Cisco Prime Optical 9.8 Basic External Authentication

August 23, 2013

This document describes the basic external authentication functionality in Cisco Prime Optical 9.8.

Contents

This document contains the following topics:

Overview

Basic external authentication enables users to log into Prime Optical only once, and thereafter access multiple operations without being required to re-enter a username and password.

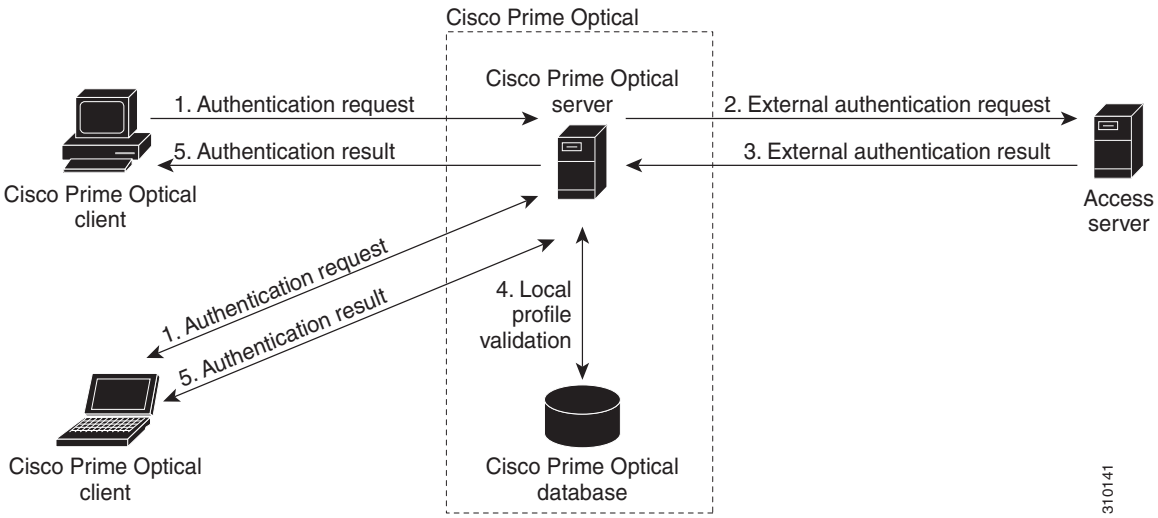
Basic external authentication involves the following protocols:

For information on the differences between the TACACS+ and RADIUS protocols, see http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml.

Cisco Systems, Inc.
www.cisco.com

The following figure illustrates the basic external authentication workflow.

Figure 1 Basic External Authentication Workflow



Note Basic external authentication is not available when Prime Optical is installed with Cisco Prime Central. For more information about Prime Central, see http://www.cisco.com/en/US/products/ps11754/tsd_products_support_series_home.html.

RADIUS

RADIUS is a distributed client/server system that secures networks against unauthorized access.

The Prime Optical server acts as a RADIUS client and sends authentication requests to a RADIUS access server implementing a single sign-on (SSO) application. The RADIUS access server verifies user identity by using Password Authentication Protocol (PAP).

The RADIUS access server is a centralized network server that stores user and credential information. Network devices such as routers, network elements (NEs), and software applications request access permission from the access server.

Once a user logs in, the RADIUS client sends a request to the access server for user access (Access-Request). Upon receiving the user credentials, the access server either accepts (Access-Accept) or rejects (Access-Reject) the request.

TACACS+

Terminal Access Controller Access Control System Plus (TACACS+) is a Cisco proprietary version of TACACS. TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server.

The Prime Optical Server acts as a TACACS+ client and sends an authentication (START) packet to the TACACS+ server. The START packet describes the type of authentication to be performed, and also contains the username and authentication data. In answering the START packet, the server responds with a REPLY packet indicating whether the authentication is finished, or must continue. If the REPLY packet indicates that authentication must continue, then it also indicates what new information is requested.

Setting the Environment

Before enabling basic external authentication in Prime Optical, you must launch the Prime Optical client and create all the necessary users as local users. You must also create these users in the access server.

Note It is possible to create additional users after enabling basic external authentication, but the Password Aging and Password Expiration Early Notification fields in **Administration > Control Panel > Security Properties** are disabled. Similarly, the Auto Disable Account field and Require Password Change on Next Login check box in **Administration > Users > Create New User** are disabled.

