

Chapter 7

Providing Threat Mitigation Services with the Threat Mitigation Application

This chapter describes the Threat Mitigation Application and how to use it to mitigate threats in the SDX network. This chapter contains the following sections:

- Overview of the Threat Mitigation Application on page 105
- Before You Install the Threat Mitigation Application on page 106
- Sample Implementation on page 107
- Installing and Initially Configuring the Threat Mitigation Application on page 108
- Configuring Threat Mitigation on page 109
- Managing Threats with the Threat Mitigation Portal on page 125
- Enabling SDX Actions from NetScreen-Security Manager on page 135

Overview of the Threat Mitigation Application

The Threat Mitigation Application helps administrators detect and respond to attacks on the network. The Threat Mitigation Application can be customized based on customer-supplied data to control the description and recommended actions for each type of attack. If the user chooses to take an action, the Threat Mitigation Application activates an SDX service for the source address of the event. The Threat Mitigation Application includes the ability to log all user operations to provide an audit trail of actions.

You can use the Threat Mitigation Application to respond to threats on the network by:

- Executing an SDX script for Juniper Networks NetScreen-Security Manager that posts information about the attack to the Threat Mitigation Portal
- Managing attacks with the Threat Mitigation Portal that provides information about the nature of the attack and possible actions
- Applying policies to the interfaces to manage problem traffic, such as applying policies that reduce the amount of available bandwidth or that block the threat

The Threat Mitigation Application deals with threats in an SDX-managed environment by providing a solution that involves using:

- Juniper Networks Intrusion Detection and Prevention (IDP) sensors to detect the threats.

IDP sensors are IDP hardware appliances that run the IDP sensor software. The sensors monitor network traffic to detect suspicious or anomalous traffic and respond as configured. IDP monitors network traffic to detect potentially detrimental traffic and responds to problem incidents to prevent damage to the network.

- Juniper Networks NetScreen-Security Manager to manage the IDP sensors and to signal the Threat Mitigation Portal when a threat is detected.

NetScreen-Security Manager is software that enables you to integrate and centralize management of your Juniper Networks security environment. NetScreen-Security Manager delivers integrated, policy-based security and network management for all Juniper Networks security devices. NetScreen-Security Manager is used for its elaborate authorization and auditing functionality, which provides more detailed reporting and analysis.

- The Threat Mitigation Portal to display detailed information about the threat and the recommended actions to the administrator.

The Threat Mitigation Portal is the user interface for the Threat Mitigation Application that enables administrators to manage threats and act on them. The administrator can react to the threat by activating a service in the SAE. The service activation can result in pushing policies, for the originating IP address, to the upstream JUNOS routing platforms in the core network or to the JUNOS edge routers, depending on the configuration.

Before You Install the Threat Mitigation Application

Installing the Threat Mitigation Application into an SDX-managed environment requires:

- The SDX UMChma package installed with your SDX application library software.
- SDX-managed JUNOS routers or JUNOS routing platforms in the network.
- Working knowledge of the NetScreen-Security Manager software and familiarity with NetScreen-Security Manager documentation. See

<http://www.juniper.net/techpubs/software/management/security-manager/>

- Working knowledge of the IDP software and familiarity with IDP documentation. See

<http://www.juniper.net/techpubs/software/management/idp/>

Before you use the Threat Mitigation Application, you typically:

- Install the transactional database. The Threat Mitigation Application provides a sample schema that includes these tables:
 - ATTACK—Attacks
 - ATTACK_TYPE—Attack types
 - ACTION—Configured actions that the application can execute
 - ATTACK_TYPE_CANDIDATE_ACTION—Candidate actions that can be taken in response to attack types

The administrator maintains the data in the ATTACK_TYPE, ACTION, and ATTACK_TYPE_CANDIDATE_ACTION tables to ensure that the data defines the relationship between attack types and candidate actions. In cases where attacks do not belong to any defined attack types, the administrator should create a default attack type and the candidate actions for the default attack type.

- Install the IDP sensors. The sensors monitor network traffic to detect suspicious or anomalous traffic and respond as configured.
- Install NetScreen-Security Manager to monitor the IDP sensors. The administrator creates the attack types that are reported to the Threat Mitigation Application.

Sample Implementation

The SDX application library provides a robust sample implementation for mitigating threats using the Threat Mitigation Application in an SDX-managed network.

The sample implementation includes:

- Policies, services, router definitions, and SAE configurations in the sample data. Sample entries for the Threat Mitigation Application have the prefix THMA.

For information about installing sample data, see *Installing and Initially Configuring the Threat Mitigation Application* on page 108.

- Data in the schema to detail attacks, actions that can be executed by the application, and actions that can be used to respond to attacks.

You can use the sample data and application to create a demonstration implementation. The router definitions, identified as THMA <routername > in the sample data, can be configured to act as simulated routers for a demonstration environment. For information about setting up a simulated router, see *SDX Monitoring and Troubleshooting Guide, Chapter 3, Configuring a Simulated Router Driver for Testing*.

You can also customize the sample data to mitigate threats in your network, or you can use the samples as a guide to create your own implementation.

The sample data uses the following terminology for the type of interface on which the service would be activated:

- Provider edge interface—Subscriber-facing interface on the JUNOS routing platform
- Forwarding interface—Forwarding interface on the JUNOS routing platform
- Subscriber interface—Subscriber interface on the JUNOSe router

Installing and Initially Configuring the Threat Mitigation Application

Because the Threat Mitigation Application relies on other components in the SDX network, you must complete several tasks before you install the Threat Mitigation Application software. After you install the software, you must also complete several configuration tasks before the application can function correctly.

For information about the location of the Threat Mitigation Application software on the application library CD, see *Chapter 1, Installing the SDX Applications*.

Before You Start

Before you install and configure the Threat Mitigation Application, you must:

1. Deploy a working SDX network.

To support the Threat Mitigation Application, you must install SAEs to manage the routers or other devices through which subscribers connect to the network. You must also install and configure the directory in which you will store the SDX data.

2. Install a J2EE application server on the host that supports the Threat Mitigation Application.

For information about installing JBoss (the J2EE application server provided with the SDX software), see *SDX Getting Started Guide, Chapter 5, Installing the SDX-300 Software*.

3. On the host that supports the Threat Mitigation Application, install a transactional database to store the data for the Threat Mitigation Application.

Installing and Initially Configuring the Threat Mitigation Application Software

To install the Threat Mitigation Application:

1. Install the Solaris package for the Threat Mitigation Application (see *Chapter 1, Installing the SDX Applications*) on the hosts that support the following components:
 - SAEs
 - Directory
 - JBoss

2. Run the configuration script to configure the Threat Mitigation Application. See *Configuring the Threat Mitigation Application* on page 115.
3. Run the load script to complete the configuration tasks for deploying the Threat Mitigation Application. See *Deploying the Threat Mitigation Application* on page 120.
4. On each host, restart JBoss.

You must restart JBoss when you have configured the Threat Mitigation Portal for the first time or you have changed the database type.

Configuring Threat Mitigation

To support threat mitigation with the Threat Mitigation Application in an SDX network, configure services that can be activated to act on threats detected by IDP sensors that are managed by NetScreen-Security Manager. We recommend that you activate the services as close as possible to the interfaces where the problem traffic entered the network.

For detailed information about configuring services, see *SDX Services and Policies Guide, Chapter 1, Managing Services*.

