Managing Security with Cisco EPOM

This chapter contains the following topics:

The Cisco EPOM security management system extends the functionality of the Cisco BTS 10200 security system which controls and monitors access to the Cisco BTS 10200 Softswitch from outside sources. This security system is important in preventing:

- Errors by personnel not trained in specific procedures
- Unauthorized changes to system provisioning
- Unauthorized viewing or modification of databases

Internal security functions include:

- Providing user interface to provision users and security classes (privilege levels)
- Storing user login profiles
- Performing user authentication
- Managing the level of access on a per user basis
- Providing session oriented security measures
- Providing transaction oriented security measures
- Logging all access activity to a log
- Maintaining security log for 7 days
- Providing user interface for security log reporting

About Cisco EPOM Security

With Cisco EPOM, you can assign a Cisco BTS 10200 login name and password to a Cisco EPOM group. This allows Cisco EPOM to restrict a user's access to that of the assigned Cisco BTS 10200 login. A combination of user identity and command tables determines if access is granted or denied.

When a user logs in to Cisco EPOM, the user's group is examined for an associated Cisco BTS 10200 login. If Cisco EPOM finds an association, Cisco EPOM queries the Cisco BTS 10200 user table for that user's assigned security level and work groups. Cisco EPOM caches the command table for each Cisco BTS 10200 EMS server. The command table defines valid noun-verb combinations as well as required

security level and work groups to run those combinations. By using the login security level and workgroups, Cisco EPOM determines if the user has permission to enter a command. This check is done for every request. If the user does not meet or exceed permission requirements, a "permission denied" message appears.

Note If no Cisco BTS 10200 login name is assigned to the Cisco EPOM group, security defaults to the user login and password that is specified for the device. (To check the user and password for a device, choose **Domains** > *domain name* > **Edit** > *device name* > **Edit**.)

Tip
- Because all commands are issued from Cisco EPOM, the commands appear in the Cisco BTS 10200 audit logs as being performed by a single Cisco BTS 10200 user. You can check the Cisco EPOM audit.log to determine who issued which commands. The trace.log shows the access denials that occurred. The audit.log and trace.log files are located on the Cisco EPOM server in /var/opt/CSCOepom/logs.

- If you modify the Cisco BTS 10200 login security level or workgroups, the impacted Cisco EPOM user must log out and log in to Cisco EPOM for those changes to take effect.

- Because Cisco EPOM caches the command table when the initial connection is made, if you change the security level or work groups for commands on the Cisco BTS 10200, you must restart Cisco EPOM for the changes to take effect.

Setting Up Cisco EPOM Security

Step 1 Create Cisco BTS 10200 users with required security levels. Refer to Chapter 17, "Security Functions and Activity Summary" in the *Cisco BTS 10200 Softswitch Operations Manual*.

Step 2 On the Cisco EPOM server, log in as admin and create user groups. See the "Adding Domains, Groups, and Users" section on page 3-10.

Step 3 On the Cisco EPOM server, create users, and assign them to the user groups that you created in Step 2. See the "Adding Domains, Groups, and Users" section on page 3-10.

Step 4 choose **Users** > *user name* > **Edit**.

The Modify User window appears.

Modify user: admin			OK	Cancel

Username	admin
First Name	Default
Last Name	Administrator
Password	******************************
Confirm Password	******************************
Email Address	
Groups	admin

Step 5   Enter a password to access Cisco EPOM.

Step 6   Choose **Users** > **Groups** > **Edit**.

The Edit Group window appears.

Step 7   Select a group from the list and click **Edit**.

Edit Group	OK	Cancel

Group Name	admin
BTS Login	
BTS Navigation Tree	

Step 8   Assign the Cisco EPOM user group to a Cisco BTS 10200 user by entering the user's Cisco BTS 10200 Login and (optional) Cisco BTS 10200 Navigation Tree.

Note   If a Cisco EPOM user group is not assigned to a Cisco BTS 10200 user, all users in that group have a security level of 10 (unrestricted).

Step 9   To verify the assigned Cisco BTS 10200 login, choose **Users** > **Groups** > *group name* > **Edit**.

The assigned login appears.

