. Use the **ip ssh version** command to specify which version of SSH that you want to configure. If you do not configure this command, SSH by default runs in compatibility mode; that is, both SSHv1 and SSHv2 connections are honored.

**Note**

SSHv1 is a protocol that has never been defined in a standard. If you do not want your router to fall back to the undefined protocol (version 1), you should use the **ip ssh version** command and specify version 2.

Use the **ip ssh rsa keypair-name** command to enable an SSH connection using Rivest, Shamir, and Adelman (RSA) keys that you have configured. If you configure the **ip ssh rsa keypair-name** command with a key-pair name, SSH is enabled if the key pair exists, or SSH will be enabled if the key pair is generated later. If you use this command to enable SSH, you do not need to configure a hostname and a domain name.

WSMA over HTTP

To run the WSMA over HTTP, the WSMA agent needs to be configured to use a service listener which is using either HTTP or HTTPS as a transport. For HTTPS, the client and server exchange keys for security and password encryption. The user ID and password of the HTTP or HTTPS session running WSMA are used for authorization and authentication purposes. The user privilege level is enforced and the client session may not have full access to the WSMA operations if the privilege level is not high enough. If AAA is configured, the AAA service is used as if a user had established an SSH session directly to the device. Using the existing security configuration makes the transition to WSMA almost seamless. After the HTTP or HTTPS session is established, the user or application invokes WSMA as a HTTP path. The default name for the path is “/wsma.”

**Note**

Privileged fifteen HTTP or HTTPS users can access the WSMA functionality.

HTTP

HTTP is a reliable request/response protocol that runs on top of a reliable transport layer. HTTPS provides strong authentication and encryption capabilities.

HTTP is configured with the **ip http server** command and HTTPS is configured using the **ip http secure-server** command.

Access Lists

You can optionally configure access lists for use with a service listener. An access list is a sequential collection of permit and deny conditions that applies to IP addresses. The Cisco IOS software tests addresses against the conditions in an access list one by one. The first match determines whether the software accepts or rejects the address. Because the software stops testing conditions after the first match, the order of the conditions is critical. If no conditions match, the software rejects the address.

The two main tasks involved in using access lists are as follows:

1. Creating an access list by specifying an access list number or name and access conditions.
2. Applying the access list to interfaces or terminal lines.

For more information about configuring access lists, see Part 3: Traffic Filtering, Firewalls, and Virus Detection of the *Cisco IOS Security Configuration Guide*, Release 12.4T.

WSMA ID

The WSMA IDs allow Cisco IOS networking devices to have unique IDs. This is important in a NAT or DHCP network where all the device IP addresses are locally significant. In this type of deployment the WSMA ID can be used to give each device a globally unique ID.

The WSMA ID can be explicitly configured based on other properties of the device such as:

- The hardware serial number
- Hostname
- IP address of an interface
- MAC address of an interface
- A user-defined string

Whenever the WSMA ID changes, all WSMA sessions are disconnected. This is to protect the management applications from not having to deal with synchronizing the state dynamically.

WSMA Security

WSMA security is integrated with AAA configuration of Cisco IOS software. The AAA associations configured on the transport layer are used by WSMA.

WSMA is designed for point-to-point operation and works over an encrypted transport. The security on the transport layer identifies and authenticates the users.

WSSE

Web Services Security Header (WSSE) is the SOAP security extension.

The WSMA profiles can be configured to expect or ignore additional security headers in the SOAP messages depending on the deployment mode. If WSMA is configured to contain a security header, the format of the header is as per the SOAP security extension, WSSE.

SOAP enforces authentication using the WSSE header. If there are any authentication errors, they are reported as SOAP faults. The authenticated message is passed on to the WSMA which checks for the authorization level of the user before applying any operation. Authorization errors are reported as a WSMA error response.

If WSMA profiles are configured not to contain the WSSE, then the security header is ignored and the transport login credentials are used for authentication. If WSSE is expected, then the details of the security header are used to authenticate the user. If the security header is missing, the incoming message is discarded and a SOAP fault is issued.

