



Cisco Transport Manager Release 8.5 Basic External Authentication

February 5, 2008

This document describes the basic external authentication functionality in Cisco Transport Manager (CTM) Release 8.5.

Contents

This document contains the following topics:

- [Introduction, page 1](#)
- [Overview, page 2](#)
- [Understanding the Custom CTM SiteMinder Agent, page 3](#)
- [System Flow, page 5](#)
- [Understanding the Typical CTM Agent Init Call Sequence, page 6](#)
- [Configuring External Authentication Settings, page 8](#)
- [Related Documentation, page 9](#)
- [Obtaining Documentation and Submitting a Service Request, page 10](#)

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.



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

© 2008 Cisco Systems, Inc. All rights reserved.

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.

Basic external authentication involves the following key components:

- [SiteMinder Policy Server, page 2](#)
- [CTM Implementation of the SiteMinder Agent, page 2](#)

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—The policy server can be configured 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.

The CTM agent implements the authentication process using the SiteMinder 4.x and 5.x authentication protocol.

CTM Implementation of the SiteMinder Agent

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:

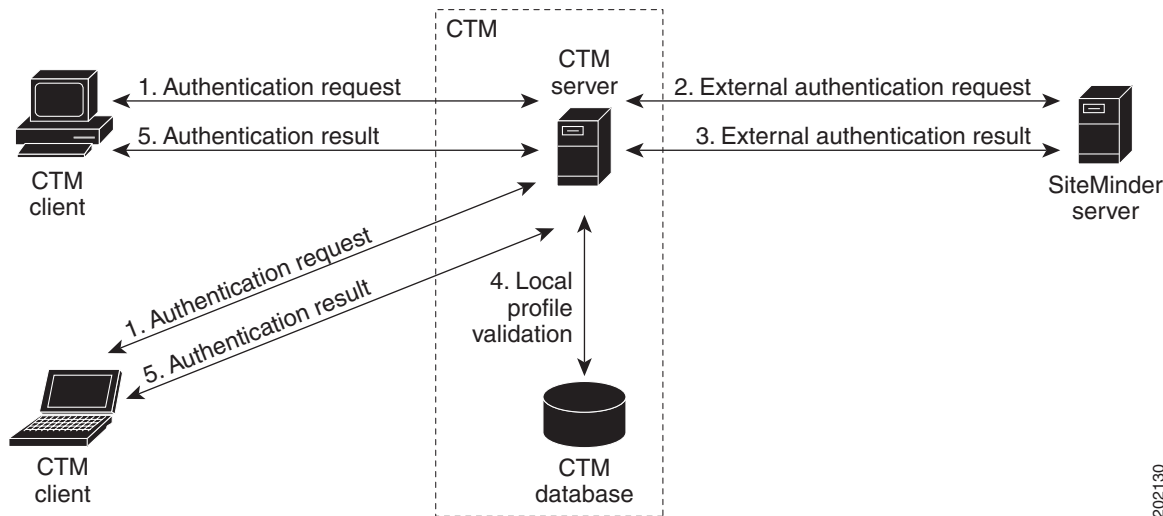
- Web agents
- Affiliate agents
- Enterprise Java bean (EJB) agents

- 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. The following figure illustrates the basic external authentication workflow.

Figure 1 Basic External Authentication Workflow



202130

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 8](#).

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

Table 1 *Default External Authentication Settings (continued)*

Property	Value
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

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 (4.x or 5.x agent) or more policy servers. 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 requests from the policy server whether 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 outcome of this step 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 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 function 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 this 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 terminates, the user must log in again to establish a new session.

