



Cisco Transport Manager Release 9.0

Basic External Authentication

May 5, 2009

This document describes the basic external authentication functionality in Cisco Transport Manager (CTM) Release 9.0.

Contents

This document contains the following topics:

- [Introduction, page 2](#)
- [Overview, page 2](#)
- [Understanding the Custom CTM SiteMinder Agent, page 4](#)
- [SiteMinder System Flow, page 6](#)
- [Understanding the Typical SiteMinder CTM Agent Init Call Sequence, page 7](#)
- [Understanding the RADIUS Implementation, page 8](#)
- [Installing RADIUS Authentication Tools, page 9](#)
- [RADIUS System Flow, page 9](#)
- [Configuring External Authentication Settings, page 11](#)
- [Caveats for Local Authentication When External Authentication Is Enabled, page 12](#)
- [Table of RADIUS Attributes, page 13](#)
- [Related Documentation, page 17](#)
- [Obtaining Documentation and Submitting a Service Request, page 17](#)



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

Introduction

CTM is an advanced management system that provides functionality at the element and network management levels for Cisco optical network elements (NEs) and switches. CTM supports fault, configuration, performance, and security management functional areas. CTM also serves as a foundation for integration into a larger overall Operations Support System (OSS) environment by providing northbound gateway interfaces to higher-layer management systems.

Overview

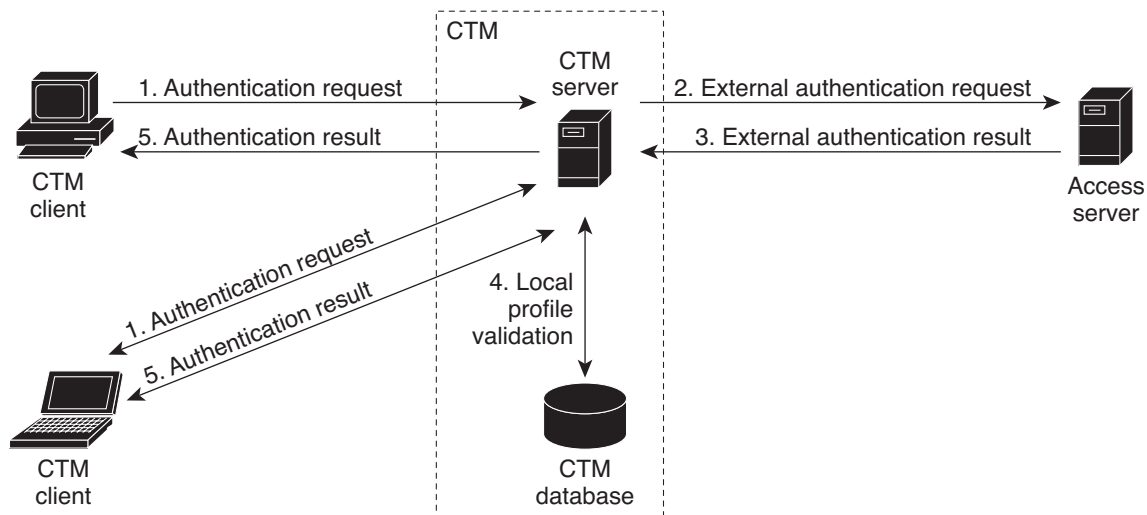
The basic external authentication feature enables CTM to authenticate users who log in through the SiteMinder policy server, a third-party application from Computer Associates International, Inc., and the RADIUS access server.

Basic external authentication involves the following key components:

- [SiteMinder Policy Server, page 2](#)
- [CTM Implementation of the SiteMinder Agent, page 3](#)
- [RADIUS Access Servers, page 3](#)
- [CTM Implementation of RADIUS, page 4](#)

The following figure illustrates the basic external authentication workflow.

Figure 1 Basic External Authentication Workflow



272687

SiteMinder Policy Server

The SiteMinder policy server:

- Provides an infrastructure for centralized and secure policy management that scales to meet the needs of large enterprise applications.
- Provides a way to uniquely identify and authenticate users and track and manage their privileges.

- Grants users access to only the applications to which they are authorized.
- Typically runs on a Windows or Solaris operating system and performs the following security operations:
 - Authentication—Supports a wide range of authentication methods, such as username and password, tokens, authentication forms, and public-key certificates.
 - Authorization—Enforces access control rules established by the policy server administrator. These rules define the operations that are allowed for each protected resource.
 - Administration—Enables you to configure the policy server using the policy server user interface. The administration service of the policy server allows the user interface to record configuration information in the policy store.