WSMA Schema

Each WSMA publishes its XML schema. It describes the XML messages that the specific WSMA is capable of understanding and executing. The WSMA schema defines the entire data required to execute an operation and ensures operations can be performed identically regardless of the type of transport used to carry the message.

How to Configure WSMA

This section contains the following tasks:

- [Enabling SSHv2 Using a Hostname and Domain Name, page 6](#), (required)
- [Enabling the HTTP Server, page 7](#), (required)
- [Enabling the HTTPS Server, page 8](#), (required)
- [Verifying the Status of the SSH Connection, page 10](#), (optional)
- [Enabling Service Listener, page 12](#), (required)
- [Enabling WSMA, page 13](#), (required)
- [Assigning WSMA IDs, page 14](#), (required)
- [Monitoring and Maintaining WSMA Sessions, page 15](#), (optional)
- [Monitoring and Maintaining WSMA Profiles, page 16](#), (optional)
- [Delivering WSMA Payloads, page 17](#), (optional)

Enabling SSHv2 Using a Hostname and Domain Name

Perform this task to configure your router for SSHv2 using a hostname and domain name.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hostname** *hostname*
4. **ip domain-name** *name*
5. **crypto key generate rsa**
6. **ip ssh** [*timeout seconds* | **authentication-retries** *integer*]
7. **ip ssh version 2**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	hostname hostname Example: Router(config)# hostname host1	Configures a hostname for your router.
Step 4	ip domain-name name Example: Router(config)# ip domain-name domain1.com	Configures a domain name for your router.
Step 5	crypto key generate rsa Example: Router(config)# crypto key generate rsa	Enables the SSH server for local and remote authentication.
Step 6	ip ssh [timeout seconds authentication-retries integer] Example: Router(config)# ip ssh timeout 120	(Optional) Configures SSH control variables on your router.
Step 7	ip ssh version 2 Example: Router(config)# ip ssh version 2	Specifies the version of SSH to be run on your router.

Enabling the HTTP Server

Perform this task to enable the HTTP server. The HTTP server is disabled by default. Once the HTTP server is enabled, you can configure optional server characteristics. For more information on configuring optional server characteristics for HTTP server, refer to “[HTTP 1.1 Web Server and Client](#)” chapter of *Cisco IOS Network Management Configuration Guide*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip http server Example: Router(config)# ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface. <p>Note If you are enabling the HTTP over Secure Socket Layer (HTTPS) server using the ip http secure-server command, you should disable the standard HTTP server using the no ip http server command. This command is required to ensure only secure connections to the server.</p>

Enabling the HTTPS Server

To disable the standard HTTP server and configure the HTTPS server with SSL 3.0, complete the procedure in this section.

Prerequisites

If a certificate authority is to be used for certification, you should declare the CA trustpoint on the routing device before enabling the secure HTTP server. For more information on declaring CA trustpoints on the routing device, refer to “[HTTPS - HTTP Server and Client with SSL 3.0](#)” chapter of the *Cisco IOS Network Management Configuration Guide*.

