Juniper Networks

SA to MAG Series Hardware Upgrade Guide

Applicable for:
Secure Access Service

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
408-745-2000
www.juniper.net

Juniper Networks SNMP Monitoring Guide

Table of Contents

OVERVIEW

This document describes guidelines and procedures for properly upgrading older Secure Access devices to the new MAG Series devices, installed both as a standalone configuration or as an HA solution, either in a 2-node or multi-node cluster configuration.

Binary export from old device and binary import of configurations to the new device is the recommended way to transfer configuration and settings from old to new platform due to simplicity of the process. However, though the steps seem simple, there are steps that will need special attention for a successful hardware swap, which are noted in this document.

PREPARATION FOR UPGRADE

Listed below are necessary items for the migration preparation:

1. **Site assessment:** Ensure proper cooling and ventilation; and also ensure network between nodes that are to be clustered are in high bandwidth, low latency LAN type connection (see http://kb.juniper.net/kb26035).

2. **Hardware:** Ensure that hardware ordered are complete (chassis, blades, fans, PSU, hard drives, or kits). Also ensure to match serial numbers of the hard drives and the blades, incorrectly using a non-paired drives could cause bootup issues and could result in an RMA. (see http://youtu.be/nF-1KPk_ZoU).

3. **Licenses:** Needed licenses should be procured and ready, and whether you need to configure as license member in an Enterprise Licensing Server environment.

4. **Software:** MAG Series devices are delivered with 7.1R1.1 factory build, and so, determine what software version will be used for the new devices and upgrade accordingly.

5. **Configuration backup:** Prefer to backup the system.cfg and user.cfg binary files immediately prior to migration. IVS,cfg is not going to be usable for MAG Series as it does not support it.

6. **Configuration documentation:** Local settings that are mostly kept in system.cfg should be documented as these will need to be manually re-entered to the MAG Series device/s.

NOTES:

1. The process of converting an existing SA standalone or cluster devices to the equivalent MAG series devices involves manually entering some settings, such as networking and clustering parameters, so please make note of these settings.
2. If you are using IVS from the SA devices, you cannot move those IVS to the new MAG devices as IVS is not supported.
3. If you are converting a cluster, all MAG series devices to be put in cluster should have same version and build of software, and same hardware platforms e,g; SM-160/SM-160, SM-360/SM-360.
4. If you are using Active Directory or ACE authentication servers, there may be a need to recreate the AD computer objects for the new MAG series devices, and/or for ACE, to regenerate/re-import the SDCONF.REC file to the devices if authentication fails after import.
5. It is assumed during this migration that the replacement MAG Series devices will be installed in the same networks as the old SA devices it is replacing.

STEP-BY-STEP PROCEDURE

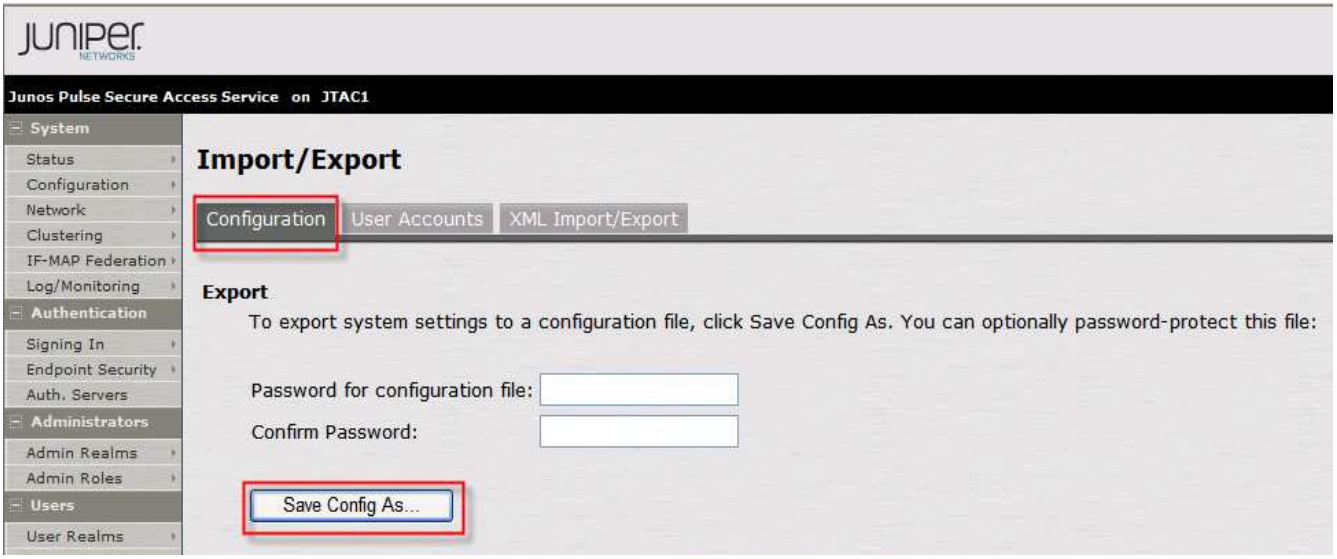
The below procedure applies to both standalone and cluster migration. The few major steps additional to clustering configurations are setting up Virtual Ports, mapping certificates to ports, setting up licensing client if using Enterprise Licensing server, and setting up NC profile.