CTM Implementation of the SiteMinder Agent

The CTM agent implements the authentication process using the SiteMinder 4.x and 5.x authentication protocols. The CTM agent does not implement the Authorization and Administration processes using the SiteMinder protocols.

SiteMinder agents enable SiteMinder to manage access to applications and content according to predefined security policies.

In a SiteMinder environment, an *agent* is a network entity that acts as a filter to enforce network access control. An agent monitors requests for resources. If a user requests a protected resource, the agent prompts the user for credentials based on an authentication schema, and sends the credentials to the policy server.

The policy server determines whether to authenticate the user based on the credentials, and whether the user is authorized for the requested resource. The policy server then communicates with the CTM agent, which allows or denies access to the requested resource.

The SiteMinder suite includes the following services, which are not available for the CTM agent:

- Web agents
- Affiliate agents
- Enterprise Java bean (EJB) agents
- Servlet agents

All other agents (including the CTM agent) are considered custom agents that must be created using the agent application program interfaces (APIs). Once created, you can configure custom agents in the policy server user interface.

To connect to the policy server, the CTM server must implement the SiteMinder agent APIs and open a secure connection for all CTM user login requests.

RADIUS Access Servers

An access server is a centralized network server that stores user and credential information. Network devices such as routers, switches, NEs, and software applications request permission from the access server. If a user wants access to a network device, the network device sends an Access-Request to the access server. The access server replies with one of the following responses:

- Access-Accept—The user can log into the network device.
- Access-Reject—User access is denied.

- Access-Challenge—Additional information is requested from the user.

The RADIUS access server:

- Verifies user identity.
- Determines whether the user is allowed to perform a task or access a network device.
- Applies rules to user accounts.

CTM Implementation of RADIUS

The CTM server acts as a RADIUS client and sends authentication requests to a RADIUS server implementing a Single-Sign-On application.

The CTM server uses the Pluggable Authentication Module (PAM) Solaris library for authentication. Specifically, it uses the `pam_radius_auth` module to authenticate users against the RADIUS access server. The PAM framework consists of the following parts:

- PAM consumers—Solaris access applications such as `login` and `rlogin`, and the CTM server.
- PAM library.
- PAM configuration file (`pam.conf`).
- PAM service modules—Also referred to as *providers*.

Understanding the Custom CTM SiteMinder Agent

The CTM server application uses the SiteMinder agent API and is insulated from specific implementation details about users who are created and managed remotely. The agent API works with the policy server to simplify CTM secure application development while increasing application scalability in terms of the number of applications and resource-privilege pairs.

The agent API insulates the CTM application from underlying technology details, including:

- Username spaces such as Lightweight Directory Access Protocol (LDAP) directories
- Authentication methods, including simple username/password validation and complex public-key infrastructure (PKI) systems

The actual CTM agent API implementation tracks the authentication process with the policy server. The user credentials are stored in the policy store (the Solaris LDAP directory server), while the authorization process behaves as it did previously. The CTM database grants CTM authorization.

Configuring the SiteMinder Installation Library

To use the external authentication feature, the server system administrator must first configure the SiteMinder library.

Verify that the SuperUser has the correct file permissions for the following libraries; then, copy the libraries to the `/opt/CiscoTransportManagerServer/lib` path:

- `libsmagentapi.so`
- `libsmcommonutil.so`
- `libsmerrlog.so`

Configuring the SiteMinder Agent 4.x

To use the SiteMinder agent 4.x protocol, you must configure the external authentication settings in the Control Panel and then reboot the server. See [Configuring External Authentication Settings, page 11](#).

Configuring the SiteMinder Agent 5.x

To use the SiteMinder agent 5.x protocol, the SiteMinder administrator must create the SmHost.conf file and put it in the /opt/CiscoTransportManagerServer/cfg path using the following SiteMinder command:

```
smreghost -i <policy_server_IP_address> -u <policy_server_admin_username> -p
<policy_server_admin_password> -hc <host_configuration_object_name> -hn
<registered_hostname>
```



Note

Verify that the SuperUser has the correct file permissions. For details about the **smreghost** command, see the SiteMinder documentation.

Default CTM Policy Server Settings

The following table lists the default CTM configuration for the SiteMinder policy server.

