Cisco Prime Optical 9.3 Basic External Authentication

June 6, 2012

This document describes the basic external authentication functionality in Cisco Prime Optical 9.3 running on a Solaris server.

Note External authentication is not supported in Cisco Prime Optical running on a Linux server.

Contents

This document contains the following topics:

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

Introduction

Cisco Prime Optical (formerly Cisco Transport Manager) is a carrier-class, multitechnology management system that integrates the end-to-end management of traditional transport networks and new carrier packet transport networks. It can help maintain the integrity of existing services, plus deliver interactive, content-based services and high-bandwidth applications.

Cisco Prime Optical manages the entire Cisco optical portfolio, including:

- Metro core
- Metro dense wavelength-division multiplexing (DWDM)
- Metro edge and access products
- New Carrier Packet Transport (CPT) System products

Prime Optical 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

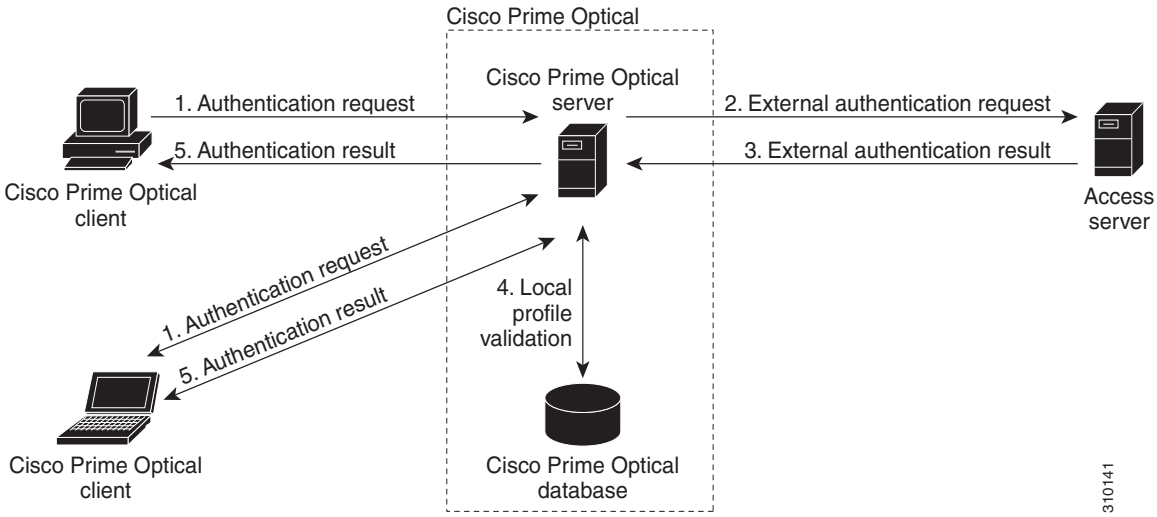
The basic external authentication feature enables Prime Optical to authenticate users who log in through the RADIUS access server.

Basic external authentication involves the following key components:

- RADIUS Access Servers, page 3
- Prime Optical Implementation of RADIUS, page 4

The following figure illustrates the basic external authentication workflow.

Figure 1 Basic External Authentication Workflow



RADIUS Access Servers

An access server is a centralized network server that stores user and credential information. Network devices such as routers, 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.

Prime Optical Implementation of RADIUS

The Prime Optical server acts as a RADIUS client and sends authentication requests to a RADIUS server implementing a single sign-on (SSO) application.

The Prime Optical 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 Prime Optical server.
- PAM library.
- PAM configuration file (pam.conf).
- PAM service modules—Also referred to as *providers*.

Default Prime Optical Policy Server Settings

The following table lists the default Prime Optical configuration for the RADIUS access server.

Table 1 Default External Authentication Settings

Property	Value
External authentication	Disabled
Allow local fallback	Enabled
Enable SysAdmin	Enabled

Understanding the RADIUS Implementation

The Prime Optical 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.

Prime Optical 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 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/ExtAuth/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

Note External authentication is not supported in Cisco Prime Optical running on a Linux server.

Step 1 Mount the Prime Optical Server Disk 1 installation DVD.

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 Prime Optical.

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

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 Prime Optical'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 Prime Optical 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 Prime Optical installation installs one user, the SysAdmin. As a SysAdmin user, you configure external authentication settings in the Prime Optical client Control Panel.
2. The Prime Optical client forwards the authentication request to the Prime Optical server.

3. The Prime Optical 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 Prime Optical client prompts the user with the request, collects the user response, and sends the response back to the Prime Optical server. The Prime Optical 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 Prime Optical server's RADIUS client sends in Access-Request messages.