Following are the steps for migration:

1. On the existing SA system, login to the standalone device or the primary node of the cluster (where the cluster was first formed) and export its binary configs (**system.cfg** and **user.cfg**).

   To export the binary configurations from the SA device:

   a. In the admin console, select **Maintenance** > **Import/Export** > **Configuration**.
   b. Under **Export**, enter a password if you'd like to password-protect the configuration file.
   c. Click **Save Config As** to save the file. By default, the filename will be **system.cfg**

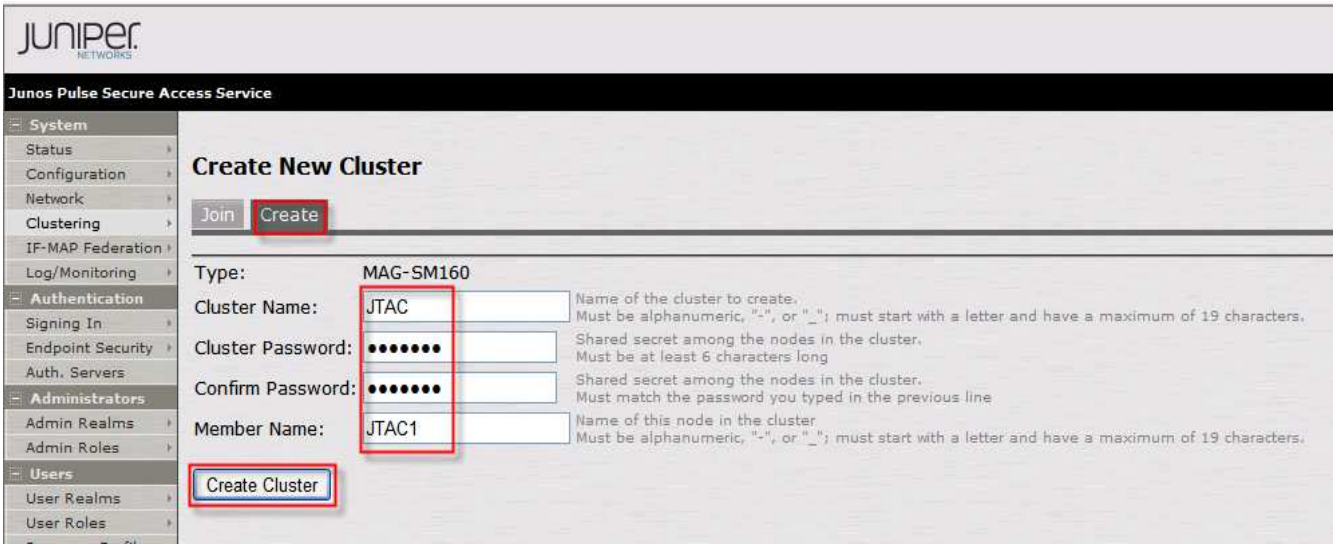


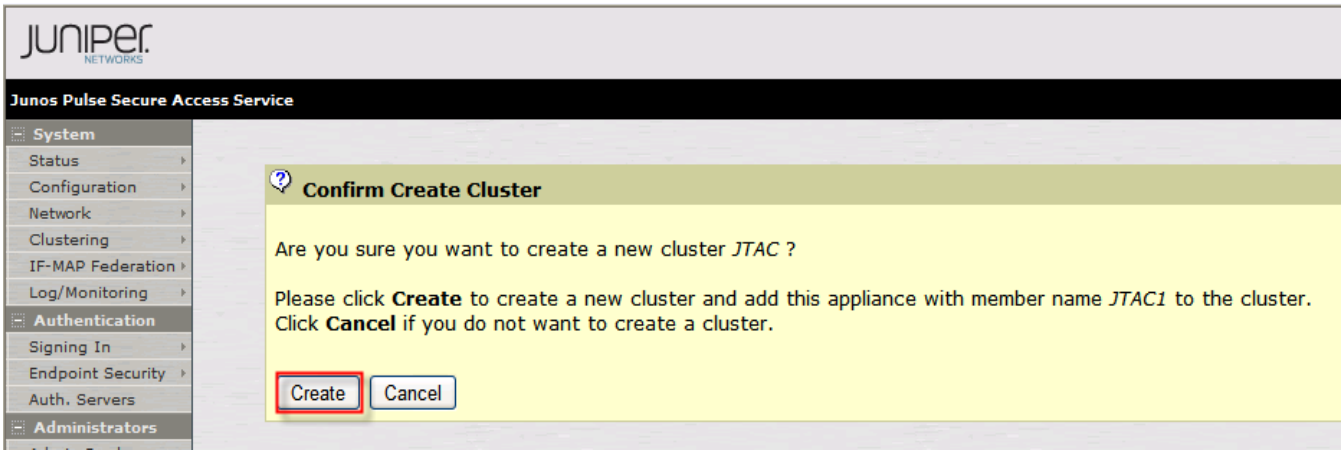
   d. In the admin console, select **Maintenance** > **Import/Export** > **User Accounts**.
   e. Under **Export**, enter a password if you'd like to password-protect the configuration file.
   f. Click **Save Config As** to save the file. By default, the filename will be **user.cfg**