Table 1 *Default External Authentication Settings*

Property	Value
External authentication	Disabled
Allow local fallback	Enabled
Enable SysAdmin	Enabled
Authorization port	44443
Authentication port	44442
Accounting port	44441
Agent name	SMCtmAgent
Shared secret (password)	CTMAgentSecret1!
Polling time (hours)	0 (disabled)
Failover	0
Number of servers	1
Server timeout	15 seconds
Minimum connections	1
Maximum connections	2
Connection steps	1
Resource	/CtmServerPrivate/index.html
Route	GET
Host configuration file	SmHost.conf

Compatibility

The external authentication feature supports the applications listed in the following table.

Table 2 *Application Compatibility*

Application	Version
SiteMinder policy server	Release 6.0 SP5
LDAP policy store	Sun directory server version 5.2

SiteMinder System Flow

Basic external authentication occurs as follows (see [Figure 1](#)):

1. The CTM installation installs one user, the SysAdmin. As a SysAdmin user, you configure external authentication settings in the CTM client Control Panel.
2. The CTM client forwards the authentication request to the CTM server.
3. The CTM server uses the SiteMinder API to authenticate the user on the SiteMinder server. If the authentication is valid, the SiteMinder server responds with true. The user type is retrieved from the database and the CTM server opens a login session with the CTM client. If the SiteMinder policy server is down but the SysAdmin user is enabled, the SysAdmin can connect to the server because the user profile is certified locally by the server. You can change the configuration by choosing the CTM server authentication process for recovery.

CTM Agent Behavior

The CTM agent initiates the following sequence of events:

1. Initialization and connection.

Before an instance of the SiteMinder agent can perform work on behalf of the CTM server, it initializes connections to one or more policy servers (4.x or 5.x agents). The administrator specifies connection parameters such as server IP address and connection ports. This step, which is generally performed only once, creates TCP connections. After the agent API initializes, all API calls are thread-safe with respect to the initialized API instance.

2. Version setting.

Immediately after initialization, the CTM agent communicates its version information to the policy server with an API command. The actual information is read from the Control Panel and reports the SiteMinder agent version numbers. The agent version is recorded in the policy server logs. When the CTM agent API initializes, the agent begins work. The CTM server begins accepting user requests, such as GET requests from Java client sessions.

The outcome of most steps can be cached to improve CTM performance. CTM can choose to cache as few or as many instances as possible. A specific instance is cached for each user connection.

3. User login request.

User logins are application-specific requests. For example, the agent accepts a user's request and issues a SiteMinder API call to determine whether the requested resource (/CtmServerPrivate/index.html) is protected. That is, the CTM agent asks the policy server if the CTM server is available for that user profile. If the resource is protected, the policy server returns

the required user credentials that must be obtained to validate the user's identity. If the resource is incorrect or unprotected, access to the requested resource is denied. The resulting output can be cached.

4. Collection of required credentials.

CTM issues a SiteMinder API login call to collect the required user credentials and authenticate the user. Upon successful authentication, the policy server creates a session and returns response attributes, including the unique session ID and the session specification. The session specification is a type of ticket that uniquely identifies the session. These policy-driven response attributes include user profile data, static or dynamic privileges, predefined authentication state attributes, and other data designated by the policy administrator. The actual implementation does not use the response attributes, because the user profile is retrieved from the CTM database.

The CTM agent caches the user session information. The CTM server configures the custom agent for version 4.x to have only one connection to the policy server. The timeout value is 15 seconds. For agent version 5.x, the configuration is set up by the SiteMinder administrator, and CTM loads all information from the SmHost.conf file.

5. CTM agent initialization.

The CTM SiteMinder agent is loaded when the application boots up. For agent version 4.x, all parameters are loaded from the database to configure a reliable connection to the policy server. For agent version 5.x, all parameters are loaded from the SmHost.conf file. The external authentication flag is loaded so that the server loads the library dynamically. This technical solution is driven by the necessity of deploying the CTM installation without the SiteMinder library, which is subject to royalties. Not all parameters require a server reboot; changes to the Enable SysAdmin and Allow Local Fallback settings take effect immediately.

Understanding the Typical SiteMinder CTM Agent Init Call Sequence

The CTM agent uses two sequences for the init call sequence, one for each agent version (4.x or 5.x).

All agent version 4.x configuration parameters are stored in the CTM database and read when the CTM server boots up. If agent version 5.x is selected, the CTM custom agent uses the server IP address and the API call to retrieve the agent configuration from the SmHost.conf file configured by the SiteMinder administrator. If the call is correct, CTM memorizes the agent API reference in a global variable so that all authentication modules can easily reference it. After the connection is up and running, CTM clients begin placing authorization requests.