Configuring Basic External Authentication

The following sections provide information on configuring basic external authentication:

Configuring Basic External Authentication for RADIUS

Configuring basic authentication for RADIUS requires editing the deployerConfigContext.xml file.

Before You Begin

Create local users as described in Setting the Environment, page 3.

To configure basic authentication for RADIUS:

Step 1 If the Prime Optical server is running, enter the **opticalctl stop** command to stop the server.

Step 2 In the /opt/CiscoTransportManagerServer/tomcat/webapps/SSO/WEB-INF/deployerConfigContext.xml file, go to the "authenticationHandlers" property list section, and uncomment the following statement by removing the enclosing <!-- and --> symbols:

```
<ref bean="radiusAuthenticationHandler"/>
```

Step 3 In the /opt/CiscoTransportManagerServer/tomcat/webapps/SSO/WEB-INF/authenticationHandlers.xml file, go to the bean definition section, and uncomment the "radiusAuthenticationHandler" bean definition.

```
<bean id="radiusAuthenticationHandler"
  class="org.jasig.cas.adaptors.radius.authentication.handler.support.Radius
  AuthenticationHandler">
          <property name="servers">
              <list>
                  <bean class="org.jasig.cas.adaptors.radius.JRadiusServerImpl">
```

```
                    <constructor-arg value="RADIUS_SERVER_HOSTNAME" />
                    <constructor-arg value="SHARED_SECRET" />
                    <constructor-arg>
                        <bean
  class="net.jradius.client.auth.PAPAuthenticator" />
                    </constructor-arg>
                    <constructor-arg value="AUTHENTICATION_PORT" />
                    <constructor-arg value="ACCOUNTING_PORT" />
                    <constructor-arg value="TIMEOUT_IN_SECS" />
                    <constructor-arg value="NUMBER_OF_RETRIES" />
                </bean>
            </list>
        </property>
        <property name="failoverOnException" value="false" />
        <property name="failoverOnAuthenticationFailure" value="false" />
    </bean>
    -->
</beans>
```

Step 4 In the “radiusAuthenticationHandler” bean definition, replace the following parameters with the appropriate values:

- RADIUS_SERVER_HOSTNAME
- SHARED_SECRET
- AUTHENTICATION_PORT
- ACCOUNTING_PORT
- TIMEOUT_IN_SECS
- NUMBER_OF_RETRIES

Step 5 Save and close the file.

Step 6 Enter the following command to change the read permissions:

```
chmod 660
/opt/CiscoTransportManagerServer/tomcat/webapps/SSO/WEB-INF/authenticationHandlers.xml
```

Step 7 Go to the /opt/CiscoTransportManagerServer/cfg/CTMServer.cfg file and set the “ext-auth” property to true.

```
<property name="ext-auth" value="true" />
```

Step 8 Enter the **opticalctl start** command to restart the Prime Optical server.

Configuring Basic Authentication for TACACS+

Configuring basic authentication for TACACS+ requires editing the deployerConfigContext.xml file.

Before You Begin

Create local users as described in Setting the Environment, page 3.

To configure basic authentication for TACACS+:

Step 1 If the Prime Optical server is running, enter the **opticalctl stop** command to stop the server.

Step 2 In the /opt/CiscoTransportManagerServer/tomcat/webapps/SSO/WEB-INF/deployerConfigContext.xml file, go to the "authenticationHandlers" property list section, and uncomment the "jaasTacacsAuthenticationHandler" bean class definition by removing the enclosing <!-- and --> symbols:

```
<bean id="jaasTacacsAuthenticationHandler"
class="org.jasig.cas.authentication.handler.support.JaasAuthenticationHandler" />
```

Step 3 Save and close the file.

Step 4 Enter the following command to generate an encrypted secret key:

```
sh /opt/CiscoTransportManagerServer/tomcat/webapps/SSO/WEB-INF/encrypt.sh <secret key>
```

Step 5 In the /opt/CiscoTransportManagerServer/tomcat/webapps/SSO/WEB-INF/jaas.config.tacacs file, go to the "JaasSecretKey" property and save the encrypted secret key. If necessary, enter a server or update the port property.