2. Make notes of all the local settings for both nodes (if not yet done during preparation stage): **IP information, clustering, virtual ports, VLANs, hosts, routes, DNS settings, SNMP (if configured).**
3. Shutdown old SA cluster or standalone devices.
4. Configure the new MAG devices with same internal/external/management ports IPs with same IP addresses as the old SA devices and the proper DNS settings. Do not configure any other settings at this time.
5. Apply the proper licenses for the new MAG devices. If the SA is a member of an Enterprise License Server, you have to manually recreate the client and re-establish connection to the license server later at the end of migration.

   Note: If upgrading a non-clustered SA device, proceed to **Step 10**.

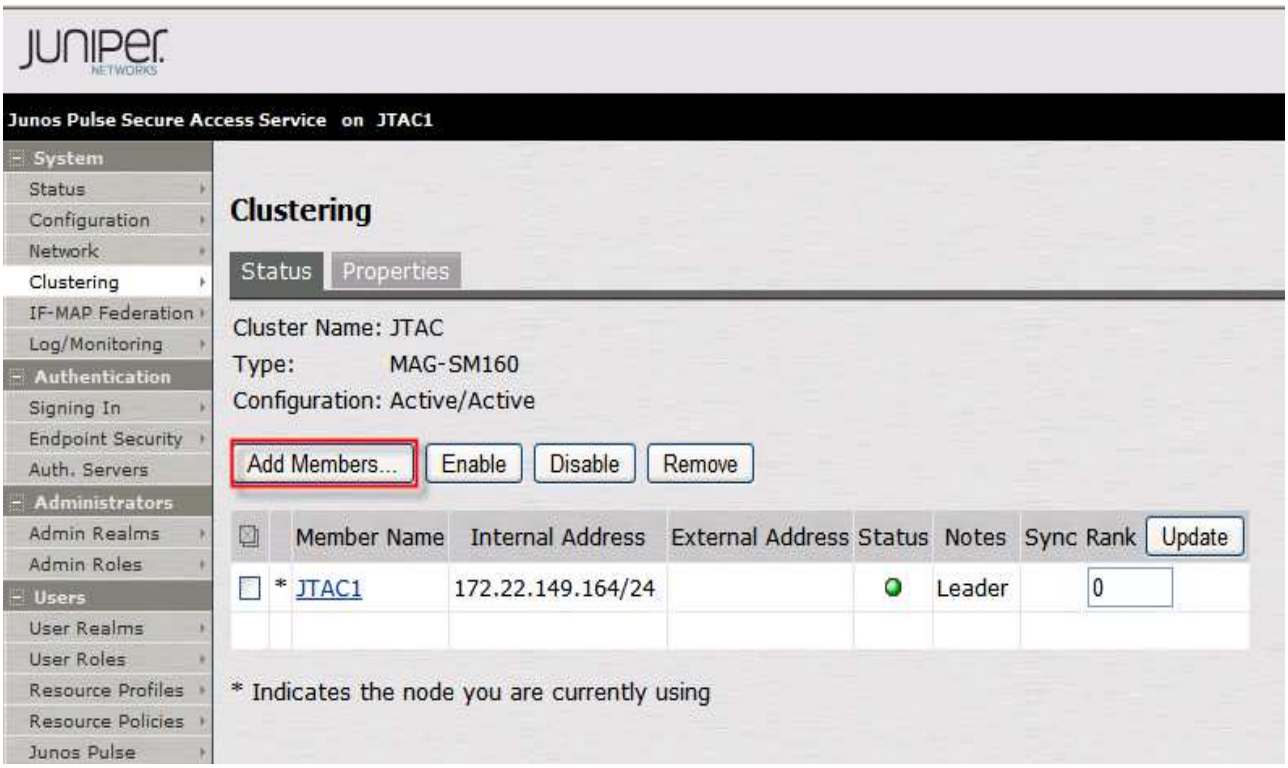
6. In the new MAG device (first device), manually create a new cluster with same name and settings as the old SA cluster (default new cluster is A/A mode, reset to A/P if needed and provide cluster VIP addresses).