SUMMARY STEPS

1. **enable**
2. **show ip http server status**
3. **configure terminal**
4. **no ip http server**
5. **ip http secure-server**
6. **ip http secure-port** *port-number*
7. **ip http secure-ciphersuite** [3des-ede-cbc-sha] [rc4-128-sha] [rc4-128-md5] [des-cbc-sha]
8. **ip http secure-client-auth**
9. **ip http secure-trustpoint** *name*
10. **end**
11. **show ip http server secure status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>Router# show ip http server status</p> <p>Example: Router# show ip http server status</p>	<p>(Optional) Displays the status of the HTTP server.</p> <ul style="list-style-type: none"> If you are unsure whether the secure HTTP server is supported in the software image you are running, enter this command and look for the line “HTTP secure server capability: {Present Not present}”. This command displays the status of the standard HTTP server (enabled or disabled).
Step 3	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 4	<p>no ip http server</p> <p>Example: Router(config)# no ip http server</p>	<p>Disables the standard HTTP server.</p> <p>Note When enabling the HTTPS server you should always disable the standard HTTP server to prevent insecure connections to the same services. This is a precautionary step (typically, the HTTP server is disabled by default).</p>
Step 5	<p>ip http secure-server</p> <p>Example: Router(config)# ip http secure-server</p>	<p>Enables the HTTPS server.</p>
Step 6	<p>ip http secure-port <i>port-number</i></p> <p>Example: Router(config)# ip http secure-port 1025</p>	<p>(Optional) Specifies the port number that should be used for the HTTPS server. The default port number is 443. Valid options are 443 or any number in the range 1025 to 65535.</p>
Step 7	<p>ip http secure-ciphersuite [3des-ede-cbc-sha] [rc4-128-sha] [rc4-128-md5] [des-cbc-sha]</p> <p>Example: Router(config)# ip http secure-ciphersuite rc4-128-sha rc4-128-md5</p>	<p>(Optional) Specifies the CipherSuites (encryption algorithms) that should be used for encryption over the HTTPS connection.</p> <ul style="list-style-type: none"> This command allows you to restrict the list of CipherSuites that the server offers the connecting clients. For example, you may want to allow only the most secure CipherSuite to be used. Unless you have a reason to specify the CipherSuites that should be used, or you are unfamiliar with the details of these CipherSuites, you should leave this command unconfigured and let the server and client negotiate the CipherSuite that they both support (this is the default).

	Command or Action	Purpose
Step 8	<pre>ip http secure-client-auth</pre> <p>Example: Router(config)# ip http secure-client-auth </p>	<p>(Optional) Configures the HTTP server to request an X.509v3 certificate from the client in order to authenticate the client during the connection process.</p> <ul style="list-style-type: none"> In the default connection and authentication process, the client requests a certificate from the HTTP server, but the server does not attempt to authenticate the client. Authenticating the client provides more security than server authentication by itself, but not all clients may be configured for CA authentication.
Step 9	<pre>ip http secure-trustpoint name</pre> <p>Example: Router(config)# ip http secure-trustpoint trustpoint-01 </p>	<p>Specifies the CA trustpoint that should be used to obtain an X.509v3 security certificate and to authenticate the connecting client's certificate.</p> <ul style="list-style-type: none"> Use of this command assumes you have already declared a CA trustpoint using the crypto ca trustpoint command and associated submode commands. Use the same trustpoint name that you used in the associated crypto ca trustpoint command.
Step 10	<pre>end</pre> <p>Example: Router(config)# end </p>	<p>Ends the current configuration session and returns you to privileged EXEC mode.</p>
Step 11	<pre>show ip http server secure status</pre> <p>Example: Router# show ip http server secure status </p>	<p>Displays the status of the HTTP secure server configuration.</p>

Verifying the Status of the SSH Connection

To display the status of the SSH connection on your router, use the **show ssh** and **show ip ssh** commands.

SUMMARY STEPS

1. **enable**
2. **show ssh**
3. **show ip ssh**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show ssh Example: Router# show ssh	Displays the status of SSH server connections.
Step 3	show ip ssh Example: Router# show ip ssh	Displays the version and configuration data for SSH.

Examples

The following sample output from the **show ssh** command displays status about SSHv2 connections.

```
Router# show ssh

Connection Version Mode Encryption Hmac          State
Username
1           2.0      IN   aes128-cbc hmac-md5      Session started   lab
1           2.0      OUT  aes128-cbc hmac-md5      Session started   lab
%No SSHv1 server connections running.
```

