TR-069 Agent

The digital subscriber line (DSL) Forum's TR-069, CPE WAN Management Protocol (CWMP), is used for communications between a customer premise equipment (CPE) and an auto-configuration server (ACS). The TR-069 Agent feature manages a collection of CPEs, with the primary capability for auto-configuration and dynamic service provisioning, software image management, status and performance monitoring and diagnostics.

Finding Feature Information

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

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

Prerequisites for the TR-069 Agent

The CPE should have an IP address and a WAN connection should be established to access the ACS.

Information About the TR-069 Agent

TR-069 Agent

The TR-069 Agent allows an ACS to provision a CPE or collection of CPEs. The provisioning mechanism includes specific provisioning parameters and a general mechanism for adding vendor-specific provisioning capabilities as needed. The identification mechanisms included in the protocol allow CPE provisioning based either on the requirements of each specific CPE, or on collective criteria such as the CPE vendor, model, software version, or other criteria.

The provisioning mechanism allows CPE provisioning at the time of initial connection to the broadband access network and the ability to reprovision at any subsequent time. This includes support for asynchronous ACS-initiated reprovisioning of a CPE.

The TR-069 Agent also supports image upgrade, configuration application, file downloads, configuration and log file uploads, and CPE monitoring.

Note The TR-069 Agent CPE devices must be set up and enabled for TR-069. An ACS used to communicate with the CPE must be TR-069 compliant in order to enable the TR-069 Agent.

RPC Support

The following remote procedure calls (RPCs) supported with the TR-069 Agent:

- Standard RPCs
  - GetRPCMethods
  - SetParameterValues
  - GetParameterValues
  - GetParameterNames
  - SetParameterAttributes
  - GetParameterAttributes
  - AddObject
  - DeleteObject
  - Reboot
  - Download
  - Upload
- Vendor RPCs
  - X_00000C_SetConfiguration
  - X_00000C_ShowStatus

CWMP Vendor Profile Schema

The following details the CWMP vendor profile schema:

- For SetConfiguration,

```
<cwmp:X_00000C_SetConfiguration>
<ErrorOption> rollback </ErrorOption>
<Target> {running-config | startup-config} </Target>
<ConfigCommandBlock> block of clis separated by newline [\n] character </ConfigCommandBlock>
<ConfigCommandList array of strings[1..unbounded] each of length 256>
<string> IOS Configuration command 1 </string>
<string> IOS Configuration command 2 </string>
</ConfigCommandList>
<ParameterKey> parameterkey </ParameterKey>
</cwmp:X_00000C_SetConfiguration>

ErrorOption => string with length 64
Target => string with length 64
```

On success,

```
<X_00000C_SetConfigurationResponse>
<Status>0</Status>
</X_00000C_SetConfigurationResponse>
```

On failure,

```
<SOAP:Fault>
<SOAP:faultcode>Client</SOAP:faultcode>
<SOAP:faultstring>CWMP fault</SOAP:faultstring>
<SOAP:detail>
<cwmp:Fault>
<FaultCode></FaultCode>
<FaultString></FaultString>

<cwmp:X_00000C_SetConfigurationFault>
<Command>IOS Configuration command that failed</Command>
<FaultCode>parse_cmd() return value</FaultCode>
</cwmp:X_00000C_SetConfigurationFault>

<cwmp:X_00000C_SetConfigurationFault>
<Command>IOS Configuration command that failed</Command>
<FaultCode>parse_cmd() return value</FaultCode>
</cwmp:X_00000C_SetConfigurationFault>

</cwmp:Fault>
</SOAP:detail>
</SOAP:Fault>
```

- For ShowStatus,

```
<cwmp:X_00000C_ShowStatus>
<ExecCommandList array of strings[1..unbounded] each of length 256 >
<string> IOS Exec command 1 </string>
<string> IOS Exec command 2 </string>
<string> IOS Exec command 3 </string>
</ExecCommandList>
</cwmp:X_00000C_ShowStatus>
```