CTM Session Services

The SiteMinder environment maintains consistent user sessions across multitiered applications. The CTM custom agent (not the policy server) maintains a per-user session specification, also called a *session ticket*. The CTM agent uses the session services of the agent API to create, delegate, validate, and terminate user sessions.

The following agent API methods implement session services:

- Login()
- Logout()

A session is created after a successful user login. Once created, a user session persists until it is terminated.

User-side session persistence is accomplished by saving the session specification that the policy server issues at the time of authentication. The session specification represents a user session and is the key to SiteMinder session management. The CTM server environment in which the user session was created is responsible for persistent storage of the session specification.

SiteMinder's universal ID integrates seamlessly with the sessioning mechanism. A universal ID identifies the user to an application in a SiteMinder environment using a unique identifier, such as a Social Security number or customer account number. The universal ID facilitates identification of users between old and new applications by delivering the user's identification automatically, regardless of the application. Once configured on the policy server, a user's universal ID is part of the session specification and is made available to agents for the duration of the entire session.

The CTM agent uses the Login() API to create sessions. This API authenticates the CTM user credentials and returns the session specification and unique session ID. Once created, the session specification is updated on subsequent agent API calls.

CTM agents use the API information to manage custom sessions and track timeouts. By default, a session times out after 15 seconds. That is, if the policy server does not trust the user within 15 seconds, the login process fails.

When the CTM server receives an authentication message from the client, the server processes the message and invokes the API login, using the global connection reference and the username and password provided by the user.

At the end of this process, SiteMinder returns a response for the user session, which either trusts or denies the user. This response must be stored at the server level to invoke all subsequent requests for the correct user instance. The CTM agent calls the Login() API to validate the session specification and verify that the session was not terminated or revoked. This validation can occur at any time during the session lifecycle. The CTM agent does not check for session expiration because CTM implements an authentication-only feature and provides a different expiration mechanism.

CTM User Logout

A CTM user session is terminated:

- After a user logs out and the agent discards the session specification
- When the session expires
- When the session is revoked

After a session is terminated, the user must log in again to establish a new session.

CTM terminates a session if a user is disabled after the session begins. CTM calls the SiteMinder Login() API to validate the session and determine whether the user is enabled. To terminate a session, the agent must discard the session specification.

When the CTM server shuts down, the connection opened with the SiteMinder policy server stops, and the policy server is informed with an API method.

Understanding the RADIUS Implementation

The CTM server operates as a RADIUS client that is responsible for passing user information to designated RADIUS servers, and then acting on the response that is returned.

CTM provides an installation script that installs the following files:

- `Pam_radius_auth.so`—A shared library file that is provided by FreeRADIUS. It is a PAM service module that encapsulates all of the RADIUS client code installed in the `usr/lib/security` directory. The `pam_radius_auth.so` file is considered a third-party component.
- `Pam_radius_auth.conf`—A configuration file installed in the `/opt/CiscoTransportManagerServer/cfg` directory. Configuration information includes the IP address of the RADIUS server, the authentication port, the shared secret, the request timeout, and the number of retries.



Note The shared secret should be a strong password that contains at least 16 characters.

The installation script also changes the `/etc/pam.conf` file to configure the PAM library to use the `pam_radius_auth.so` service module for authentication.

Installing RADIUS Authentication Tools

Step 1 Mount the CTM Server Disk 1 installation CD.

Step 2 Enter the following command:

```
cd /cdrom/ExtAuth/bin
```

Step 3 Launch the `./pam_radius_auth_install` interactive script to install and configure the RADIUS client for CTM.



Note This step also copies the RADIUS files locally to `/opt/ExtAuth`, so that you can proceed without using a CD.

Step 4 Follow the interactive script to install and add the RADIUS server configuration. The interactive script allows you to:

- Install the PAM service module and RADIUS configurations.
 - Add configuration information for other RADIUS servers at any time.
 - Delete or modify configuration information.
 - Change the order of the RADIUS servers, because the position of a RADIUS server determines the order that CTM's RADIUS client follows when requesting authentication when more than one RADIUS server is present.
 - Uninstall the PAM service module and RADIUS configurations.
-

RADIUS System Flow

Users must be configured on both the CTM local authentication database and the remote access server. Usernames must be the same, but passwords can differ.