To use the Threat Mitigation Application, perform the following tasks:

- Configuring a Database to Store Attack and Response Data on page 110
- Configuring the Threat Mitigation Application on page 115
- Deploying the Threat Mitigation Application on page 120
- Applying SDX Services to Manage Threats on page 121
- Classifying Subscribers and Interfaces on page 123

Some sections provide references to entries in the sample data that demonstrate an implementation.

After performing these tasks, configure the script used by NetScreen-Security Manager to implement the messaging that records attacks and identifies actions that the SDX software should take in response to those attacks. See *Enabling SDX Actions from NetScreen-Security Manager* on page 135.

Configuring a Database to Store Attack and Response Data

The Threat Mitigation Application requires a transactional database to store attack types and candidate responses. For information about databases that we have tested for use with the Threat Mitigation Application, see the *SDX Application Library Release Notes*.

The Threat Mitigation Application provides sample data for a schema that includes these tables:

- **ATTACK_TYPE**—Contains information about the attacks that NetScreen-Security Manager is expected to send to the Threat Mitigation Application. The administrator maintains this data. See *Configuring Attack Types in the Database* on page 111.
- **ACTION**—Contains information about the SDX services that are activated to respond to attacks. The administrator maintains this data. See *Configuring Actions in the Database* on page 112.
- **ATTACK_TYPE_CANDIDATE_ACTION**—Contains information about the actions that can be taken in response to specific attack types. The administrator maintains this data. See *Configuring Candidate Actions in the Database* on page 114.
- **ATTACK**—Contains information about the attacks that are managed by the Threat Mitigation Application. The Threat Mitigation Portal displays this information on various pages, including the Attack Details page. For information about how the Threat Mitigation Portal displays the attributes, see *About the Record Servlet* on page 125.

To use the Threat Mitigation Application, the administrator must create data in the **ATTACK_TYPE**, **ACTION**, and **ATTACK_TYPE_CANDIDATE_ACTION** tables to define the relationship between attack types and candidate actions. The information in the **ATTACK** table is managed by the Threat Mitigation Application and must not be modified by an administrator. The attributes specified in the tables are referenced in the XML schema for NetScreen-Security Manager attack events.

To configure the database:

1. Create a database, tables, and user for the database by using the following database schema file:

```
/opt/UMC/conf/thma/etc/< database >/thma.sql
```

where **< database >** is the selected database when you run the load script. This file is created when you install the Solaris package for the Threat Mitigation Application.

2. Load the sample data for the database using the following file:

```
/opt/UMC/conf/thma/etc/< database >/data.sql
```

where **< database >** is the selected database when you run the load script. This file is created when you install the Solaris package for the Threat Mitigation Application.

Configuring Attack Types in the Database

The ATTACK_TYPE table contains data about all the attacks that NetScreen-Security Manager is expected to send to the Threat Mitigation Application. Attacks are considered to be the same attack type if their category, subcategory, and definingAttributes values are the same.



NOTE: The ATTACK_TYPE table must contain a special attack type with category and subcategory values of DEFAULT to respond to attacks that do not match a configured attack type.

The entry in the `/opt/UMC/conf/thma/etc/< database >/data.sql` file contains the attributes in the format:

```
INSERT INTO ATTACK_TYPE
VALUES ('<category>', '<subcategory>', '<definingAttributes>', '<description>');
```

For example:

```
INSERT INTO ATTACK_TYPE
VALUES ('DEFAULT', 'DEFAULT', 'srcAddr', 'There is no specific information for this type
of attack.');
```

ATTACK_TYPE Attributes

The Threat Mitigation Portal displays the configured attributes for the attack types that are used by the Threat Mitigation Application.

category

- Category of the attack; displayed in the Attack Details page.
- Value—Text string
- Examples
 - DEFAULT
 - predefined

subcategory

- Subcategory of the attack; displayed in the Attack Type column.
- Value—Text string
- Examples
 - DEFAULT
 - FTP:USER:ROOT
 - ICMP:EXPLOIT:FLOOD

definingAttributes

- Attributes used to identify an attack. Defining attributes determine whether an attack is a new record or an update to an existing attack record. The srcAddr attribute is always considered a defining attribute for the attack, even if it is not specified as a defining attribute.
- Value—List of defining attributes separated by semicolons
 - srcAddr—Source address; displayed in the Source column
 - srcPort—Source port; displayed in the Attack Details page
 - dstAddr—Destination address; displayed in the Destination column
 - dstPort—Destination port; displayed in the Attack Details page
 - protocol—Protocol; displayed in the Attack Details page
 - user—User; displayed in the Attack Details page
 - app—Application; displayed in the Attack Details page
 - uri—Uniform resource identifier; displayed in the Attack Details page
- Examples
 - srcAddr
 - srcAddr;dstAddr;dstPort
 - srcAddr;dstAddr

description

- Description of the attack; displayed in the Attack Details page.
- Value—Text string
- Examples
 - There is no specific information for this type of attack.
 - This attack indicates an ICMP session that contains more than 250 ICMP packets per second. This may indicate that an attacker is trying to degrade network performance, causing poor service for legitimate users.

Configuring Actions in the Database

The ACTION table contains data about services to activate in response to an attack. The administrator must add one ACTION table entry for each SDX service that is used as an action in the Threat Mitigation Application.

The entry in the `/opt/UMC/conf/thma/etc/<database>/data.sql` file contains the attributes in the format:

```
INSERT INTO ACTION
VALUES ('<serviceName>', '<name>', '<description>');
```

For example:

```
INSERT INTO ACTION
VALUES ('BlockAttacker', 'Block Attacker', 'This action blocks all traffic to and from the attacker.');
```

ACTION Attributes

The Threat Mitigation Portal displays the configured attributes for the actions that are used by the Threat Mitigation Application.

serviceName

- Service activated in response to an attack.
- Value—Text string
 - The following values are passed to the service as parameter substitutions:
 - category—Name of the category
 - subcategory—Name of the subcategory
 - severity—Severity level as a number in the range 0–5
 - 0—not set
 - 1—info
 - 2—warning
 - 3—minor
 - 4—major
 - 5—critical
 - srcAddr—IP address; enclose in single quotes if not in IPv4 format
 - srcPort—Port number
 - dstAddr—IP address; enclose in single quotes if not in IPv4 format
 - dstPort—Port number
 - protocol—Protocol number
 - user—Username
 - app—Name of the application
 - uri—Uniform resource identifier

The category, subcategory, user, app, and uri parameters are encoded as valid parameter names (not text strings) so that these parameter values can be provided to the policies.

For example, you could define a policy that takes the app parameter as the value for a policer rate with a default value of 64000. Then, you could define global parameters named after different applications, such as http = 32000. When the attack includes an HTTP application, the Threat Mitigation Application would pass app = http, and 32000 would be the value in the policer definition.

- Example—BlockAttacker

name

- Name of action; displayed in the Action drop-down list.
- Value—Text string
- Example—Block Attacker

description

- Description of the action; displayed in the Action Help page.
- Value—Text string
- Example—This action blocks all traffic to and from the attacker.

Configuring Candidate Actions in the Database

The ATTACK_TYPE_CANDIDATE_ACTION table contains data about the possible services to activate in response to a particular type of attack.