The following sample output from the **show ip ssh** command displays the version of SSH that is enabled, the authentication timeout values, and the number of authentication retries.

```
Router# show ip ssh

SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```

Troubleshooting Tips

The **ip ssh version** command can be used for troubleshooting your SSH configuration. By changing versions, you can determine which SSH version has a problem.

What to Do Next

For more information about the **ssh** command, see the *Cisco IOS Security Command Reference*, Release 12.2SR.

Enabling Service Listener

To enable a service listener, perform the following task:

Prerequisites

- If you configure service listener over SSH, you must first configure SSH.
- If you configure service listener over HTTP, you must first configure HTTP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **wsma profile listener** *profile-name*
4. **encap** {**soap11** | **soap12**}
5. **transport** {**ssh** **subsys** *subsys-name* | **http** **path** *path-name* | **https** **path** *path-name*}
6. **idle-timeout** *minutes*
7. **max-message** *message-size*
8. **acl** *acl-number*
9. **stealth**
10. **wsse**

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	wsma profile listener <i>profile-name</i> Example: Router(config)# wsma profile listener prof1	Creates a service listener and enters the WSMA listener configuration mode.
Step 4	encap { soap11 soap12 }	(Optional) Configures an encapsulation for the service listener profile.
	Example: Router(config-wsma-listen)# encap soap12	

	Command or Action	Purpose
Step 5	transport { ssh subsys <i>subsys-name</i> http path <i>path-name</i> https path <i>path-name</i> } Example: Router(config-wsma-listen)# transport ssh subsys wsma	Defines a transport configuration for the WSMA profile.
Step 6	idle-timeout <i>minutes</i> Example: Router(config-wsma-listen)# idle-timeout 345	(Optional) Specifies the amount of time (in minutes) to keep the session alive in the absence of any data traffic.
Step 7	max-message <i>message-size</i> Example: Router(config-wsma-listen)# max-message 290	(Optional) Specifies the maximum receive message size (between 1 to 2000 kbytes).
Step 8	acl <i>acl-number</i> Example: Router(config-wsma-listen)# acl 34	(Optional) Defines the ACL group to use.
Step 9	stealth Example: Router(config-wsma-listen)# stealth	(Optional) Configures the service to not send SOAP fault messages in response to corrupted XML messages.
Step 10	wsse Example: Router(config-wsma-listen)# wsse	(Optional) Enables the Web Services Security Header (WSSE) for a WSMA profile. <ul style="list-style-type: none"> By default, WSSE is enabled. Enter the no wsse command to disable WSSE.

Enabling WSMA

Perform this task to enable a specific WSMA and associate it with a profile.

Prerequisites

A service listener must be configured and enabled.

SUMMARY STEPS

- enable**
- configure terminal**
- wsma agent** {**config** | **exec** | **fileSYS** | **notify**} **profile** *profile-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	wsma agent {config exec fileysys notify} profile profile-name Example: Router(config)# wsma agent config profile prof1	Enables the WSMA and associates it with a profile.

Assigning WSMA IDs

Perform this task to assign unique WSMA IDs to Cisco IOS networking devices.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<pre>wsma id {hardware-serial hostname ip-address interface-type mac-address interface-type string value}</pre> <p>Example: Router(config)# wsma id ip-address fastethernet 0/1</p>	Assigns unique WSMA IDs to Cisco IOS networking devices.

Monitoring and Maintaining WSMA Sessions

Perform this task to monitor and maintain WSMA sessions, perform the following task:

SUMMARY STEPS

1. `enable`
2. `show wsma agent {counters | schema} [config | exec | filesys | notify]`
3. `debug wsma agent [config | exec | filesys | notify]`
4. `clear wsma agent [config | exec | filesys | notify] counters`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p>Example: Router> enable</p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<pre>show wsma agent {counters schema} [config exec filesys notify]</pre> <p>Example: Router# show wsma agent config counters</p>	Displays the specified statistics counters, or schema for the WSMA.
Step 3	<pre>debug wsma agent [config exec filesys notify]</pre> <p>Example: Router#debug wsma agent config</p>	Enables debugging of WSMA.
Step 4	<pre>clear wsma counters [config exec filesys notify] counters</pre> <p>Example: Router#clear wsma agent filesys counters</p>	Clears WSMA statistics counters for all WSMA types.

Examples

The counters return the following information:

- messages received—The total number of messages that were passed from the service profile into the WSMA.
- replies sent—The total number of reply messages sent to the services profile.
- faults—The number of faults that prevented a received message producing a reply.

