

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 *SRC 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*.
- **ACTION**—Contains information about the SRC services that are activated to respond to attacks. The administrator maintains this data. See *Configuring Actions in the Database*.
- **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*.
- **ATTACK**—Contains information about the attacks that are managed by the Threat Mitigation Application. The SRC-TMP displays this information on various pages, including the Attack Details page. For information about how the SRC-TMP displays the attributes, see *Overview of the Threat Mitigation Application*.

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.