The following describes the system flow:

1. The CTM installation installs one user, the SysAdmin. As a SysAdmin user, you configure external authentication settings in the CTM client Control Panel.
2. The CTM client forwards the authentication request to the CTM server.
3. The CTM server's RADIUS client sends an Access-Request message to the RADIUS access server. The access server replies with an Access-Accept RADIUS message if the user credentials are accepted, with an Access-Reject if the user credentials are rejected, or with an Access-Challenge. For an Access-Challenge, the access server sends a human-readable request to the user; the CTM client prompts the user with the request, collects the user response, and sends the response back to the CTM server. The CTM server sends a new Access-Request with the user's response to the access server. This process continues cyclically until the access server sends an Access-Accept or Access-Reject RADIUS message. For details, see <http://www.ietf.org/rfc/rfc2865.txt>.

The following table describes the RADIUS attributes that CTM server's RADIUS client sends in Access-Request messages.

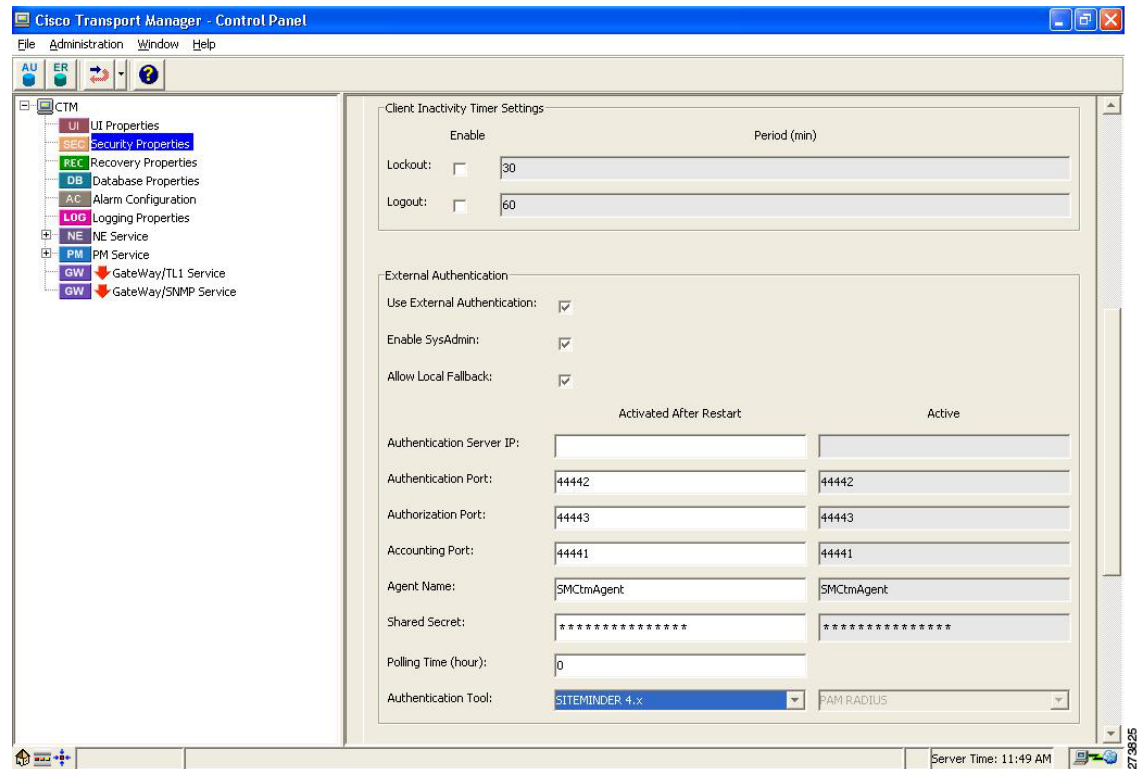
Table 3 *Attributes That the CTM Server's RADIUS Client Sends in Access-Request Messages*

RADIUS Attribute	Description
User-Name <i>value</i>	CTM user's name
User-Password <i>value</i>	Encrypted user's password
NAS-IP-Address <i>value</i>	CTM host's IPv4 address
NAS-Identifier <i>value</i>	ctms
NAS-Port-Type <i>value</i>	5 (virtual) Note This attribute instructs the server to indicate that the user is not on a physical port.
NAS-Port <i>value</i>	Process ID of the RADIUS client
Service-Type <i>value</i>	8 (authenticate only) Note This attribute is present in the first Access-Request message, but is missing from the RADIUS server's Access-Challenge replies. For this reason, the RADIUS server administrator must not configure the RADIUS server to check for the existence of this attribute in every Access-Request message.