The entry in the `/opt/UMC/conf/thma/etc/< database >/data.sql` file contains the attributes in the format:

```
INSERT INTO ATTACK_TYPE_CANDIDATE_ACTION
VALUES ('<category>', '<subcategory>', '<serviceName>');
```

For example:

```
INSERT INTO ATTACK_TYPE_CANDIDATE_ACTION
VALUES ('DEFAULT', 'DEFAULT', 'BlockAttack');
```

ATTACK_TYPE_CANDIDATE_ACTION Attributes

The Threat Mitigation Portal displays the configured attributes for the attack type and candidate actions.

category

- Category of the attack; displayed in the Attack Details page.
- Value—Text string
- Examples
 - DEFAULT
 - predefined

subcategory

- Subcategory of the attack; displayed in the Attack Type column.
- Value—Text string
- Examples
 - DEFAULT
 - FTP:USER:ROOT
 - ICMP:EXPLOIT:FLOOD

serviceName

- Service activated in response to an attack.
- Value—Text string
- Example—BlockAttacker

Configuring the Threat Mitigation Application

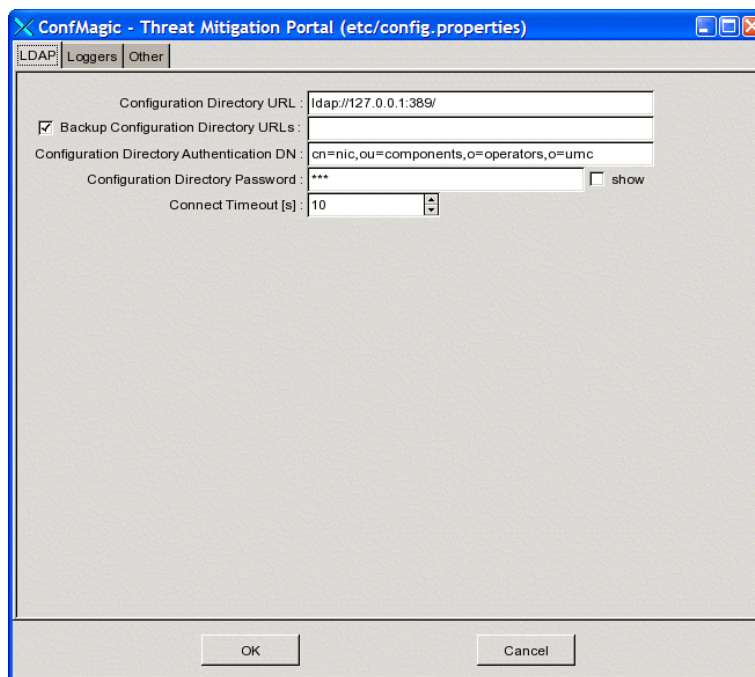
The Threat Mitigation Application configuration script updates the bootstrap configuration for the Threat Mitigation Application and configures the Threat Mitigation Portal.

To configure the Threat Mitigation Application:

1. On the host, log in as `root` or as another authorized administrator.
2. Launch the configuration tool.

`/opt/UMC/conf/thma/etc/config`

The configuration tool window appears.

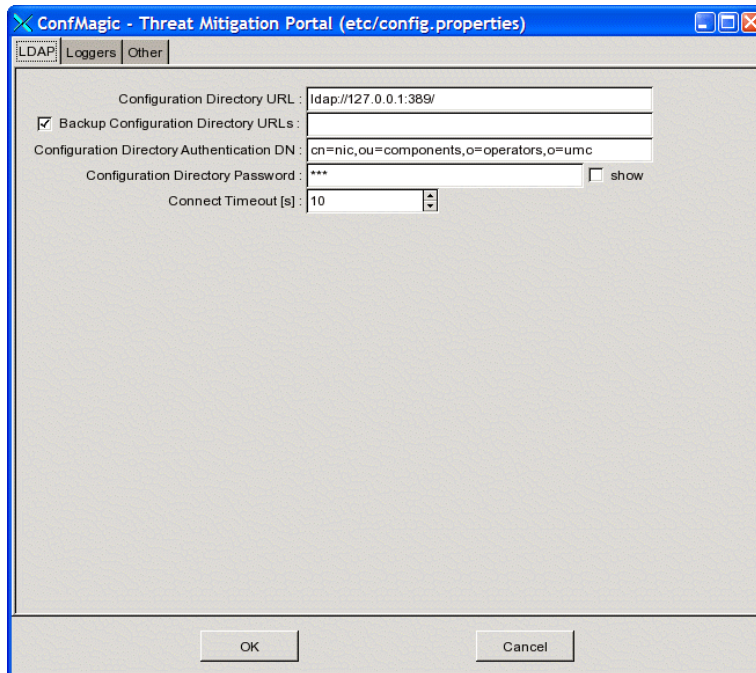


3. Edit or accept the values for the fields in the appropriate tab to perform these tasks:
 - Configuring Connections to the Directory on page 116
 - Configuring Logging on page 118
 - *Configuring the Threat Mitigation Portal* on page 119
4. Click OK.
5. A file called `config.properties` appears in the `/opt/UMC/conf/thma/etc` folder, and it is added to the `/opt/UMC/conf/thma/webapp/thma.ear` file.

Configuring Connections to the Directory

The Threat Mitigation Application loads configurations from the directory. If you install the directory on a different host than the J2EE application server, you must modify the bootstrap properties to specify the directory host.

To configure the connections to the directory for the Threat Mitigation Application, edit or accept the default values for the fields in the LDAP tab.



Configuration Directory URL

- URL of the primary directory.
- Value—URL in the format ldap:// <host > : <port > /
 - <host > —IP address or name of directory host
 - <port > —Port of directory host
- Default—ldap://127.0.0.1:389/
- Property name—Config.java.naming.provider.url

Backup Configuration Directory URLs

- List of redundant directories.
- Value—Space-separated list of URLs; URLs have the format ldap:// <host > : <port > /
 - <host > —IP address or name of directory host
 - <port > —Port of directory host
- Default—Unspecified

- Example—`ldap://192.0.2.1:389/ ldap://192.0.2.3:389/`
- Property name—`Config.net.juniper.smgmt.des.backup_provider_urls`

Configuration Directory Authentication DN

- DN of the directory entry that defines the username with which the SDX component accesses the directory.
- Value— `<DN >`
- Default—`cn = nic, ou = Components, o = Operators, o = umc`
- Example—`cn = conf, o = Operators, o = umc`
- Property name—`Config.java.naming.security.principal`

Configuration Directory Password

- Password with which the Threat Mitigation Application accesses the directory.
- Value—Text string
- Default—`nic`
- Example—`secret`
- Property name—`Config.java.naming.security.credentials`

Connect Timeouts [s]

- Maximum time that the directory eventing system (DES) waits for the directory to respond.
- Value—Number of seconds in the range 1–2147483647
- Default—10
- Example—5
- Property name—`Config.net.juniper.smgmt.des.connect.timeout`

Configuring Logging

To configure logging for the Threat Mitigation Application, edit or accept the default values for the fields in the Loggers tab.