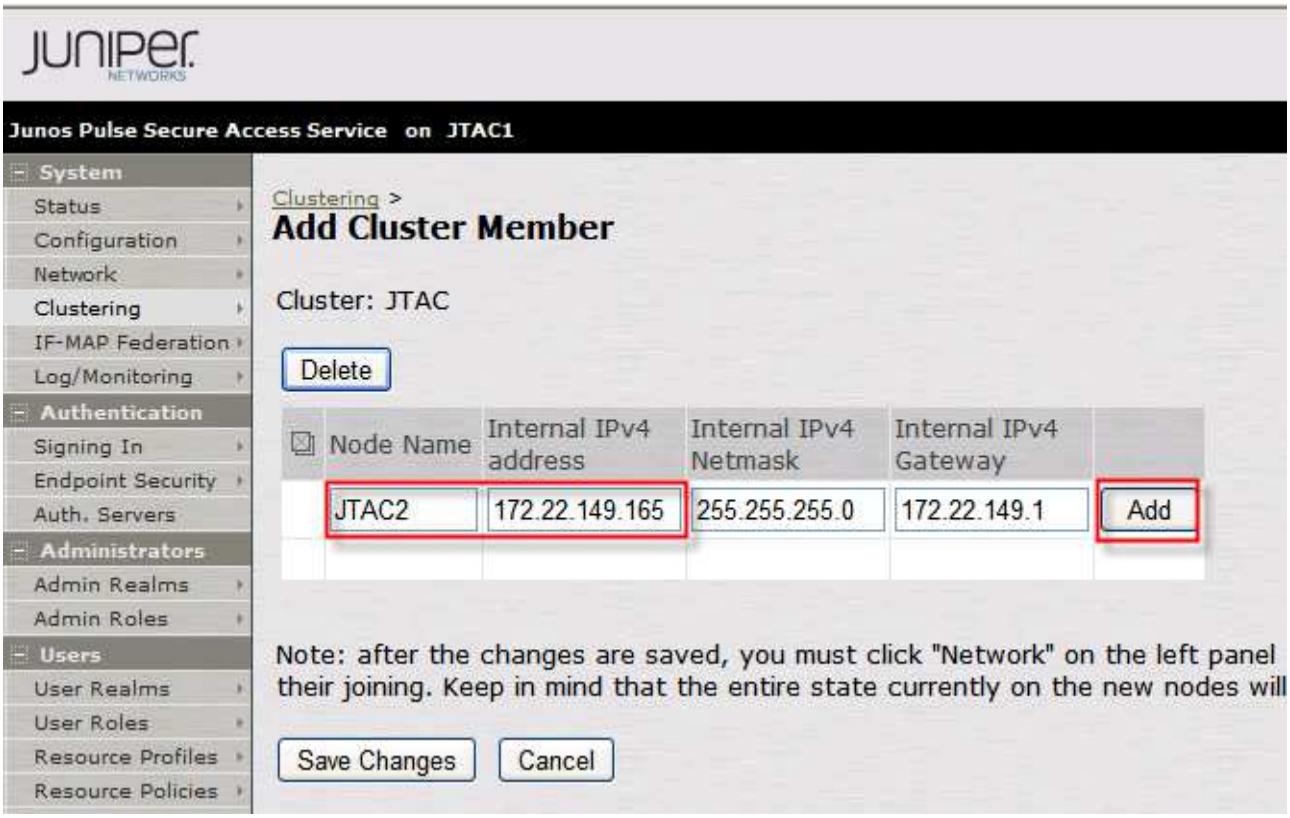


7. Add the second device to the cluster in the primary node cluster configuration