On success,

```
<cwmp:X_00000C_ShowStatusResponse>
<ExecResponseList array of ExecResponseStruct [1..unbounded]>
<ExecResponseStruct>
<Command> IOS Exec command 1 </Command>
```

```
<Response> output of command 1</Response>
</ExecResponseStruct>

<ExecResponseStruct>
<Command> IOS Exec command 2 </Command>
<Response> output of command 2 </Response>
</ExecResponseStruct>

<ExecResponseStruct>
<Command> IOS Exec command 3 </Command>
<Response>output of command 3</Response>
</ExecResponseStruct>

</ExecResponseList>
</cwmp:X_00000C_ShowStatusResponse>
```

On failure,

```
<SOAP:Fault>
<SOAP:faultcode>Client</SOAP:faultcode>
<SOAP:faultstring>CWMP fault</SOAP:faultstring>
<SOAP:detail>
<cwmp:Fault>
<FaultCode></FaultCode>
<FaultString></FaultString>
</cwmp:Fault>
</SOAP:detail>
</SOAP:Fault>
```

HTTP Digest Authentication Support

The TR-069 Agent uses HTTP as the transport and needs support for digest authentication from the HTTP client infrastructure.

Note This feature is not a TR-069 Agent-exclusive feature and can be used in other scenarios to configure HTTP Digest Authentication Support.

HTTP Cookie Support Per RFC2965

A cookie is a piece of HTTP state information generated and sent by an HTTP server in response to an HTTP request. The HTTP client returns the cookie containing the state information back to the HTTP server in its next HTTP request. This scenario is used to create a stateful session with HTTP requests and responses. The TR-069 Agent uses HTTP as the transport and needs support for both Netscape cookies and RFC 2965 in HTTP client infrastructure.

Note This feature is not a TR-069 Agent-exclusive feature and can be used in other scenarios to clear, monitor and troubleshoot HTTP cookies.