The screenshot shows the 'Loggers' tab in the 'ConfMagic - Threat Mitigation Portal' configuration window. The window has three tabs: 'LDAP', 'Loggers', and 'Other'. The 'Loggers' tab is active and contains the following configuration options:

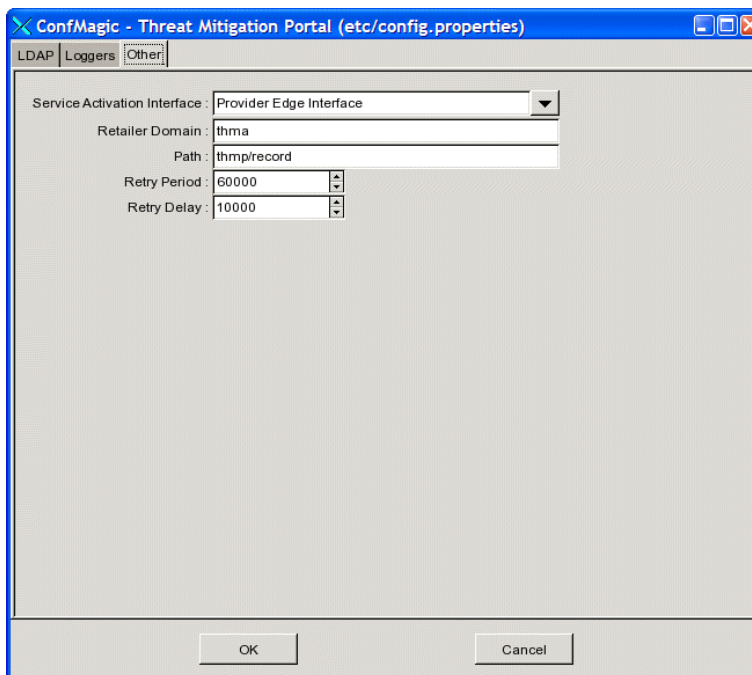
- Error Log Filter (e.g. %error-): /error-
 - Error Log File: thma_error.log (Browse...)
 - Error Rollover File: thma_error.alt (Browse...)
 - Error Log Rollover Size: 1000000 (spinners)
- Info Log Filter (e.g. %info-): /info-
 - Info Log File: thma_info.log (Browse...)
 - Info Log Rollover File: thma_info.alt (Browse...)
 - Info Log Rollover Size: 1000000 (spinners)
- Debug Log Filter (e.g. %debug-): /debug-
 - Debug Log File: thma_debug.log (Browse...)
 - Debug Log Rollover File: thma_debug.alt (Browse...)
 - Debug Log Rollover Size: 1000000 (spinners)
- Audit Log Filter (e.g. %audit,%info-): Audit,%info-
 - Audit Log File: thma_audit.log (Browse...)
 - Audit Rollover File: thma_audit.alt (Browse...)
 - Audit Log Rollover Size: 1000000 (spinners)
- Error Syslog Filter (e.g. %error-): /error-
 - Error Syslog Hostname: loghost
- Info Syslog Filter (e.g. %info-warning): /info-warning
 - Info Syslog Hostname: loghost

At the bottom of the window are 'OK' and 'Cancel' buttons.

For more information about logging, see *SDX Monitoring and Troubleshooting Guide, Chapter 2, Configuring Logging for SDX Components*.

Configuring the Threat Mitigation Portal

To configure the Threat Mitigation Portal, edit or accept the default values for the fields in the Other tab.



Service Activation Interface

- Type of interface on which the service would be activated.
- Value
 - Provider Edge Interface (JUNOS subscriber-facing interface)
 - Forwarding Interface (JUNOS forwarding interface)
 - Subscriber Interface (JUNOS subscriber interface)
- Guidelines—If you change this property, you must reconfigure your NIC host. For more information, see *Using the NIC Resolver for the Threat Mitigation Portal* on page 127.
- Default—Provider Edge Interface

Retailer Domain

- Retailer domain for the Threat Mitigation Portal.
- Value—Text string
- Guidelines—This property must match one of the retailer domain names defined for the retailer in the target of the subscriber classification rules used for the interfaces managed by the Threat Mitigation Application. For more information about adding retailers, see *SDX Subscribers and Subscriptions Guide, Chapter 8, Configuring Subscribers and Subscriptions*.
- Default—thma

Path

- Pathname for the Threat Mitigation Portal and record servlet.
- Value— < pathname >
- Default—/thmp/record

Retry Period

- Time to wait between two consecutive retries of all pending service activation or deactivation tasks that were executed unsuccessfully.
- Value—Number of milliseconds in the range 0–9223372036854775807
- Guidelines—Do not specify too small a value, because the number of attempts could cause network overload.
- Default—60000

Retry Delay

- Time to wait before retrying all pending service activation or deactivation tasks that were executed unsuccessfully.
- Value—Number of milliseconds in the range 0–9223372036854775807
- Default—10000

Deploying the Threat Mitigation Application

The Threat Mitigation Application load script configures components (such as the J2EE application server, directory, and database) on the local host. However, depending on the components used, their installation host, and their configuration, you may need to manually configure some of the components or modify the configuration.

The Threat Mitigation Application load script automates the process of deploying the Threat Mitigation Application in JBoss (if it is installed locally) and completes these configuration tasks:

- Configures the *jbosscmp-jdbc.xml* file inside the */opt/UMC/conf/thma/webapp/thma.ear* file and the data source deployment descriptor based on the type of database specified and the database connection information.
- Installs the JDBC driver, data source deployment descriptor, and authentication configurations in JBoss (if JBoss is installed locally).
- Loads the Threat Mitigation Application sample data in the directory.
- Creates the database schema and loads sample database records. Follow the instructions at the end of the load script to complete the database configuration for the selected database. Some databases might require additional steps, such as creating a database user or enabling a remote TCP/IP connection.

To deploy the Threat Mitigation Application:

1. On the host, log in as `root` or as another authorized administrator.
2. Invoke the script by accessing the folder `/opt/UMC/conf/thma/etc` and running the `load` command.

```
cd /opt/UMC/conf/thma/etc  
./load
```

3. Deploy the `thma.ear` file by using the procedure appropriate for your Web application server.

If you are using JBoss, copy the file to the JBoss `/default/deploy` directory. For example:

```
cp /opt/UMC/conf/thma/webapp/thma.ear  
/opt/UMC/jboss/server/default/deploy
```

Applying SDX Services to Manage Threats

You can configure services to control problem traffic, such as limiting bandwidth or blocking traffic, in response to detection of malicious traffic. The Threat Mitigation Application passes the defining attribute values of the attack type to the service as parameters for possible use in the policies. The Threat Mitigation Application supports service activation on the JUNOS forwarding interface, the JUNOS provider edge interface, or the JUNOS subscriber interface. You can configure only one of these interfaces as the service activation interface for the Threat Mitigation Application, but you can use an aggregate service to apply the policies on a combination of those interfaces. For information about configuring the service activation interface, see *Configuring the Threat Mitigation Portal* on page 119.

The following example describes how to configure policies to decrease the amount of bandwidth available to the attacker and to block the attack or the attacker as implemented in the sample data. You can use any of these services or create your own services to define actions for the Threat Mitigation Application.

To configure services and policies to handle threats:

1. In Policy Editor, create a policy that defines an action to be taken.

The sample data for each type of interface contains these policy groups:

- `blockAttack`—Blocks all traffic between the source and destination addresses for the specified protocol and ports. If the protocol or ports are not specified, then the default value is any protocol and any port.
- `blockAttacker`—Blocks all traffic coming from or going to the source address.
- `default`—Forwards traffic.
- `slowAttacker`—Limits the bandwidth available for all traffic coming from or going to the source address according to the specified rate.

For a policy folder that contains these policy groups for the JUNOS forwarding interface, see *ou = forwardingInterface, ou = thma, o = Policies, o = umc* in the sample data.

For a policy folder that contains these policy groups for the JUNOS provider edge interface, see *ou = peInterface, ou = thma, o = Policies, o = umc* in the sample data.

For a policy folder that contains these policy groups for the JUNOS subscriber interface, see *ou = subrInterface, ou = thma, o = Policies, o = umc* in the sample data.

For information about configuring policies, see *SDX Services and Policies Guide, Chapter 5, Configuring and Managing Policies*.