Configuring External Authentication Settings

The following figure shows the External Authentication fields in the Control Panel. Complete the following steps to configure external authentication settings, which are stored in the CTM database.

Figure 2 External Authentication Fields



Step 1 In the Domain Explorer window, choose **Administration > Control Panel**.

Step 2 Click **Security Properties**.

Step 3 In the External Authentication area, configure the following settings:

- Use External Authentication—If checked, all authentication options are enabled, and the external authentication feature is active.
- Enable SysAdmin—If checked, the SysAdmin user can always log into CTM, even if the Allow Local Fallback check box is unchecked and the policy server is down.
- Allow Local Fallback—If checked, the CTM client users can still log into the CTM server even if the policy server is unreachable. The SysAdmin user should enable the Allow Local Fallback setting in case the policy server is unavailable.
- Authentication Server IP—(Applicable only to SiteMinder 4.x) Specify the IP address of the policy server. IPv6 addresses are not supported.
- Authentication Port—(Applicable only to SiteMinder 4.x) Specify the policy server port for authentication (for example, 44442).

- Authorization Port—*(Applicable only to SiteMinder 4.x)* Specify the policy server port for authorization (for example, 44441).
- Accounting Port—*(Applicable only to SiteMinder 4.x)* Specify the policy server port for accounting (for example, 44443).
- Agent Name—*(Applicable only to SiteMinder 4.x)* Enter the name that the policy server uses to identify the custom CTM agent.
- Shared Secret—*(Applicable only to SiteMinder 4.x)* Enter the parameter that the CTM policy server uses to create a unique ID.
- Polling Time—*(Applicable only to SiteMinder 4.x and 5.x)* Enter the polling frequency (in hours) for the policy server to update the parameters. The default value is 0, meaning that polling is disabled.
- Authentication Tool—Specify the third-party tool used for authentication. Valid values are SiteMinder 4.x, SiteMinder5.x, and PAM RADIUS.



Note The Active column lists the current configuration settings on the CTM server. The Activated After Restart column lists the new configuration settings that take effect after the CTM server reboots.

Changes to the Enable SysAdmin and Allow Local Fallback settings are applied immediately. Changes to the other settings take effect after the CTM server reboots.

Step 4 Click **Save**.

Step 5 The SiteMinder policy server administrator must complete the following additional substeps:

- a. The configuration server side is the same as a web agent. Add the following string as a protected resource:

```
/CtmServerPrivate/index.html
```

- b. Set **GET** as an action.
- c. Choose **Basic** as the policy server configuration credential.
- d. Use the SiteMinder Test tool to trust the CTM parameters.

Step 6 To enable external authentication, you must restart the CTM server. Enter the following command:

```
ctms-stop ; ctms-start
```

Caveats for Local Authentication When External Authentication Is Enabled

When external authentication is enabled, the local authentication system is subject to the following caveats:

- Because user credentials (passwords) are not checked against passwords in the local database, the following CTM authentication features might not work in all cases:
 - User lockout

- Autologin

The preceding features do not work when a user is logged in and the access server or the access server administrator changes that user's credentials. For example, the RADIUS RSA authentication manager can authenticate users by means of hardware devices (tokens) that generate a pseudorandom number that is used as a password. This number changes every minute, so a locked out user does not know which password was used to log in successfully in the past. To prevent this problem, open the CTM client and in the Domain Explorer, choose **Administration > Control Panel > Security Properties** and uncheck the **Lockout Enable** check box.

- If the CTM client disconnects from the CTM server, the client automatically tries to log in again using the cached username and password, which are no longer valid. The automatic login attempts fail. To resolve this problem, close the automatic login wizard and launch the CTM client again.
- Password aging rules and login preferences do not work, because they are demanded of the external access server. For this reason, these rules must remain disabled on the CTM client. When external authentication is enabled, the following fields in the **Control Panel > Security Properties > CTM Security** tab are automatically set to 0 (disabled):
 - Password Aging
 - Password Expiration Early Notification
 - Max Retries
 - Login Disable Period
- The password change feature changes the local password. For this reason, do not use the password change feature when external authentication is enabled. Furthermore, password changing policies are access server dependent. In the Domain Explorer, choose **Administration > CTM Users**. In the CTM Users table, choose **Edit > Create**. In the Create New User wizard, uncheck the **Require Password Change on Next Login** check box.
- Although authentication is external, authorization is local. For example, user privileges are managed locally.

