

Before You Install the Threat Mitigation Application

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

- The UMChma package installed with your SRC application library software.
- SRC-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.