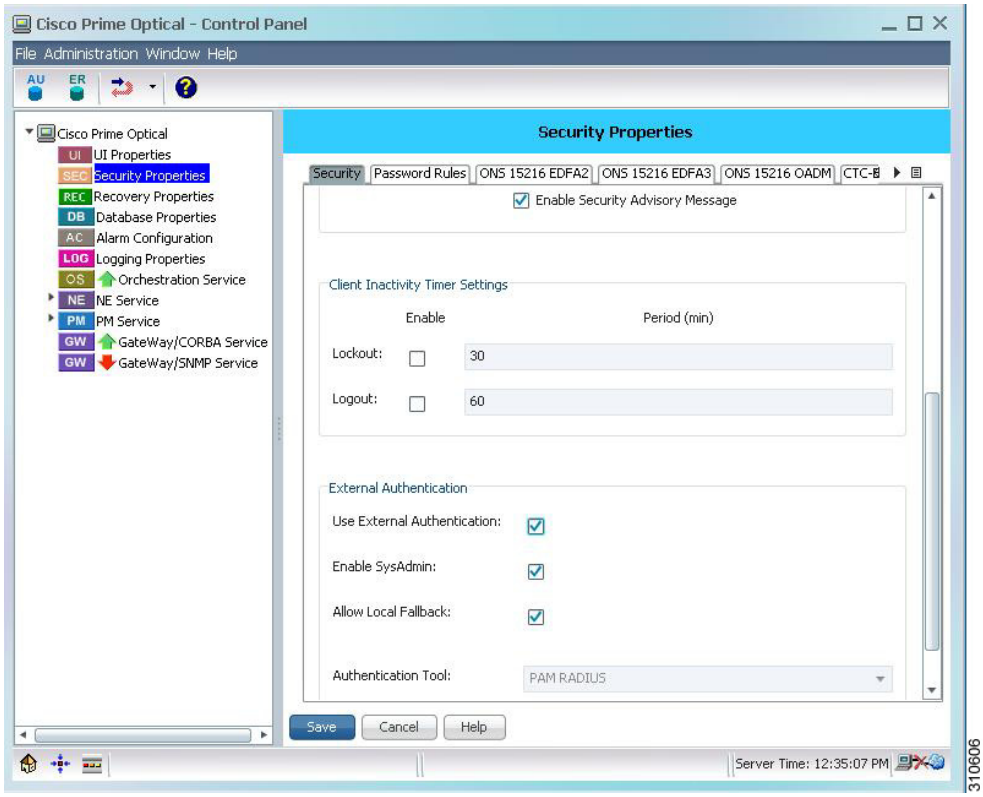
Table 2 Attributes That the Prime Optical Server's RADIUS Client Sends in Access-Request Messages

RADIUS Attribute	Description
User-Name *value*	Prime Optical user's name
User-Password *value*	Encrypted user's password
NAS-IP-Address *value*	Prime Optical host's IPv4 address
NAS-Identifier *value*	ctms
NAS-Port-Type *value*	5 (virtual) **Note** This attribute instructs the server to indicate that the user is not on a physical port.
NAS-Port *value*	Process ID of the RADIUS client
Service-Type *value*	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 Prime Optical 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 Prime Optical, even if the Allow Local Fallback check box is unchecked and the policy server is down.
- Allow Local Fallback—If checked, the Prime Optical client users can still log into the Prime Optical 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 Tool—*Display only.* Indicates that PAM RADIUS is the third-party tool used for authentication.

Step 4 Click **Save**.

Step 5 To enable external authentication, you must restart the Prime Optical 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 Prime Optical 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 Prime Optical client and in the Domain Explorer, choose **Administration > Control Panel > Security Properties** and uncheck the **Lockout Enable** check box.
- If the Prime Optical client disconnects from the Prime Optical 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 Prime Optical 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 Prime Optical client. When external authentication is enabled, the following fields in the **Control Panel > Security Properties > 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 > Users**. In the Cisco Prime Optical 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 Prime Optical 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 Prime Optical 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 Prime Optical support for the attribute:
  - Yes—Supported
  - No—Not supported
  - N/A—Not applicable
  - Partial—Partially supported

Table 3 RADIUS Attributes

Request	Accept	Reject	Challenge	No.	Attribute	Details	RFC	RFC Req. Type	Sup-ported?
0-1	0-1	0	0	1	User-Name	The value is the username of the authenticating Prime Optical 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 IPv4 address of the host where the Prime Optical server is running.	2865	MUST	Yes

Table 3 RADIUS Attributes (continued)

Request	Accept	Reject	Challenge	No.	Attribute	Details	RFC	RFC Req. Type	Sup-ported?
0-1	0	0	0	5	NAS-Port	The value is the Prime Optical server process ID, which changes every time the Prime Optical 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
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

Table 3 RADIUS Attributes (continued)

Request	Accept	Reject	Challenge	No.	Attribute	Details	RFC	RFC Req. Type	Sup-ported?
0	0+	0+	0+	18	Reply-Message	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 Prime Optical 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. The RADIUS server administrator must not configure the RADIUS server to deliver this attribute in Access-Accept or Access-Reject messages.	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
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 Prime Optical.	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

Table 3 RADIUS Attributes (continued)

Request	Accept	Reject	Challenge	No.	Attribute	Details	RFC	RFC Req. Type	Sup-ported?
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 Prime Optical documentation online at http://www.cisco.com/en/US/products/ps11670/tsd_products_support_series_home.html.

The Prime Optical documentation set comprises the following guides:

- *Release Notes for Cisco Prime Optical 9.3*—Describes the caveats for Prime Optical.
- *Cisco Prime Optical 9.3 Installation Guide*—Explains how to install Prime Optical and how to upgrade from previous releases.
- *Cisco Prime Optical 9.3 User Guide*—Describes how to use the Prime Optical software, which consists of user applications and tools for network discovery, network configuration, connection management, fault management, system administration, and security management.

- *Cisco Prime Optical 9.3 GateWay/CORBA User Guide and Programmer Manual*—Describes the GateWay/CORBA northbound interface product that is available for Prime Optical. This document serves as a reference for developers of OSS applications that work with the GateWay/CORBA interface.
- *Cisco Prime Optical 9.3 Database Schema*—Describes the database schema that Prime Optical 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 Prime Optical.
- *Cisco Prime Optical 9.3 High Availability Installation Guide*—Explains how to install Prime Optical in a high availability (HA) environment.

Note To obtain the *Cisco Prime Optical 9.3 High Availability Installation Guide*, contact your Cisco account representative.

- *Cisco Prime Optical 9.3 ML Provisioning Methodology*—Describes the methodology that Prime Optical uses to provision ML-series cards.
- *Cisco Prime Optical 9.3 Basic External Authentication*—This document.
- *Migration Matrix for Service Pack Releases*—Describes the migration matrix for 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.