Table of RADIUS Attributes

The following table lists the RADIUS attributes that CTM R9.0 supports. The table uses the following values:

- Request/Accept/Reject/Challenge:
 - 0—The attribute **MUST NOT** be present in the packet.
 - 0+—Zero or more instances of the attribute **MAY** be present in the packet.
 - 0-1—Zero or one instance of the attribute **MAY** be present in the packet.
 - 1—Exactly one instance of the attribute **MUST** be present in the packet.
- No.—Number of the RADIUS attribute as specified in the referenced RFC.
- Attribute—Name of the RADIUS attribute.
- Details—Details about the attribute: how it is used, delivered, or interpreted by the RADIUS client on the CTM server.
- RFC—Number of the referenced RFC.
- RFC Req. Type—Whether a “requirement statement” is present in the referenced RFC.

- MUST, MUST NOT, SHOULD, MAY, and so on—Requirement types as specified in RFC 2119. These words indicate that a requirement statement is present in the RFC. Note that the “MAY” requirements are optional requirements.
- Unspecified—The attribute has no associated requirement statement. The RFC contains only a description of the attribute.
- Supported—Indicates CTM support for the attribute:
 - Yes—Supported
 - No—Not supported
 - N/A—Not applicable
 - Partial—Partially supported

Table 4 RADIUS Attributes

Request	Accept	Reject	Challenge	No.	Attribute	Details	RFC	RFC Req. Type	Supported?
0-1	0-1	0	0	1	User-Name	The value is the username of the authenticating CTM user.	2865	MUST	Yes
0-1	0	0	0	2	User-Password	—	2865	MUST	Yes
0-1	0	0	0	3	CHAP-Password	Does not include the PPP protocol to connect users with the RADIUS client.	2865	MUST	N/A
0-1	0	0	0	4	NAS-IP-Address	The value is the IP version 4 address of the host where the CTM server is running.	2865	MUST	Yes
0-1	0	0	0	5	NAS-Port	The value is the CTM server process ID, which changes every time the CTM server is restarted.	2865	MAY	Yes
0-1	0-1	0	0	6	Service-Type	The value is 8 (authenticate only). This attribute is present in the first Access-Request message, but is missing from the RADIUS server’s Access-Challenge replies. For this reason, the RADIUS server administrator must not configure the RADIUS server to check for the existence of this attribute in every Access-Request message. RSA Authentication Manager 7.1 uses Challenge/Response.	2865	MAY	Partial
0-1	0-1	0	0	7	Framed-Protocol	—	2865	MAY	N/A

Table 4 RADIUS Attributes (continued)

Request	Accept	Reject	Challenge	No.	Attribute	Details	RFC	RFC Req. Type	Supported?
0-1	0-1	0	0	8	Framed-IP-Address	—	2865	MAY	N/A
0-1	0-1	0	0	9	Framed-IP-Netmask	—	2865	MAY	N/A
0	0-1	0	0	10	Framed-Routing	—	2865	Unspecified	N/A
0	0+	0	0	11	Filter-Id	Not applicable because users are not routers.	2865	MUST NOT	N/A
0-1	0-1	0	0	12	Framed-MTU	—	2865	MAY	N/A
0+	0+	0	0	13	Framed-Compression	—	2865	MAY	N/A
0+	0+	0	0	14	Login-IP-Host	—	2865	MAY	N/A
0	0-1	0	0	15	Login-Service	—	2865	Unspecified	N/A
0	0-1	0	0	16	Login-TCP-Port	—	2865	Unspecified	N/A
0	0+	0+	0+	18	Reply-Message	<p>This attribute is used during the Challenge/Response handshake only. The value is a human-readable string and is contained in the Access-Challenge messages received from the RADIUS server. The CTM client displays the string to the user. This attribute is partially supported because it is not displayed in Access-Accept or Access-Reject messages received from the RADIUS server.</p> <p>The RADIUS server administrator must not configure the RADIUS server to deliver this attribute in Access-Accept or Access-Reject messages.</p>	2865	MAY	Partial
0-1	0-1	0	0	19	Callback-Number	—	2865	MAY	N/A
0	0-1	0	0	20	Callback-Id	—	2865	MAY	N/A
0	0+	0	0	22	Framed-Route	Not applicable because users are not routers.	2865	MUST NOT/ SHOULD	N/A
0	0-1	0	0	23	Framed-IPX-Network	—	2865	Unspecified	N/A

