

## Adding a Secure Access Cluster Overview

---

When you add a Secure Access cluster in NSM, you first add the cluster and then add each member. Adding a member is similar to adding a standalone device.

Secure Access clusters can be configured by the device administrator to operate in active/passive mode or in active/active mode. Clusters in active/passive mode are made up of a primary member and a secondary member. All traffic flows through the primary member. If the primary member fails, then the secondary member takes over.

In active/active mode, traffic is load-balanced across all cluster members. If one member fails, then load balancing takes place among the surviving members.

In active/active Network Connect (NC) deployments, we recommend that you do the following:

- Split the NC IP pool into node-specific subpools.
- Perform static route configuration on the backend router infrastructure in a coordinated fashion, with static routes to each subpool pointing to the internal IP address of the hosting cluster node as the next-hop gateway.



**NOTE:** The Secure Access device does not support a common IP address pool for NC for an active/active cluster.

---

The number of members permitted in a cluster depends on whether the cluster is configured in active/active mode or in active/passive mode. You can have no more than two cluster members in active/passive mode. In active/active mode you can have up to eight members.

Before you can activate a cluster member in NSM, the device administrator must have already created the cluster and added, configured, and enabled the physical cluster member. See the *Juniper Network Secure Access Administration Guide* for details on creating and configuring clusters.

Secure Access devices configured in a cluster must have a cluster object and member objects defined in the NSM before the Secure Access cluster nodes can be recognized by NSM. Nodes from this cluster that subsequently contact NSM will be represented by fully functional member icons in the Cluster Manager. Cluster members whose DMI agents do not contact NSM will be displayed in the NSM Device Monitor as unconnected devices.

Secure Access devices use member IDs to identify each cluster member object. When importing cluster members, the member ID is imported as part of the cluster.

To add a Secure Access cluster to NSM, first add the cluster object, and then add its members. You add cluster members one at a time, in a similar manner to adding standalone devices.



**NOTE:** Adding a cluster and adding a cluster member have no effect on the cluster itself. The cluster and cluster members must already exist.

---

Once a Secure Access cluster is managed by NSM, subsequent changes applied to the cluster by NSM will be synchronized by the cluster across all cluster members. Similarly, changes to a Secure Access cluster membership that occur through administrator action on the native device UI will be reflected back to NSM, and NSM will display the modified cluster.

You can add a Secure Access cluster from your existing network into NSM and import their configurations. Using the Add Device Wizard, you configure a connection between the management system and the physical device, and then import all device parameters.

- Related Topics**
- Adding a Secure Access Cluster with Imported Cluster Members
  - Creating and Applying a Secure Access Device Template
  - Promoting a Secure Access Device Configuration to a Template

---

Published: 2009-08-20