Device Gateway Association and Port Mapping Support

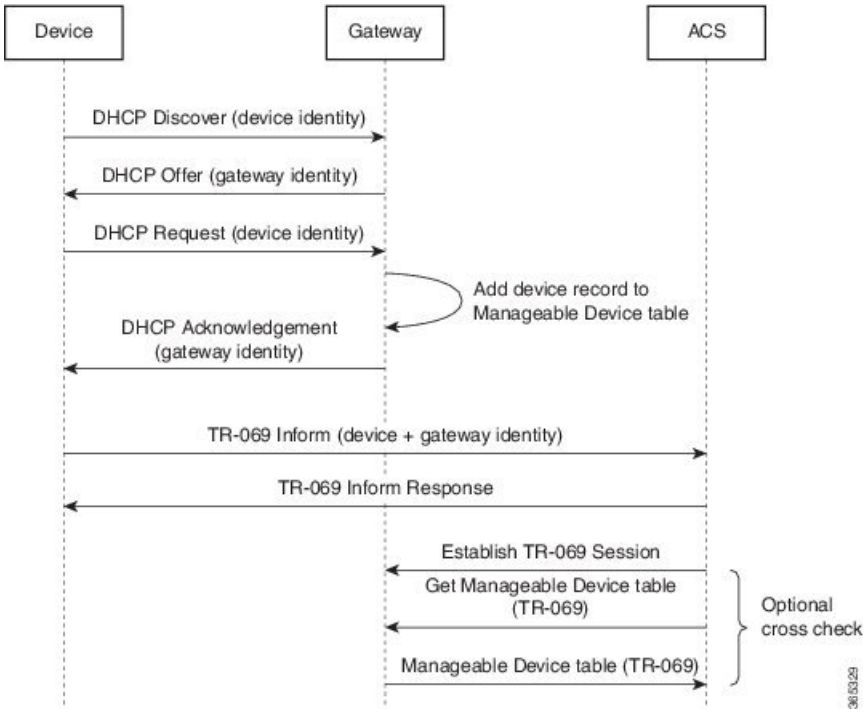
Device Gateway Association

The CPE WAN Management Protocol (CWMP) can be used to remotely manage customer premise equipment (CPE) devices that are connected over a LAN through a gateway. If Auto Configuration Server (ACS) manages both the Device and the Gateway through which the device is connected , ACS determines the identity of the gateway by checking the device gateway association information. The ACS with the device gateway association profile can identify the end devices behind each gateway. The device gateway association constitutes Annex F (previously part of TR-111), part of the TR-069 standard. The mechanism defined for device gateway association relies on the Device's use of Dynamic Host Configuration Protocol (DHCP) Option 125. The end devices will pass on their identity to the gateway via vendor-specific DHCP option. When the gateway receives this information, the gateway populates the ManageableDevice table containing identity information for each device on its LAN. The parameters, which are supported on the gateway as part of device gateway association is as follows:

- **InternetGatewayDevice.ManagementServer.ManageableDeviceNumberOfEntries**
- **InternetGatewayDevice.ManagementServer.ManageableDevice.{i}**
  - **ManufacturerOUI**
  - **ProductClass**
  - **SerialNumber**

The device gateway association functionality does not support configuring IP addresses manually on the end devices. The IP addresses are assigned to the end devices via DHCP by the gateway. You must configure **renew deny unknown** command under the DHCP server configuration to initiate the DHCP discovery process for the end devices after a gateway reload.

Figure 1: Device-Gateway Association using DHCP Discover



The following example shows how to set up the Device-Gateway Association and Port Mapping feature via a Dynamic Host Configuration Protocol (DHCP) on VLAN interface:

```
ip dhcp excluded-address 15.15.15.1
!
ip dhcp pool NET-POOL1
 network 15.15.15.0 255.255.255.0
 default-router 15.15.15.1
 lease 0 0 5
 renew deny unknown
 end
 interface Vlan102
  ip address pool NET-POOL1
  end
```

Port Mapping Support

The CPE WAN Management Protocol (CWMP) can be used to remotely manage customer premise equipment (CPE) devices that are connected via a LAN through a network address translation (NAT) gateway. This can be achieved by making use of the PortMapping functionality. This feature helps in maintaining the privacy of the IP addresses of the end devices as the communication happens with the auto-configuration server (ACS) in the public domain. The gateway supports the following CWMP parameters:

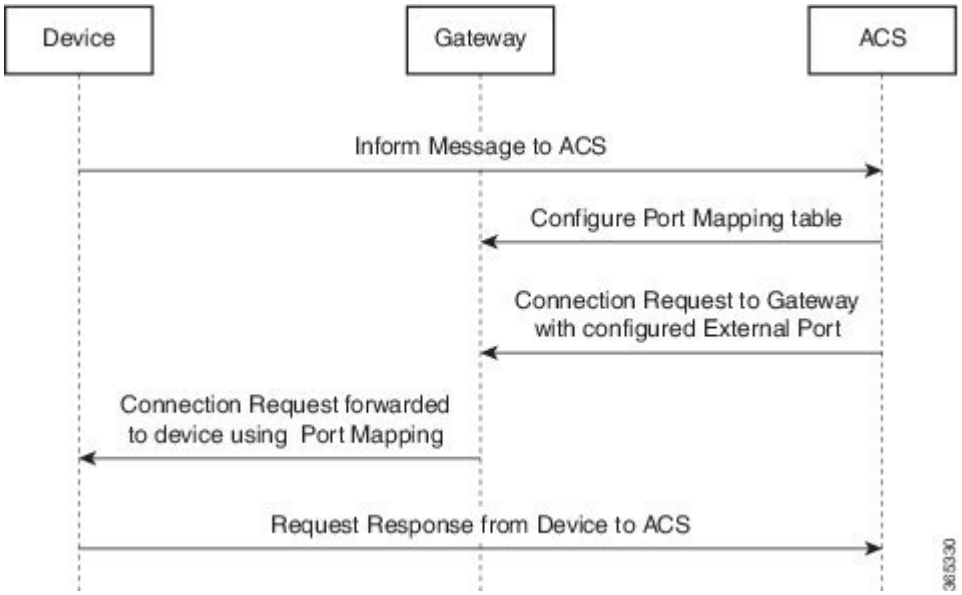
- **InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.PortMappingNumberOfEntries**
- **InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.Port-Mapping.{i}.**
  - **PortMappingEnabled**
  - **PortMappingLeaseDuration**