```
Router# show wsma agent config counters
```

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

```
Router#show wsma config schema
```

```
New Name Space 'urn:cisco:wsma-config'
<VirtualRootTag> [0, 1] required
  <WSMA-Config> [0, 1] required
    <request> 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
```

Monitoring and Maintaining WSMA Profiles

Perform this task to monitor and maintain service listeners.

SUMMARY STEPS

1. **enable**
2. **show wsma profile {connections | counters | schema} [name profile-name]**
3. **debug wsma profile listener**
4. **clear wsma profile [profile-name] {connections | counters}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router>enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show wsma profile {connections counters schema} [name profile-name] Example: Router# show wsma profile connection	Displays the specified service profile connections, statistics counters, or schema.

	Command or Action	Purpose
Step 3	<code>debug wsma profile listener</code>	Enables debugging of WSMA profiles.
	Example: Router# debug wsma profile listener	
Step 4	<code>clear wsma profile [profile-name] {connections counters}</code>	Clears WSMA profile sessions or statistic counters.
	Example: Router# clear wsma profile prof1 counters	

Delivering WSMA Payloads

An XML payload is typically wrapped in a SOAP message for data transportation. Without a correct design of SOAP messages, an XML payload may not be exchanged properly even if the payload follows a common XML schema. The XML payload over all transports is identical. WSMA support both SOAP1.1 and SOAP1.2. The SOAP header supports two modes of security, no wsse and wsse.

Use the following XML to deliver WSMA payloads:

WSMA EXEC Request : Ping

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <SOAP:Body>
    <request xmlns="urn:cisco:wsma-exec" correlator="01">
      <execCLI>
        <cmd>ping oz-dirt</cmd>
      </execCLI>
    </request>
  </SOAP:Body>
</SOAP:Envelope>]]>]]>
```

WSMA EXEC Response:Ping

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <SOAP:Body>
    <response xmlns="urn:cisco:wsma-exec" correlator="01" success="1">
      <execLog>
        <dialogueLog>
          <sent>ping oz-dirt</sent>
          <received>Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.1.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms</received>
        </dialogueLog>
      </execLog>
    </response>
  </SOAP:Body>
</SOAP:Envelope>]]>]]>
```

WSMA Config Request: CMD Data Model

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <SOAP:Body>
    <request xmlns="urn:cisco:wsma-config" correlator="4.1">
      <configApply details="all">
        <config-data>
          <cli-config-data>
            <cmd>no cns config partial mixy</cmd>
            <cmd>no stupid</cmd>
            <cmd>no cns exec 80 </cmd>
          </cli-config-data>
        </config-data>
      </configApply>
    </request>
  </SOAP:Body>
</SOAP:Envelope>]]]]>
```

WSMA Config Response: CMD Data Model

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <SOAP:Body>
    <response xmlns="urn:cisco:wsma-config" correlator="4.1" success="1">
      <resultEntry lineNumber="1" cliString="no cns config partial mixy">
        <success change="NO_CHANGE" mode="IMMEDIATE" />
      </resultEntry>
      <resultEntry lineNumber="2" cliString="no stupid">
        <failure errorType="TEMPORARY" errorCode="PARSE_ERROR_NOMATCH" />
      </resultEntry>
      <resultEntry lineNumber="3" cliString="no cns exec 80 ">
        <success change="NO_CHANGE" mode="IMMEDIATE" />
      </resultEntry>
    </response>
  </SOAP:Body>
</SOAP:Envelope>]]]]>
```

WSMA Config Request: Block Data Model

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <SOAP:Body>
    <request xmlns="urn:cisco:wsma-config" correlator="5.1">
      <configApply details="all">
        <config-data>
          <cli-config-data-block>no cns config partial mixy
no stupid
no cns exec 80</cli-config-data-block>
        </config-data>
      </configApply>
    </request>
  </SOAP:Body>
</SOAP:Envelope>]]]]>
```