Table 4 RADIUS Attributes (continued)

Request	Accept	Reject	Challenge	No.	Attribute	Details	RFC	RFC Req. Type	Supported?
0-1	0-1	0	0-1	24	State	This attribute is received from the RADIUS server during Challenge/Response handshakes and is retransmitted unchanged to the RADIUS server.	2865	MUST	Yes
0	0+	0	0	25	Class	Not applicable because RADIUS accounting is not supported (RFC 2866).	2865	SHOULD/MUST NOT	N/A
0+	0+	0	0+	26	Vendor-Specific	No specific attributes for CTM.	2865	MAY	No
0	0-1	0	0-1	27	Session-Timeout	—	2865	Unspecified	N/A
0	0-1	0	0-1	28	Idle-Timeout	—	2865	Unspecified	N/A
0	0-1	0	0	29	Termination-Action	—	2865	MAY	N/A
0-1	0	0	0	30	Called-Station-Id	—	2865	Unspecified	N/A
0-1	0	0	0	31	Calling-Station-Id	No dialing service is provided.	2865	SHOULD	N/A
0-1	0	0	0	32	NAS-Identifier	The value is ctms.	2865	MUST	Yes
0+	0+	0+	0+	33	Proxy-State	Not applicable because Proxy-State is a RADIUS server attribute only.	2865	MUST	N/A
0-1	0-1	0	0	34	Login-LAT-Service	—	2865	MAY	N/A
0-1	0-1	0	0	35	Login-LAT-Node	—	2865	MAY	N/A
0-1	0-1	0	0	36	Login-LAT-Group	—	2865	MAY	N/A
0	0-1	0	0	37	Framed-AppleTalk-Link	—	2865	Unspecified	N/A
0	0+	0	0	38	Framed-AppleTalk-Network	—	2865	Unspecified	N/A
0	0-1	0	0	39	Framed-AppleTalk-Zone	Not applicable because the serial AppleTalk protocol is not present.	2865	SHOULD	N/A
0-1	0	0	0	60	CHAP-Challenge	—	2865	MAY	N/A
0-1	0	0	0	61	NAS-Port-Type	The value is 5 (virtual). This attribute instructs the server to indicate that the user is not on a physical port.	2865	MAY	Yes
0-1	0-1	0	0	62	Port-Limit	—	2865	MAY	N/A
0-1	0-1	0	0	63	Login-LAT-Port	—	2865	MAY	N/A
0	0	0	0-1	76	Prompt	The echo is considered to be always off.	2869	MAY	No

Related Documentation


Note

You can access the most current CTM R9.0 documentation online at http://www.cisco.com/en/US/products/sw/opticsw/ps2204/tsd_products_support_series_home.html.

The CTM documentation set comprises the following guides:

- *Release Notes for Cisco Transport Manager Release 9.0*—Describes the caveats for CTM.
- *Cisco Transport Manager Release 9.0 Installation Guide*—Explains how to install CTM and how to upgrade from previous releases.
- *Cisco Transport Manager Release 9.0 User Guide*—Describes how to use the CTM software, which consists of user applications and tools for network discovery, network configuration, connection management, fault management, system administration, and security management.
- *Cisco Transport Manager Release 9.0 GateWay/CORBA User Guide and Programmer Manual*—Describes the CTM GateWay/CORBA northbound interface product that is available for CTM. This document serves as a reference for developers of OSS applications that work with the CTM GateWay/CORBA interface.
- *Cisco Transport Manager Release 9.0 Database Schema*—Describes the database schema that CTM uses to store information in a Structured Query Language (SQL) database such as the Oracle database. The document is designed for users who need to create their own reports without using CTM.
- *Cisco Transport Manager Release 9.0 High Availability Installation Guide*—Explains how to install CTM in a high availability (HA) environment.


Note

The *Cisco Transport Manager Release 9.0 High Availability Installation Guide* is not available online. Contact your Cisco account representative to obtain this guide.

- *Cisco Transport Manager Release 9.0 ML Provisioning Methodology*—Describes the methodology that CTM uses to provision ML-series cards.
- *Cisco Transport Manager Release 9.0 Basic External Authentication*—This document.
- *Migration Matrix for Cisco Transport Manager Service Pack Releases*—Describes the migration matrix for CTM service pack releases.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, 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, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, 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. (0903R)

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.

© 2008–2009 Cisco Systems, Inc. All rights reserved.