- **RemoteHost**
- **ExternalPort**
- **InternalPort**
- **PortMappingProtocol**
- **InternalClient**
- **PortMappingDescription**

- **InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPP-Connection.{i}.PortMappingNumberOfEntries**
- **InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPP-Connection.{i}.PortMapping.{i}.**
  - **PortMappingEnabled**
  - **PortMappingLeaseDuration**
  - **RemoteHost**
  - **ExternalPort**
  - **InternalPort**
  - **PortMappingProtocol**
  - **InternalClient**
  - **PortMappingDescription**

Note The ACS must provide values for the mandatory parameters—**ExternalPort**, **InternalPort**, **PortMappingProtocol**, and **InternalClient**—to the gateway for adding the port mapping for an end device. There is no support to limit the portmapping to a particular host using **RemoteHost** parameter.

Figure 2: Connection request via a NAT Gateway using PortMapping table



The following is an example Port Mapping Support on a device configured as a gateway and ACS.

For the below parameters configured on ACS,

```
Destination IP (InternalClient) - 15.15.15.2
Source port (ExternalPort)  - 9000
Destination port (InternalPort) - 7547
PortMappingProtocol - TCP
```

the following NAT command is configured on the gateway:

```
ip nat inside source static tcp 15.15.15.2 7547 10.194.145.170 9000 extendable
```

10.194.145.170 is the RemoteHost and the IP address of the device or gateway provisioned by ACS. This is the IP address corresponding to the interface with the configuration **cwmp wan default** command.

How to Configure and Enable the TR-069 Agent

Setting Up the CPE to Communicate with the ACS

Perform this task and the following tasks to configure and enable the TR-069 agent on the CPE. If an Ethernet or Serial interface is used to communicate with ACS, these tasks need not be performed manually because the tasks are automated by using the AutoInstall feature. For more information on the AutoInstall feature, refer to *Using AutoInstall to Remotely Configure Cisco Networking Devices*. For an example on configuring CWMP with the autoinstall feature, see the *Example: Configuring and Enabling CWMP using the Autoinstall feature* section.

Before you begin

If the ACS URL is an HTTP URL, enable the Cisco IOS HTTP Server using the **ip http server**command. If the ACS URL is an HTTPS URL, enable the Cisco IOS HTTP Secure Server using the **ip http secure-server**

command. For more information about the **ip http server** and **ip http secure-server** commands, refer to the *Cisco IOS Network Management Command Reference*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cwmp agent**
4. **management server url** *acs-url*
5. **management server password** [*encryption-type* | *cleartext-password*] *passwd*
6. **provision code** *code-string*
7. **exit**
8. **interface** *type number*
9. **cwmp wan**
10. **cwmp wan default**
11. **exit**
12. **cwmp agent**
13. **enable download**
14. **session retry limit** *session-count*
15. **request outstanding** *request-count*
16. **parameter change notify interval** *time-interval*
17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**cwmp agent** **Example:** `Device(config)# cwmp agent`	Enables TR-069 Agent configuration mode.
Step 4	**management server url** *acs-url* **Example:** `Device(config-cwmp)# management server url http://172.25.117.78:7547/acs` **Example:**	Specifies the HTTP/HTTPS URL to reach the ACS. This URL is used by the CPE to establish the TR-069 session with the ACS.