For example:

```
CAS {
com.cisco.xmp.jaas.tacacs.TacacsLoginModule required
debug=true
JaasSecretKey="/0ETVZtttpE="
server="tacacs-server.example.com"
port="49";
};
```

Step 6 In the /opt/CiscoTransportManagerServer/tomcat/conf/catalina.properties file, go to the "java.security.auth.login.config" property and uncomment the "java.security.auth.login.config" property by removing the preceding # symbol.

Step 7 Go to the /opt/CiscoTransportManagerServer/cfg/CTMServer.cfg file and set the "ext-auth" property to true.

```
<property name="ext-auth" value="true" />
```

Step 8 Enter the **opticalctl start** command to restart the Prime Optical server.

Configuring RADIUS Failover

You can configure Prime Optical to direct all RADIUS traffic to a standby RADIUS server if the primary RADIUS server becomes unavailable. All RADIUS traffic is directed to the standby server.

Before You Begin

Complete the steps in Configuring Basic External Authentication for RADIUS, page 3.

To configure RADIUS failover:

Step 1 If the Prime Optical server is running, enter the **opticalctl stop** command to stop the server.

Step 2 In the /opt/CiscoTransportManagerServer/tomcat/webapps/SSO/WEB-INF/authenticationHandlers.xml file, go to the "servers" property section and add another bean definition that designates a standby server.

For example:

```
<property name="servers">
```

```
        <list>
            <bean
                class="org.jasig.cas.adaptors.radius.JRadiusServerImpl">
                <constructor-arg value="radius-server1.example.com" />
                <constructor-arg value="testing123" />
                <constructor-arg>
                    <bean class="net.jradius.client.auth.PAPAuthenticator" />
                </constructor-arg>
                <constructor-arg value="1812" />
                <constructor-arg value="1813" />
                <constructor-arg value="3" />
                <constructor-arg value="3" />
            </bean>
            <bean
                class="org.jasig.cas.adaptors.radius.JRadiusServerImpl">
                <constructor-arg value="radius-server2.example.com" />
                <constructor-arg value="testing456" />
                <constructor-arg>
                    <bean class="net.jradius.client.auth.PAPAuthenticator" />
                </constructor-arg>
                <constructor-arg value="1812" />
                <constructor-arg value="1813" />
                <constructor-arg value="3" />
                <constructor-arg value="3" />
            </bean>
        </list>
    </property>
```

where `radius-server1.example.com` is the primary server and `radius-server2.example.com` is the standby server.

Note You can add multiple servers by adding additional bean definitions. Failover will occur on servers in the order in which they appear in the “servers” property section.

Step 3 To enable failover because of server problems (for example, when a server is unreachable), set the “failoverOnException” property to true. For example:

```
<property name="failoverOnException" value="true" />
```

Step 4 To enable failover when a server rejects a user (Access-Reject), set the “failoverOnAuthenticationFailure” property to true. For example:

```
<property name="failoverOnAuthenticationFailure" value="true" />
```

Step 5 Enter the **opticalctl start** command to restart the Prime Optical server.

Disabling Fallback to Local Authentication

You can disable fallback to local authentication, which is enabled by default.

Before You Begin

Complete the steps in Configuring Basic External Authentication, page 3.

To disable fallback to local authentication:

Step 1 If the Prime Optical server is running, enter the opticalctl stop command to stop the server.

Step 2 In the /opt/CiscoTransportManagerServer/tomcat/webapps/SSO/WEB-INF/deployerConfigContext.xml file, go to the "authenticationHandlers" property section and comment the "jdbcAuthenticationHandler" bean class definition by adding the enclosing <!-- and --> symbols:

```
<ref bean="jdbcAuthenticationHandler"/>
```

Step 3 Enter the **opticalctl start** command to restart the Prime Optical server.

Local Authentication Limitations

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

- 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. See Setting the Environment, page 3 to disable these rules.
- The password change feature changes the *local password only* and does not affect the access server password.
- Although authentication is external, authorization is local. For example, user privileges are managed locally. The external server only grants or denies access. It does not recognize different access privileges for different users.

Related Documentation

See *Cisco Prime Optical 9.8 Documentation Overview* for a list of Prime Optical 9.8 guides.

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.