2. In SDX Admin, create a new scope or use an existing scope for the services that define actions to be taken in response to attacks on different interfaces.

For a sample scope that applies to the JUNOS forwarding interface, see *l = THMA-ForwardingInterface, o = Scopes, o = umc*.

For a sample scope that applies to the JUNOS provider edge interface, see *l = THMA-PInterface, o = Scopes, o = umc*.

For a sample scope that applies to the JUNOS subscriber interface, see *l = THMA-SubrInterface, o = Scopes, o = umc*.

For general information about configuring scopes, see *SDX Services and Policies Guide, Chapter 1, Managing Services*.

3. For the scope used in Step 2:
 - a. Create a service that defines actions to be taken in response to threats. You can create different types of services. For example, you can create aggregate services to apply the policies on these interfaces.

The sample data contains normal value-added services that specify the policy group configured in Step 1.

For a sample service to block attacks on the forwarding interface, see *serviceName = BlockAttack, l = THMA-ForwardingInterface, o = Scopes, o = umc*.

- b. Assign the scope to a subscriber folder to make the service available to these subscribers.

For a sample on the JUNOS forwarding interface, see *ou = routers, retailerName = SP-THMA, o = Users, o = umc*.

For a sample on the JUNOS provider edge interface, see *ou = subscribers_pelf, retailerName = SP-THMA, o = Users, o = umc*.

For a sample on the JUNOS subscriber interface, see *ou = subscribers_subrIf, retailerName = SP-THMA, o = Users, o = umc*.

For information about configuring services and assigning scopes, see *SDX Services and Policies Guide, Chapter 1, Managing Services*. For information about adding subscribers, see *SDX Subscribers and Subscriptions Guide, Chapter 8, Configuring Subscribers and Subscriptions*.

4. Create service subscriptions for subscribers. In the sample data, we create a subscription at the folder level to allow all subscribers in the folder to inherit the subscription. Configure the subscriptions to manually activate the service through the Threat Mitigation Portal.

For a sample implementation, see *serviceName = BlockAttack, retailerName = SP-THMA, o = Users, o = umc* in the sample data.

For information about configuring subscriptions, see *SDX Subscribers and Subscriptions Guide, Chapter 8, Configuring Subscribers and Subscriptions*.

Classifying Subscribers and Interfaces

To apply policies to the forwarding interfaces, you configure additional entries in the subscriber classification and interface classification scripts. For general information about classifying subscribers and interfaces, see *SDX Subscribers and Subscriptions Guide, Chapter 4, Classifying Interfaces and Subscribers*.

Example: Subscriber Classification Scripts

In the subscriber classification script, threat mitigation requires the assignment of a subscriber profile for the forwarding interface and for any interface other than the forwarding interface (such as the provider edge interface on the JUNOS routing platform).

The Threat Mitigation Application needs to identify subscriber sessions in which to activate services persistently. These subscriber sessions should have a login name so that subscriber entries in the directory can be shared among the managed routers or interfaces. The login name must be unique. We recommend using the interface name and virtual router name to construct a unique login name. The login name must end in `@ <retailer's domain >` and must not contain a `/` (slash) or another `@` (at sign).

```
[routerName=commonRouterProfile,ou=routers,retailername=SP-THMA,o=Users,o=UMC?loginName=<-virtualRouterName.replace("@", "_")+@thma"->??]
# host subscriber for JUNOS routers
interfaceName=="FORWARDING_INTERFACE"
```

This subscriber classification for the forwarding interface sets the virtual router name as the login name and thma as the service provider's domain name. The domain name must match the value of the Retailer Domain field specified when configuring the Threat Mitigation Portal. See *Configuring the Threat Mitigation Portal* on page 119.

```
[uniqueID=DefaultTHMASubscriber,ou=subscribers,retailername=SP-THMA,o=Users,o=UMC?loginName=<-interfaceName.replace("@", "_").replace("/", "_")+ "_" +virtualRouterName.replace("@", "_")+@thma"->??]
# anything that is not the forwarding interface uses default subscriber
interfaceName!="FORWARDING_INTERFACE"
```

This subscriber classification for the provider edge interface sets the interface name as the login name.

To view the subscriber classifications referenced in this section, see $l = THMA$, $l = SAE$, $ou = staticConfiguration$, $ou = Configuration$, $o = Management$, $o = umc$ in the sample data.

Example: Interface Classification Scripts for JUNOS Routing Platforms

An entry is needed in the interface classification script to specify the default policy for forwarding interfaces and provider edge interfaces on the JUNOS routing platforms. For example:

```
[policyGroupName=default,ou=forwardingInterface,ou=thma,o=Policies,o=UMC]
# manage router interface for mirroring
interfaceName=="FORWARDING_INTERFACE"
```

```
[policyGroupName=default,ou=peInterface,ou=thma,o=Policies,o=UMC]
# manage interfaces with an alias indicating
# an enterprise customer
interfaceName!="FORWARDING_INTERFACE"
```

To view the interface classifications referenced in this section, see the interface classification for the THMA < number > routers listed under $o = Network$, $o = umc$ in the sample data.

Example: Interface Classification Scripts for JUNOSe Routers

An entry is needed in the interface classification script to specify the default policy for subscriber interfaces on the JUNOSe routers. For example:

```
# generic PPP users
[policyGroupName=default,ou=subInterface,ou=thma,o=Policies,o=UMC]
pppLoginName!=""

# define DHCP interfaces here
[policyGroupName=DHCP,ou=junose,ou=sample,o=Policies,o=umc]
# all fastEthernet interfaces
interfaceName="fastEthernet*"
```

To view the interface classifications referenced in this section, see the interface classification for $orderedCimKeys = THMA_JUNOSE$, $o = Network$, $o = umc$ in the sample data.

Managing Threats with the Threat Mitigation Portal

The Threat Mitigation Portal provided with the SDX software is designed to be used with the sample data for the Threat Mitigation Application. The Threat Mitigation Portal is a Web application that lets you use a Web browser to manage threats.

Once you have configured and deployed the Threat Mitigation Application, you can use the Threat Mitigation Portal to manage attack events. See *Installing and Initially Configuring the Threat Mitigation Application* on page 108.

Overview of the Threat Mitigation Portal

When the NetScreen-Security Manager reports incidents to the Threat Mitigation Portal, the Threat Mitigation Portal:

- Provides a description of the incident, including source IP address, destination IP address, attack type, severity, time of first received record, time of last received record, count of repeated attacks, and possible actions.
- Allows the administrator to choose how to handle the threat in the appropriate manner by taking action, activating or deactivating a service, or managing an action already taken.
- Displays general information if the SDX software cannot collect information about an attack type because it is not defined in the ATTACK_TYPE table.

About the Record Servlet

The record servlet receives messages from the SDX **thm.py** script that runs in NetScreen-Security Manager. The SDX **thm.py** script posts messages to a specified URL. The default pathname in the URL is `/thmp/record`. For information about changing the default pathname, see *Configuring the Threat Mitigation Portal* on page 119.

NetScreen-Security Manager sends the following information from its XML schema to the record servlet for display in the Threat Mitigation Portal.

- `dayId`—Date of the record as displayed in the Attack ID column to the left of the colon.
- `recordId`—Identifier for the record as displayed in the Attack ID column to the right of the colon.
- `timeReceived`—Time the attack event is received as displayed in the First Received Time and Last Received Time columns.
- `subCategory`—Subcategory of the attack as displayed in the Attack Type column.
- `srcAddr`—Source address of the attack as displayed in the Source column.
- `dstAddr`—Destination address of the attack as displayed in the Destination column.