	Command or Action	Purpose
	`Device(config-cwmp)# management server url https://172.25.117.78:7547/acs`	
Step 5	**management server password** [*encryption-type* | *cleartext-password*] *passwd* **Example:** `Device(config-cwmp)# management server password 0 cisco`	Specifies the CPE password that is used in the authentication phase. • This password will be provided to the ACS when the CPE is challenged for credential as part of authentication during the session establishment.
Step 6	**provision code** *code-string* **Example:** `Device(config-cwmp)# provision code ABCD`	Specifies the provision code to be used by the CPE.
Step 7	**exit** **Example:** `Device(config-cwmp)# exit`	Exits TR-069 Agent configuration mode and returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Device# interface serial 0/0`	Enters interface configuration mode.
Step 9	**cwmp wan** **Example:** `Device(config-if)# cwmp wan`	(Optional) Defines the WAN interfaces on the CPE. **Note** Any interface without this command is considered a LAN interface by TR-069 protocol. There can be multiple WAN and LAN interfaces configured on the CPE. By default, an ATM interface on the CPE will be considered a WAN interface by the TR-069 protocol.
Step 10	**cwmp wan default** **Example:** `Device(config-if)# cwmp wan default`	Defines the default WAN interfaces on the CPE device. **Note** Among the multiple WAN interfaces, there can be only one default WAN interface in which the TR-069 communication could happen. If you try to configure this command on multiple interfaces, only the latest configuration will be active and the previous default WAN interface will become a WAN interface, ensuring only one interface is the default at any point in time.
Step 11	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 12	**cwmp agent** **Example:** `Device(config)# cwmp agent`	Enables TR-069 Agent configuration mode.
Step 13	**enable download** **Example:** `Device(config-cwmp)# enable download`	(Optional) Enables the CPE to permit a software download. By default, this command is disabled.
Step 14	**session retry limit** *session-count* **Example:** `Device(config-cwmp)# session retry limit 10`	(Optional) Sets the session retry count whenever the TR-069 session establishment fails with the ACS. • The range for the session count argument is 0 to 15. • The default value is 11.
Step 15	**request outstanding** *request-count* **Example:** `Device(config-cwmp)# request outstanding 6`	(Optional) Sets the count for the number of requests that can be sent by CPE to ACS without receiving the acknowledgement. • The range for the request count argument is 0 to 10. • The default value is 5.
Step 16	**parameter change notify interval** *time-interval* **Example:** `Device(config-cwmp)# parameter change notify interval 75`	(Optional) Sets the time interval, in seconds, for the parameter change notifications. • The range for the time interval argument is 15 to 300. • The default value is 60.
Step 17	**end** **Example:** `Device(config-cwmp)# end`	Exits TR-069 Agent configuration mode and returns to privileged EXEC mode.

What to do next

Proceed to *Enabling the TR-069 Agent on the CPE* task.

Enabling the TR-069 Agent on the CPE

Before you begin

You must have set up the CPE as specified in the *Setting Up the CPE to Communicate with the ACS* task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cwmp agent**

4. **enable**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**cwmp agent** **Example:** `Device(config)# cwmp agent`	Enables TR-069 Agent configuration mode.
Step 4	**enable** **Example:** `Device(config-cwmp)# enable`	Enables the CPE to initiate a TR-069 session with the ACS.
Step 5	**end** **Example:** `Device(config-cwmp)# end`	Exits TR-069 Agent configuration mode and returns to privileged EXEC mode.

Initiating a TR-069 Agent Session from the ACS

Before you begin

You must have set up the CPE by using *Setting Up the CPE to Communicate with the ACS* task and enabled the TR-069 Agent on the CPE by using the *Enabling the TR-069 Agent on the CPE* task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cwmp agent**
4. **connection request username** *username*
5. **connection request username [** *encryption-type* | *cleartext-password*] *passwd*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**cwmp agent** **Example:** `Device(config)# cwmp agent`	Enables TR-069 Agent configuration mode.
Step 4	**connection request username** *username* **Example:** `Device(config-cwmp)# connection request username cisco`	Specifies the username used to authenticate an ACS which makes a connection request to a CPE.
Step 5	**connection request username [** *encryption-type* | *cleartext-password*] *passwd* **Example:** `Device(config-cwmp)# connection request password 0 cisco`	Specifies the password used to authenticate an ACS which makes a connection request to a CPE.
Step 6	**end** **Example:** `Device(config-cwmp)# end`	Exits TR-069 Agent configuration mode.

