

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 your Net

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 SRC-TMP 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 SRC-TMP automatically tries to reactivate the service according to the configuration properties (see Configuring the Threat Mitigation Application).