- severity—Severity of the attack as displayed in the Severity column.
- repeatCount—Number of occurrences of the attack as displayed in the Repeat Count field.

The record servlet maps an attack ID with an attack type and its defining attributes (including protocol, source address, source port, destination address, destination port, user, application, uri). If the servlet receives more than one record for the same attack type with the same defining attribute values, the servlet stores the record with that attack ID once and increases the value of Repeat Count for that attack ID by one for each subsequent occurrence. The record servlet also records the highest severity of all attacks with the same defining attribute values and updates the last received timestamp.

If applicable, the Threat Mitigation Portal displays the following information in the Attack Details page.

- category—Category of the attack; displayed in the Attack Type field.
- subCategory—Subcategory of the attack; displayed in the Attack Type field.
- srcAddr—Source address of the attack; displayed in the Source field.
- srcDns—The result of a reverse DNS lookup on the source address of the attack; displayed in the Source DNS field as a comma-separated list.
- srcPort—Source port of the attack; displayed in the Source Port field.
- dstAddr—Destination address of the attack; displayed in the Destination field.
- dstDns—The result of a reverse DNS lookup on the destination address of the attack; displayed in the Destination DNS field as a comma-separated list.
- dstPort—Destination port of the attack; displayed in the Destination Port field.
- protocol—Protocol of the attack; displayed in the Protocol field.

For information about the SDX **thm.py** script that runs in NetScreen-Security Manager, see *Enabling SDX Actions from NetScreen-Security Manager* on page 135.

Configuring and Deploying the Threat Mitigation Portal

The Threat Mitigation Portal provided with the SDX software is designed to be used with the threat mitigation implementation in the sample data. To configure the Threat Mitigation Portal, see *Configuring the Threat Mitigation Portal* on page 119. To deploy the Threat Mitigation Portal, see *Deploying the Threat Mitigation Application* on page 120.

Using the NIC Resolver for the Threat Mitigation Portal

The Threat Mitigation Application pushes policies to the interfaces from which the problem traffic enters the network. To do so, the Threat Mitigation Portal must be able to map from a given attack source IP address to the SAEs managing the interfaces on the routers where that traffic enters the network. The Threat Mitigation Application uses the network information collector (NIC) to perform this mapping. Each service activation interface uses a different NIC configuration.

For information about the NIC configuration for each interface, see:

- JUNOS provider edge interface—Configuring the NIC for Provider Edge Interfaces on page 127
- JUNOS forwarding interface—Configuring the NIC for Forwarding Interfaces on page 128
- JUNOS subscriber interface—Configuring the NIC for Subscriber Interfaces on page 128

For more information about configuring the service activation interface, see *Configuring the Threat Mitigation Portal* on page 119.

Configuring the NIC for Provider Edge Interfaces

To configure the NIC to map the source IP address for a given attack to the SAEs managing the JUNOS subscriber-facing interfaces, use the `OnePopStaticRouteIp` configuration scenario and restart the NIC host. The `OnePopStaticRouteIp` configuration scenario resolves an assigned IP address for a subscriber whose traffic enters the network through an interface on a JUNOS routing platform to a reference for the SAE that manages the interface. The realm for this configuration accommodates the situation in which the network publisher component gathers interface information for the JUNOS routing platforms. The resolution process takes a subscriber's IP address as a key and returns a reference to the SAE that manages the interface. For information about configuring the NIC, see *SDX Network Guide: SAE, Juniper Networks Routers, and NIC, Chapter 5, Locating Subscriber Information*.

If you associate an existing address pool with an interface and you do not want to wait for this new information to be propagated based on the Cache Entry Age property of the NIC proxy or the Event Life Expectancy property of the agents, then you must manually clear the NIC proxy cache. To clear the NIC proxy cache when the application is deployed in a J2EE container that supports Java Management Extension (JMX) software, use the `NicProxyMgmt` MBean. Otherwise, you must restart the application or the application server. For information about modifying the NIC proxy cache properties, see *SDX Network Guide: SAE, Juniper Networks Routers, and NIC, Chapter 7, Configuring Applications to Communicate with an SAE*. For information about modifying the event life expectancy for agents, see *SDX Network Guide: SAE, Juniper Networks Routers, and NIC, Chapter 12, Reviewing the NIC Configuration*.

Configuring the NIC for Forwarding Interfaces

To configure the NIC to map the source IP address for a given attack to the SAEs managing the JUNOS forwarding interfaces, use the OnePop configuration scenario and restart the NIC host. The realm for the OnePop configuration scenario accommodates the situation in which IP address pools are configured locally on each VR. The resolution process takes a subscriber's IP address as the key and returns a reference to the SAE managing this subscriber as the value. For information about configuring the NIC, see *SDX Network Guide: SAE, Juniper Networks Routers, and NIC, Chapter 5, Locating Subscriber Information*.

Configuring the NIC for Subscriber Interfaces

To configure the NIC to map the source IP address for a given attack to the SAEs managing the JUNOS subscriber interfaces, use the OnePopAllRealms configuration scenario and restart the NIC host. The realm for the OnePopAllRealms configuration scenario accommodates the situations in which IP address pools are configured locally on each VR or IP address pools are shared by VRs in the same POP. The resolution process takes a subscriber's IP address as the key and returns a reference to the SAE managing this subscriber as the value. For information about configuring the NIC, see *SDX Network Guide: SAE, Juniper Networks Routers, and NIC, Chapter 5, Locating Subscriber Information*.

If the IP address pools are shared across multiple VRs, you must also configure an external plug-in for the SAE plug-in agent in the NIC host as follows:

```
Plugin.nic.objectref=corbaname::<host>:<port>/NameService#nicsae/saePort
```

- < host > is the name or IP address of the COS name server
- < port > is the TCP port

For information about configuring the SAE for external plug-ins, see *SDX Subscribers and Subscriptions Guide, Chapter 6, How to Configure SAE Plug-Ins*.

Accessing the Threat Mitigation Portal

To access the Threat Mitigation Portal:

1. In your Web browser, enter the name or IP address of the host and the port number on which you installed the Threat Mitigation Application in the format:

```
http(s)://<host>:<port>/thmp
```

A Connect to dialog box appears.

2. In the Connect to dialog box, enter your username and password, and click OK. The default values are:

```
User name—admin
Password—secret
```

The Threat Mitigation Portal appears.

The screenshot shows the Juniper Threat Mitigation Portal. At the top left is the Juniper Networks logo. Below it is a dark blue header with 'Threat Mitigation Portal' and a 'Home' link. A navigation menu on the left lists: Home, Action Required, Start Pending, Stop Pending, and Action Taken. The main content area is titled 'Threat Mitigation Portal' and includes a welcome message: 'Welcome to the Threat Mitigation Portal.' Below this are four links: 'Action Required Attacks', 'Action Start Pending Attacks', 'Action Stop Pending Attacks', and 'Action Taken Attacks'. There are two input fields: 'Display 20 attacks per page.' and a checkbox for 'Page refreshes every 30 seconds.' The Juniper yourNet logo is at the bottom right.

3. To modify the number of attacks displayed on each page from 20, enter the number in the Display attacks per page field.
4. To modify the page refresh rate, select the Page refreshes every 30 seconds check box, and enter the number of seconds in the text box.