Configuring HTTP Digest Authentication Support

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http digest algorithm** *digest-algorithm*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip http digest algorithm** *digest-algorithm* **Example:** `Device(config)# ip http digest algorithm md5`	Configures the MD5 digest algorithm parameter. • The choices for the digest algorithm parameter are MD5 and MD5-sess. • MD5 is the default.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode.

Troubleshooting Tips

The following command can help troubleshoot the HTTP Digest Authentication Support:

- **show ip http client connection** --Displays all open client connections.

Clearing the HTTP Cookies

Perform this task to clear the HTTP cookies.

SUMMARY STEPS

1. **enable**
2. **clear ip http client cookie** [**domain** *cookie-domain* | **name** *cookie-name* | **session** *session-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ip http client cookie** [**domain** *cookie-domain*	**name** *cookie-name*	**session** *session-name*]	Clears the HTTP cookies.

	Command or Action	Purpose
	Example: `Device# clear ip http client cookie name test`	

Troubleshooting Tips

The following command can help troubleshoot the HTTP cookies:

- **show ip http client cookie** --Displays the HTTP cookies.

Monitoring and Troubleshooting the HTTP Cookies

SUMMARY STEPS

1. **enable**
2. **show ip http client cookie {brief | summary}** [**domain** *cookie-domain* | **name** *cookie-name* | **session** *session-name* **]**
3. **debug ip http cookie**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip http client cookie {brief | summary}** [**domain** *cookie-domain* | **name** *cookie-name* | **session** *session-name* **]** **Example:** `Device# show ip http client cookie brief name test`	Shows the HTTP cookies.
Step 3	**debug ip http cookie** **Example:** `Device# debug ip http cookie`	Troubleshoots the HTTP cookies.

Configuration Examples for TR-069 Agent

Example: Setting Up the CPE to Communicate with the ACS

The following example shows how to set up the CPE to communicate with the ACS. The ACS URL is http://172.25.117.78:7547/acs and the password is lab.

```
!
configure terminal
 cwmp agent
  management server url http://172.25.117.78:7547/acs
  management server password 0 lab
  provision code ABCD
  exit
 interface ethernet 0/0
  cwmp wan
  cwmp wan default
  exit
 cwmp agent
  enable download
  session retry limit 12
  request outstanding 3
  parameter change notify interval 120
!
```

Example: Configuring and Enabling CWMP using the Autoinstall feature

The following example shows how to configure CWMP using the autoinstall feature. Use the following set of commands in the network-config file or <hostname>-config file or router-config file in the TFTP server. No additional manual configuration is required for configuring CWMP on the device.

```
!
cwmp agent
 enable
 enable download
 management server password lab
 management server url http://10.1.98.229:7547/acs
 connection request username user1
 connection request password lab
!
ip http server
!
```

Additional References for TR-069 Agent

The following sections provide references related to the TR-069 Agent feature.

Related Documents

Related Topic	Document Title
TR-069 Agent commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Network Management Command Reference*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Standards

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

MIBs

MIB	MIBs Link
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
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for TR-069 Agent

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

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

Table 1: Feature Information for TR-069 Agent

Feature Name	Releases	Feature Information
TR-069 Agent		The TR-069 Agent feature manages a collection of CPEs, with the primary capability for auto-configuration and dynamic service provisioning, software image management, status and performance monitoring and diagnostics. The following commands were introduced or modified: **cwmp agent**, **cwmp wan**, **cwmp wan default**, **debug cwmp**, **enable**, **enable download**, **management server password**, **management server url**, **parameter change notify interval**, **provision code**, **request outstanding**, **session retry limit**, **show cwmp map**, **show cwmp methods**, **show cwmp parameter**, **show cwmp persistent**, **show cwmp session**.

Glossary

ACS--auto-configuration server.

CPE--customer premise equipment.