WSMA Config Response: Block Data Model

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <SOAP:Body>
    <response xmlns="urn:cisco:wsma-config" correlator="5.1" success="1">
      <resultEntry lineNumber="1" cliString="no cns config partial mixy">
        <success change="NO_CHANGE" mode="IMMEDIATE" />
      </resultEntry>
      <resultEntry lineNumber="2" cliString="no stupid">
        <failure errorType="TEMPORARY" errorCode="PARSE_ERROR_NOMATCH" />
      </resultEntry>
      <resultEntry lineNumber="3" cliString="no cns exec 80">
        <success change="NO_CHANGE" mode="IMMEDIATE" />
      </resultEntry>
    </response>
  </SOAP:Body>
</SOAP:Envelope>]]>]]>
```

WSMA Config Request: EDI Data Model

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <SOAP:Body>
    <request xmlns="urn:cisco:wsma-config" correlator="6.1">
      <configApply details="all">
        <config-data>
          <xml-config-data>
            <Device-Configuration><cns operation="delete" >
<config><partial><HostNameAddressConfigurationServer>mixy</HostNameAddressConfigurationServer><PortNumberConfigServiceDefault80>80</PortNumberConfigServiceDefault80></partial></config></cns><stupid operation="delete" /><cns operation="delete"
><exec><P>80</P></exec></cns> </Device-Configuration>
            </xml-config-data>
          </config-data>
        </configApply>
      </request>
    </SOAP:Body>
  </SOAP:Envelope>]]>]]>
```

WSMA Config Response: EDI Data Model

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <SOAP:Body>
    <response xmlns="urn:cisco:wsma-config" correlator="6.1" success="1">
      <resultEntry lineNumber="1" cliString="no cns config partial mixy 80">
        <success change="NO_CHANGE" mode="IMMEDIATE" />
      </resultEntry>
      <resultEntry lineNumber="2" cliString="no stupid">
        <failure errorType="TEMPORARY" errorCode="PARSE_ERROR_NOMATCH" />
      </resultEntry>
    </response>
  </SOAP:Body>
</SOAP:Envelope>]]>]]>
```

```

        </resultEntry>
        <resultEntry lineNumber="3" cliString="no cns exec 80">
            <success change="NO_CHANGE" mode="IMMEDIATE" />
        </resultEntry>
    </response>
</SOAP:Body>
</SOAP:Envelope>]]>]]>

```

WSMA File List Request

```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <SOAP:Body>
        <request xmlns="urn:cisco:wsma-filesystem" correlator="2"><fileList/></request>
    </SOAP:Body>
</SOAP:Envelope>]]>]]>

```

WSMA File List Response

```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <SOAP:Body>
        <response xmlns="urn:cisco:wsma-filesystem" correlator="2" success="1">
            <fileSystemList>
                <fileSystem name="nvram" type="nvram" size="522232" freespace="516471"
readable="true" writeable="true">
                    <directory name="/" fullName="nvram:/" readFlag="true"
writeFlag="true">
                        <file name="startup-config" fullName="nvram:/startup-config"
size="2134" readFlag="true" writeFlag="true"/>
                        <file name="private-config" fullName="nvram:/private-config"
size="1527" readFlag="false" writeFlag="false"/>
                        <file name="underlying-config" fullName="nvram:/underlying-config"
size="2134" readFlag="true" writeFlag="true"/>
                        <file name="persistent-data" fullName="nvram:/persistent-data"
size="99" readFlag="false" writeFlag="false"/>
                        <file name="ifIndex-table" fullName="nvram:/ifIndex-table" size="0"
readFlag="true" writeFlag="true"/>
                    </directory>
                </fileSystem>
                <fileSystem name="disk2" type="disk" size="64229376" freespace="63987712"
readable="true" writeable="true">
                    <directory name="/" fullName="disk2:/" readFlag="true" writeFlag="true"
modDate="1979-11-30T00:00:00.000Z">
                        <file name="spec.odm" fullName="disk2:/spec.odm" size="131739"
readFlag="true" writeFlag="true" modDate="2007-08-31T05:11:36.000Z"/>
                    </directory>
                </fileSystem>
                <fileSystem name="bootflash" type="flash" size="14942208"
freespace="8455208" readable="true" writeable="true">
                    <directory name="/" fullName="bootflash:/" readFlag="true"
writeFlag="true">
                        <file name="c7200-kboot-mz.bw"
fullName="bootflash:/c7200-kboot-mz.bw" size="5131872" readFlag="true" writeFlag="true"
modDate="1999-11-30T00:01:47.000Z"/>
                    </directory>
                </fileSystem>
            </fileSystemList>
        </response>
    </SOAP:Body>
</SOAP:Envelope>]]>]]>

```