Creating Custom Navigation Trees

With Cisco EPOM, you can create custom navigation trees that define how Cisco BTS 10200 objects (such as media gateways, subscribers, and call agents) are presented. These trees are defined by an .xml file that follows simple syntax rules. The tree is then assigned to a Cisco EPOM user group. Customized trees allow administrators to define and limit navigation functionality based on a user's job function.

Example of a Navigation Tree

The defaulttree.xml file shown here is located in:
/opt/CSCOepom/tomcat/webapps/ROOT/xml/bts/navigation.

You can use this file as a template for defining new trees.

```
<tree name="default">

    <baseurl name="bts">
        <urlprefix><![CDATA[/bts/btscomp.jsp?_inv=[_inv]&_noun=]]></urlprefix>
    </baseurl>

    <baseurl name="btssearch">
        <urlprefix><![CDATA[/bts/btscompsearch.jsp?_inv=[_inv]&_noun=]]></urlprefix>
    </baseurl>

    <baseurl name="btsstatus">
        <urlprefix><![CDATA[/bts/btscompstatus.jsp?_inv=[_inv]&_noun=]]></urlprefix>
    </baseurl>

    <baseurl name="btsdiag">
        <urlprefix><![CDATA[/bts/btscompdiag.jsp?_inv=[_inv]&_noun=]]></urlprefix>
    </baseurl>

    <baseurl name="btswizard">
        <urlprefix><![CDATA[/bts/btswizard.jsp?_inv=[_inv]&_noun=]]></urlprefix>
    </baseurl>

    <baseurl name="images">
        <urlprefix>../images/treemenuimage</urlprefix>
    </baseurl>

    <imagepath>
        <url base="images"/>
    </imagepath>

    <image name="BTS10200">
        <url base="images">16x16_BTS_10200_Softswitch_Blue.gif</url>
    </image>

    <image name="tablegrp">
        <url base="images">table16_window.gif</url>
    </image>

    <image name="bts">
        <url base="images">table16.gif</url>
    </image>

    <image name="btssearch">
        <url base="images">table16_basicquery.gif</url>
    </image>

    <image name="btsstatus">
        <url base="images">table16_show.gif</url>
    </image>

    <image name="btsdiag">
        <url base="images">table16_diag.gif</url>
    </image>

    <image>
        <url base="images">menu_folder_open.gif</url>
```

```
        </image>

        <image>
            <url base="images">menu_folder_closed.gif</url>
        </image>

        <image>
            <url base="images">menu_corner.gif</url>
        </image>

        <image>
            <url base="images">menu_corner_plus.gif</url>
        </image>

        <image>
            <url base="images">menu_corner_minus.gif</url>
        </image>

        <image>
            <url base="images">menu_bar.gif</url>
        </image>

        <image>
            <url base="images">menu_link.gif</url>
        </image>

        <cssclassmap type="branch" class="parent_node"/>
        <cssclassmap type="node" class="child_node"/>

        <imagemap type="branch" image="tablegrp"/>
        <imagemap type="node" image="bts"/>

        <root name="[_hostname]" class="parent_node" image="BTS10200">
            <url base="btsstatus"><![CDATA[system&_cmd=do_status]]></url>
            <branch name="bts.head.ain">
            <node name="bts.ani_wb_list"
            <url base="bts">ani_wb_list</url>
            </node>

            <node name="bts.cust_grp"
            <url base="bts">cust_grp</url>
            </node>

            <node name="bts.dn2cust_grp"
            <url base="bts">dn2cust_grp</url>
            </node>

            <node name="bts.ii_restrict_list"
            <url base="bts">ii_restrict_list</url>
            </node>

            </branch>
        </root>
    </tree>
```

Activating the Navigation Tree

Step 1 Create the .xml file that defines your navigation tree. (See the "Example of a Navigation Tree" section on page 6-4.)

Step 2 Place the .xml file in the /opt/CSCOepom/tomcat/webapps/ROOT/xml/bts/navigation directory.

Step 3   Choose **Users** > **Groups** > *group name* > **Edit**.

The Edit Group window appears.

Edit Group	OK	Cancel

Group Name	admin
BTS Login	
BTS Navigation Tree	

Step 4   In the Cisco BTS 10200 Navigation Tree field, enter the name of the file that you created.

Step 5   Click **OK**.

Note   If you do not specify the name of a customized navigation tree, Cisco EPOM uses the defaulttree.xml.