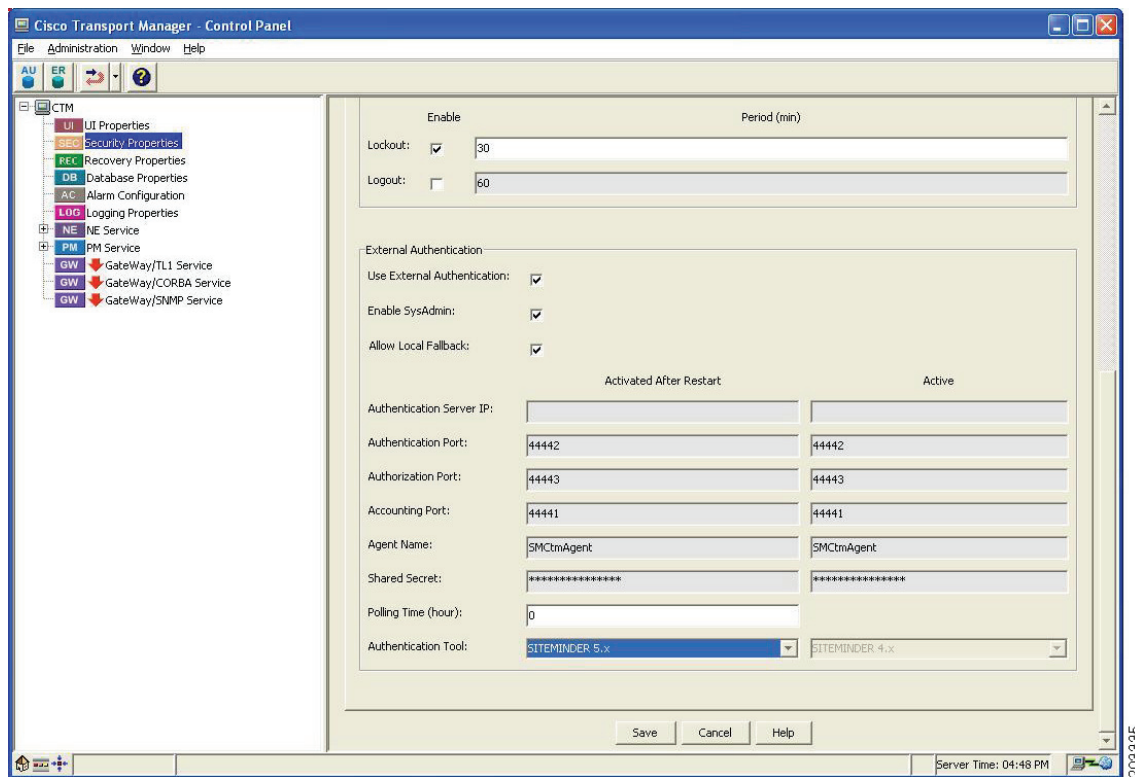
CTM terminates a session if a user is disabled after the session begins. CTM calls the SiteMinder Login() API to validate the session and determine whether the user is enabled. To terminate a session, the agent must discard the session specification.

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.

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**—Specify the IP address of the policy server.
- **Authentication Port**—Specify the policy server port for authentication (for example, 44442).
- **Authorization Port**—Specify the policy server port for authorization (for example, 44441).
- **Accounting Port**—Specify the policy server port for accounting (for example, 44443).
- **Agent Name**—Enter the name that the policy server uses to identify the custom CTM agent.
- **Shared Secret**—Enter the parameter that the CTM policy server uses to create a unique ID.
- **Polling Time**—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.



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.

Related Documentation



Note

You can access the most current CTM R8.5 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 8.5](#)—Describes the caveats for CTM.
- [Cisco Transport Manager Release 8.5 Installation Guide](#)—Explains how to install CTM and how to upgrade from previous releases.

- *Cisco Transport Manager Release 8.5 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 8.5 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 8.5 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 8.5 High Availability Installation Guide*—Explains how to install CTM in a high availability (HA) environment.



Note The *Cisco Transport Manager Release 8.5 High Availability Installation Guide* is not available online. Contact your Cisco account representative to obtain this guide.

- *Cisco Transport Manager Release 8.5 ML Provisioning Methodology*—Describes the methodology that CTM uses to provision ML-series cards.
- *Cisco Transport Manager Release 8.5 Basic External Authentication*—This document.

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, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, 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, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, 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. (0801R)

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.

© 2007–2008 Cisco Systems, Inc. All rights reserved.