```

        <file name="startup-config.base"
fullName="bootflash:/startup-config.base" size="1808" readFlag="true" writeFlag="true"
modDate="1999-11-30T00:23:26.000Z"/>
        <file name="startup-config.12dec03.balam"
fullName="bootflash:/startup-config.12dec03.balam" size="1598" readFlag="true"
writeFlag="true" modDate="2000-01-05T22:54:50.000Z"/>
    </directory>
</fileSystem>
</fileSystemList>
</response>
</SOAP:Body>
</SOAP:Envelope>]]>]]>

```

WSMA File Copy Request

```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <SOAP:Body>
        <request xmlns="urn:cisco:wsma-filesystem" correlator="12">
            <fileCopy erase="0" overwrite="1" filesize="131739">
                <srcURL>tftp://oz-dirt/jbalestr/spec.odm</srcURL>
                <dstURL>test</dstURL>
            </fileCopy>
        </request>
    </SOAP:Body>
</SOAP:Envelope>]]>]]>

```

WSMA File Copy Response

```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <SOAP:Body>
        <response xmlns="urn:cisco:wsma-filesystem" correlator="12" success="1">
            <copyStatus></copyStatus>
        </response>
    </SOAP:Body>
</SOAP:Envelope>]]>]]>

```

WSMA File Delete Request

```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <SOAP:Body>
        <request xmlns="urn:cisco:wsma-filesystem" correlator="6">
            <fileDelete>
                <deleteFileList>
                    <filename>brick</filename>
                </deleteFileList>
            </fileDelete>
        </request>
    </SOAP:Body>
</SOAP:Envelope>]]>]]>

```

WSMA File Delete Response

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <SOAP:Body>
    <response xmlns="urn:cisco:wsma-filesystem" correlator="6" success="1">
      <deleteStatusList>
        <deleteStatus>
          <fileName>brick</fileName>
          <status>DELETED</status>
        </deleteStatus>
      </deleteStatusList>
    </response>
  </SOAP:Body>
</SOAP:Envelope>]]]]>
```

Configuration Examples for WSMA

This section provides the following configuration examples:

- [Enabling SSHv2 Using a Hostname and Domain Name: Example, page 22](#)
- [Enabling SSHv2 Using RSA Keys: Example, page 22](#)
- [Configuring WSMA: Example, page 23](#)
- [Configuring the WSMA Listener Profile with Different Parameters: Example, page 23](#)
- [Displaying WSMA Profile Parameters: Example, page 23](#)

Enabling SSHv2 Using a Hostname and Domain Name: Example

The following example shows how to configure SSHv2 using a hostname and a domain name:

```
configure terminal
hostname host1
ip domain-name domain1.com
crypto key generate rsa
ip ssh timeout 120
ip ssh version 2
```

Enabling SSHv2 Using RSA Keys: Example

The following example shows how to configure SSHv2 using RSA keys:

```
configure terminal
ip ssh rsa keypair-name sshkeys
crypto key generate rsa usage-keys label sshkeys modulus 768
ip ssh timeout 120
ip ssh version 2
```

Configuring WSMA: Example

The following example shows how to configure WSMA:

```
configure terminal
wsma agent config profile prof
```

Configuring the WSMA Listener Profile with Different Parameters: Example

The following example shows how to configure WSMA over SSHv2:

```
configure terminal
wsma profile listener mySession
  transport ssh subsystem wsma
  acl 34
  encaps soap12
exit
```