You can manage the attacks that fall into these categories:

- Action Required—This page displays information about the attacks that require some action to be taken. See *Managing Attacks Requiring Action* on page 130.
- Start Pending—This page displays the attacks that are pending service activation. See *Managing Attacks Pending Service Activation* on page 131.
- Stop Pending—This page displays the attacks that are pending service deactivation. See *Managing Attacks Pending Service Deactivation* on page 132.
- Action Taken—This page displays the attacks for which some action was taken. See *Managing Attacks with Activated Services* on page 134.

The information provided about the attacks include attack ID, source and destination addresses, attack type, severity, first and last time the event was received, action that can be taken or action that was taken, and the time that the action was taken.

Managing Attacks Requiring Action

To manage attacks that require action to be taken:

1. In the Threat Mitigation Portal navigation pane, click Action Required.

The Action Required page displays all attacks that require action.


Action Required Attacks

Sorted By Ordered By

Attack ID	Source	Destination	Attack Type	Severity	First Received	Last Received	Repeat Count	Action 	
20051222:3	joe@thma	116.3.2.39	ICMP EXPLOIT FLOOD	major	Thursday, December 22, 2005 7:20:33 AM	Thursday, December 22, 2005 7:21:33 AM	32	<input type="text" value="Slow Attacker to 512kb/s"/>	<input type="button" value="Take Action"/> <input type="button" value="Delete"/>



The Attack ID is linked to the Attack Details page, which displays more information about the attack record.

The help button  provides information about the possible actions that can be taken in response to an attack. For example, the Help could recommend blocking the attack, blocking the attacker, or slowing the attacker.

2. To sort the attacks by a different category, select another category from the Sorted By drop-down list, and click Sort.
3. To sort the attacks in a different order, select the order from the Ordered By drop-down list, and click Sort.
4. To take action, select the action from the Action drop-down list, and click Take Action to update the state of the attack in that row and activate the service that represents the action to be taken.

If the attack is no longer in the same state as when you clicked Take Action, the action is aborted, and a message explains that the attack has been handled. Otherwise, the result depends on whether the service is activated.

- If a service is activated, the attack is moved to the Action Taken page.
 - If a service is waiting to be activated, the attack is placed in a pending state and appears in the Start Pending page.
5. To delete the attack, click Delete in the row for the attack.

Managing Attacks Pending Service Activation


To manage attacks waiting for service activation:

1. In the Threat Mitigation Portal navigation pane, click Start Pending.

The Start Pending page displays all attacks whose status is pending due to service activation.


Service Start Pending Attacks

Sorted By Ordered By

Attack ID	Source	Destination	Attack Type	Severity	First Received	Last Received	Repeat Count	Action 	Last Failure Time	
20060512:65	jane@virneo.com	labsrv-net7.kanlab.jnpr.net	TELNET USER ROOT	minor	Friday, May 12, 2006 11:28:58 AM	Friday, May 12, 2006 11:28:58 AM	1	Slow Attacker to 512kb/s	Friday, May 12, 2006 12:07:01 PM	<input type="button" value="Cancel"/> <input type="button" value="Force Cleanup"/>

Juniper yourNet

The Attack ID is linked to the Attack Details page, which displays more information about the attack record.

The help button  provides information about the possible actions that can be taken in response to an attack. For example, the Help could recommend blocking the attack, blocking the attacker, or slowing the attacker.

2. To sort the attacks by a different category, select another category from the Sorted By drop-down list, and click Sort.
3. To sort the attacks in a different order, select the order from the Ordered By drop-down list, and click Sort.
4. In the Service Start Pending Attacks table, you have the following options:
 - Click Cancel in a row to remove the attack from the Start Pending page and deactivate the service.

If the attack is no longer in the same state as when you clicked Cancel, the action is aborted, and a message explains that the attack has been handled. Otherwise, the result depends on whether the service is deactivated.

- If the service is deactivated, the attack is moved to the Action Required page.
- If the service is waiting to be deactivated, the attack is placed in a pending state and appears in the Stop Pending page. The Last Failure Time column indicates the time when the service deactivation was triggered.

- Click Force Cleanup in a row to delete the attack from the database.

You are responsible for ensuring that the service is deactivated. The Threat Mitigation Portal does not try to deactivate the service in this case.

- Click Retry in a row to manually reactivate the service.

If the attack is no longer in the same state as when you clicked Retry, the action is aborted, and a message explains that the attack has been handled. Otherwise, the result depends on whether the service is activated.

- If the service is activated, the attack is moved to the Action Taken page.
- If the service is waiting to be activated, the attack stays in the same state and continues to appear in the Start Pending page. The Last Failure Time column indicates the time when the service activation was triggered.

The Threat Mitigation Portal automatically tries to reactivate the service according to the configuration properties (see *Configuring the Threat Mitigation Portal* on page 119).

Managing Attacks Pending Service Deactivation


To manage attacks waiting for service deactivation:

- In the Threat Mitigation Portal navigation pane, click Stop Pending.

The Stop Pending page displays all attacks whose status is pending due to service deactivation.


Service Stop Pending Attacks

Sorted By Ordered By

Attack ID	Source	Destination	Attack Type	Severity	First Received	Last Received	Repeat Count	Action 	Last Failure Time	
20060512:63	null	labsrv-net7.kanlab.jnpr.net	TELNET USER ROOT	minor	Friday, May 12, 2006 11:15:47 AM	Friday, May 12, 2006 11:16:10 AM	2	Slow Attacker to 512kb/s 	Friday, May 12, 2006 12:13:01 PM	<input type="button" value="Cancel"/> <input type="button" value="Force Cleanup"/> <input type="button" value="Retry"/>



The Attack ID is linked to the Attack Details page, which displays more information about the attack record.

The help button  provides information about the possible actions that can be taken in response to an attack. For example, the Help could recommend blocking the attack, blocking the attacker, or slowing the attacker.

2. To sort the attacks by a different category, select another category from the Sorted By drop-down list, and click Sort.
3. To sort the attacks in a different order, select the order from the Ordered By drop-down list, and click Sort.
4. In the Service Stop Pending Attacks table, you have these options.
 - Click Cancel in a row to remove the attack from the Stop Pending page and activate the service.

If the attack is no longer in the same state as when you clicked Cancel, the action is aborted, and a message explains that the attack has been handled. Otherwise, the result depends on whether the service is activated.

- If the service is activated, the attack is moved to the Actions Taken page.
- If the service is waiting to be activated, the attack record is placed in a pending state and appears in the Start Pending page. The Last Failure Time column indicates the time when the service activation was triggered.
- Click Force Cleanup in a row to delete the attack from the database.

You are responsible for ensuring that the service is deactivated. The Threat Mitigation Portal does not try to deactivate the service in this case.

- Click Retry in a row to try to manually deactivate the service again.

If the attack is no longer in the same state as when you clicked Retry, the action is aborted, and a message explains that the attack has been handled. Otherwise, the result depends on whether the service is deactivated.

- If the service is deactivated, the attack is moved to the Action Required page.
- If the service is waiting to be deactivated, the attack record stays in the same state and continues to appear in the Stop Pending page. The Last Failure Time column indicates the time when the service deactivation was triggered.

The Threat Mitigation Portal automatically tries to deactivate the service again according to the configuration properties (see *Configuring the Threat Mitigation Portal* on page 119).

Managing Attacks with Activated Services


To manage attacks for which some action was taken:

1. In the Threat Mitigation Portal navigation pane, click Action Taken.

The Action Taken page displays all attack records whose status is action taken.