Displaying WSMA Profile Parameters: Example

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

```
Router# show wsma profile connection

listener session dog: 0 open connections: 0 closing connections
Encap: soap11
Max message (RX) is 50 Kbytes
SOAP Faults are sent
Idle timeout infinite
Listening via ssh
SSH listener, 3 sessions accepted, 0 sessions rejected
listener session dog1: 0 open connections: 0 closing connections
Encap: soap11
Max message (RX) is 50 Kbytes
SOAP Faults are sent
Idle timeout infinite
Listening via ssh
SSH listener, 0 sessions accepted, 0 sessions rejected
```

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

```
Router# show wsma profile counters

Statistics for dog
  incoming total 156, bad XML 30, oversized 0
  outgoing total 167, absorbed 0
  message internal errors 1
Connection Accepts 3, local hangup 0, remote hangup 3
  session internal errors 0
Statistics for dog1
  incoming total 0, bad XML 0, oversized 0
  outgoing total 0, absorbed 0
  message internal errors 0
Connection Accepts 0, local hangup 0, remote hangup 0
  session internal errors 0
```

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

```
Router# show wsma profile schema
```

```

Schema dog
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

```

Additional References

The following sections provide references related to WSMA.

Related Documents

Related Topic	Document Title
IP access lists	Part 3: Traffic Filtering, Firewalls, and Virus Detection of the <i>Cisco IOS Security Configuration Guide</i>
IP access lists commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Security Command Reference</i>
Secure Shell and Secure Shell Version 2	“Configuring Secure Shell” and “Configuring Secure Shell Version 2 Support” sections of the <i>Cisco IOS Security Configuration Guide</i>
Security commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Security Command Reference</i>
Network Management commands (including EEM commands): complete command syntax, defaults, command mode, command history, usage guidelines, and examples.	<i>Cisco IOS Network Management Command Reference</i>

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	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
RFC 2246	<i>The TLS Protocol Version 1.0</i>
RFC 4251	<i>The Secure Shell (SSH) Protocol Architecture</i>
RFC 4252	<i>The Secure Shell (SSH) Authentication Protocol</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Network Management Command Reference* at http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

- **acl**
- **clear wsma agent**
- **clear wsma profile**
- **debug wsma agent**
- **debug wsma profile**
- **encap**
- **idle-timeout**
- **max-message**
- **show wsma agent**
- **show wsma id**
- **show wsma profile**
- **stealth**
- **transport**
- **wsma agent**
- **wsma id**
- **wsma profile**

Feature Information for WSMA

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.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. 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 WSMA

Feature Name	Releases	Feature Information
Web Services Management Agent	12.4(24)T	<p>The WSMA feature enables you to perform network configurations via the Cisco command-line interface (CLI) over an encrypted transport.</p> <p>The WSMA protocol defines a simple mechanism through which a network device can be managed, configuration data information can be retrieved, and new configuration data can be uploaded and manipulated. WSMA uses an Extensible Markup Language (XML)-based data encoding for the configuration data and protocol messages.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • Information about WSMA, page 2 <p>The following commands were introduced:</p> <p>acl, clear wsma agent, clear wsma profile, debug wsma agent, debug wsma profile, encap, idle-timeout, max-message, show wsma agent, show wsma id, show wsma profile, stealth, transport, wsma agent, wsma id, wsma profile</p>

Glossary

SSHv2—Secure Shell Version 2. SSH runs on top of a reliable transport layer and provides strong authentication and encryption capabilities. SSHv2 provides a means to securely access and securely execute commands on another computer over a network.

WSMA—Web Services Management Agent. A protocol that defines a simple mechanism through which a network device can be managed, configuration data information can be retrieved, and new configuration data can be uploaded and manipulated.

XML—Extensible Markup Language. A standard maintained by the World Wide Web Consortium (W3C) that defines a syntax that lets you create markup languages to specify information structures. Information structures define the type of information (for example, subscriber name or address), not how the information looks (bold, italic, and so on). External processes can manipulate these information structures and publish them in a variety of formats. XML allows you to define your own customized markup language.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

.Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.