Action Taken Attacks

Sorted By Ordered By

Attack ID	Source	Destination	Attack Type	Severity	First Received	Last Received	Repeat Count	Action 	Action Taken Time	
20060404:33	joe@thma	hactar.kanlab.jnpr.net	ICMP EXPLOIT FLOOD	minor	Thursday, April 27, 2006 6:32:13 PM	Thursday, April 27, 2006 6:32:13 PM	1	Block Attack	Thursday, April 27, 2006 12:24:50 PM	<input type="button" value="Stop"/> <input type="button" value="Force Cleanup"/>
20051222:2	116.3.2.79	116.3.1.45	TROJAN AUTOPROXY INFECTED-HOST	critical	Thursday, December 22, 2005 7:20:57 AM	Thursday, December 22, 2005 7:20:57 AM	4	Block Attacker	Friday, December 30, 2005 11:46:35 AM	<input type="button" value="Stop"/> <input type="button" value="Force Cleanup"/>
20051222:1	116.3.1.22	116.3.3.193	FTP USER ROOT	minor	Thursday, December 22, 2005 7:18:58 AM	Thursday, December 22, 2005 7:19:58 AM	84	Block Attack	Wednesday, January 11, 2006 3:39:28 PM	<input type="button" value="Stop"/> <input type="button" value="Force Cleanup"/>



The Attack ID is linked to the Attack Details page, which displays more information about the attack record.

The help button  provides information about the possible actions that can be taken in response to an attack. For example, the Help could recommend blocking the attack, blocking the attacker, or slowing the attacker.

2. To sort the attacks by a different category, select another category from the Sorted By drop-down list, and click Sort.
3. To sort the attacks in a different order, select the order from the Ordered By drop-down list, and click Sort.
4. To cancel the action, click Stop in that row to update the state and deactivate the service that represents the action that was taken.

If the attack is no longer in the same state as when you clicked Stop, the action is aborted, and a message explains that the attack has been handled. Otherwise, the result depends on whether the service is deactivated.

- If a service is deactivated, the attack is moved to the Action Required page.
- If a service is waiting to be deactivated, the attack record is placed in a pending state and appears in the Stop Pending page.

5. To delete the attack, click Force Cleanup in the row for the attack.

You are responsible for ensuring that the service is deactivated. The Threat Mitigation Portal does not try to deactivate the service in this case.

Enabling SDX Actions from NetScreen-Security Manager

After you complete all the configuration in the SDX software, you configure the SDX **thm.py** script—a script that implements the messaging to record problem incidents and identifies the action for the SDX software to take. If the **thm.py** script cannot send an event to the Threat Mitigation Portal, it records the event in a file.

In a testing environment, you can use the **thm.sh** script to set up and troubleshoot a configuration that integrates NetScreen-Security Manager into an SDX-managed environment. The **thm.sh** script sets the library paths, redirects debugging output, and executes the **thm.py** script. Do not use the **thm.sh** script in a production environment.

The **thm.py** script requires Python version 2.3. The SMCpython package in the SDX software distribution contains Python version 2.3.

Before You Configure Scripts

Complete all other configuration for the Threat Mitigation Application.

Verify the location where Python is installed on the system. If you installed Python from the SDX software distribution, the default installation directory is */opt/UMC/python*. If you installed Python to a different directory, update the paths in *thm.py* and in *thm.sh* (if you use this file).

For a production environment, start NetScreen-Security Manager in an environment in which the library path includes the Python libraries.

Configuring Scripts

The **thm.py** script provides configuration properties to allow you to create customized implementations. You can locate the scripts in the */opt/UMC/conf/thma/scripts* directory.

To configure SDX scripts:

1. Edit the *thm.py* file to set the configuration properties. Use the field descriptions in the following list to complete the entries in this file.
2. Copy the *thm.py* file and the *thm.sh* file (if you use this file) to the appropriate directory for NetScreen-Security Manager. For the location of this directory, see the NetScreen-Security Manager documentation at

<http://www.juniper.net/techpubs/software/management/security-manager/>

RECORD_URL

- URL of the record interface for the Threat Mitigation Portal that stores information received from NetScreen-Security Manager. The interface records information about detrimental traffic in the ATTACK table in the database. The security rules configured in NetScreen-Security Manager determine the type of incidents recorded.
- Value—URL in the form “http(s):// < user > : < password > @ < host > : < port > /thmp/record”
 - < user > —Client ID
 - < password > —Password associated with the client ID
 - < host > —Hostname or IP address of the server on which the Threat Mitigation Portal runs
 - < port > —Port number used by the Threat Mitigation Portal on the server
- Guidelines—Enclose the URL in quotation marks because this entry is a Python string.
- Default—RECORD_URL = “http://admin:secret@127.0.0.1:8080/thmp/record”
- Example—RECORD_URL = “https://admin:secret@192.0.2.25:8443/thmp/record”

FAIL_DIR

- Pathname to the directory that records incidents that were not successfully sent to the record URL.
- Value—Pathname in the form “ < pathname > ”
- Guidelines—Enclose the pathname in quotation marks because this entry is a Python string.
- Default—FAIL_DIR = “failedEvents”

FAIL_FILE_LIMIT

- Maximum number of events that will be recorded in the fail directory. If this number is exceeded, the oldest event is deleted to make room for the most recent event. If this number is 0, the script will not add any failed events, check the fail directory for failed events, or spawn the daemon process.
- Value—Integer in the range 0–2147483647
- Default—FAIL_FILE_LIMIT = 100

NUM_RETRIES

- Number of times the script (and daemon process) will retry sending an event to the record URL if the first attempt fails. If the retry limit is reached, the script gives up and writes the event to the fail directory. If the retry limit is reached by the daemon process, it stops trying to send failed events until its next interval. For example, if NUM_RETRIES is 2, then the script will try at most 3 times to send an event to the record URL.
- Value—Integer in the range 0–2147483647
- Default—NUM_RETRIES = 2

DAEMON_INTERVAL

- Amount of time that the daemon process will take between attempts to send events to the fail directory. When first started, the daemon process will wait this number of seconds before trying to send events recorded in the fail directory. If it fails to send any event in the fail directory, it will not try to send any more events for this amount of time.
- Value—Number of seconds in the range 0–604800 (1 week)
- Default—DAEMON_INTERVAL = 30

DEBUG

- Specifies whether or not to print debugging messages.
- Value
 - True—Print messages.
 - False—Do not print messages.
- Guidelines—Set this value to True only for troubleshooting. Set this value to False to minimize the effects on performance.
- Default—DEBUG = True

SEND_XML

- Specifies whether or not to send attack log events to the Threat Mitigation Portal as an XML document.
- Value
 - True—The attack log event is sent to the Threat Mitigation Portal as an XML document.
 - False—The script parses the XML document and posts the relevant data as individual request parameters.
- Guidelines—Set this value to True to minimize CPU resources consumed by this script. Set this value to False to minimize the CPU resources used by the Threat Mitigation Portal in recording the attack. Setting this value to False will cause the script to consume approximately 60% more CPU resources.
- Default—SEND_XML = False

BACKGROUND_LOG_FILE

- Name of the file that logs messages for the process that retries sending attack log events. This file is created in the directory specified by FAIL_DIR.
- Value—Filename in the form “ < filename > ”
- Guidelines—Enclose the filename in quotation marks because this entry is a Python string. Set this value to None for no background logging.
- Default—BACKGROUND_LOG_FILE = “thm.log”

BACKGROUND_LOG_FILE_LIMIT

- Maximum size of the background log file. If this number is exceeded, a sequence number is appended to the filename and a new log file is started.
- Value—Number of bytes in the range 0–2147483647
- Default—BACKGROUND_LOG_FILE_LIMIT = 50000