and save the settings.

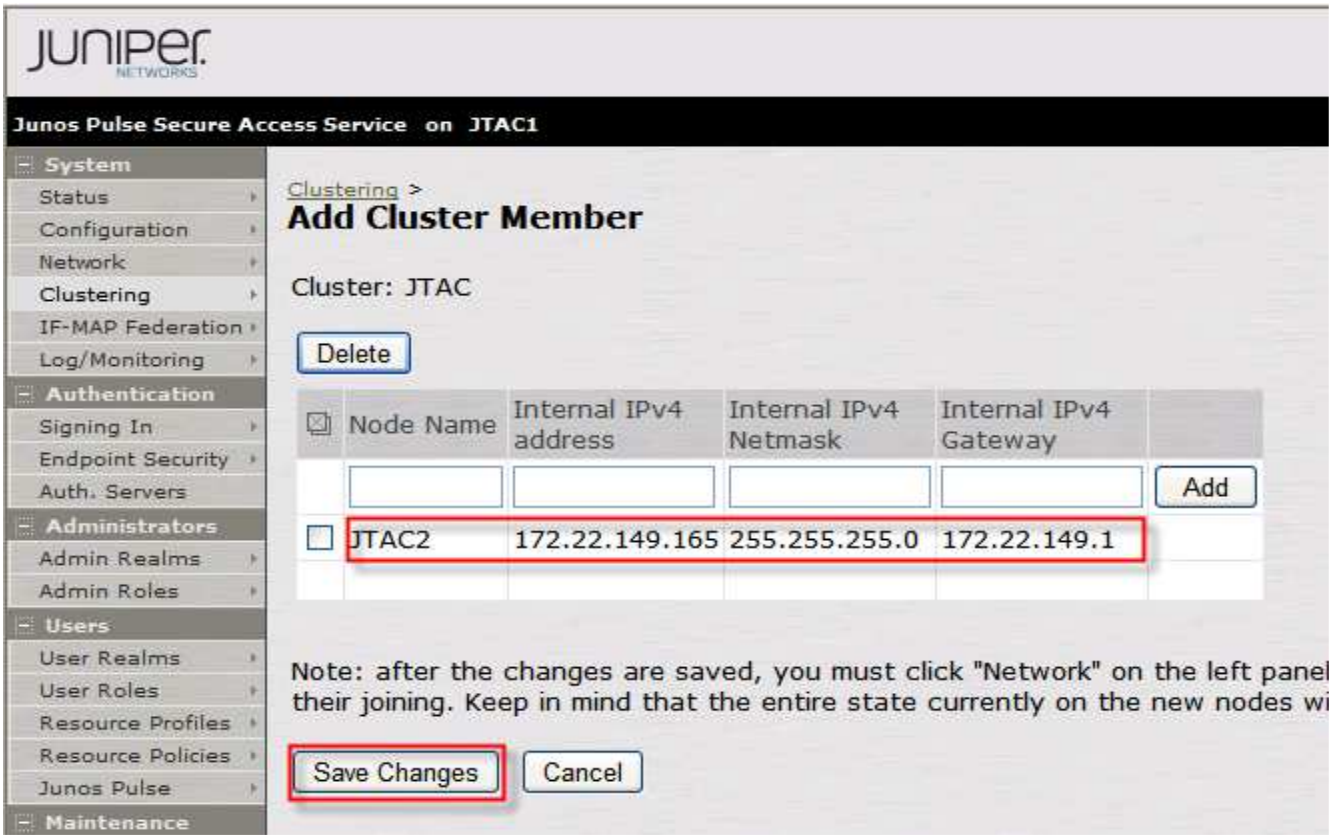
   Add a member by clicking **Add Members**:



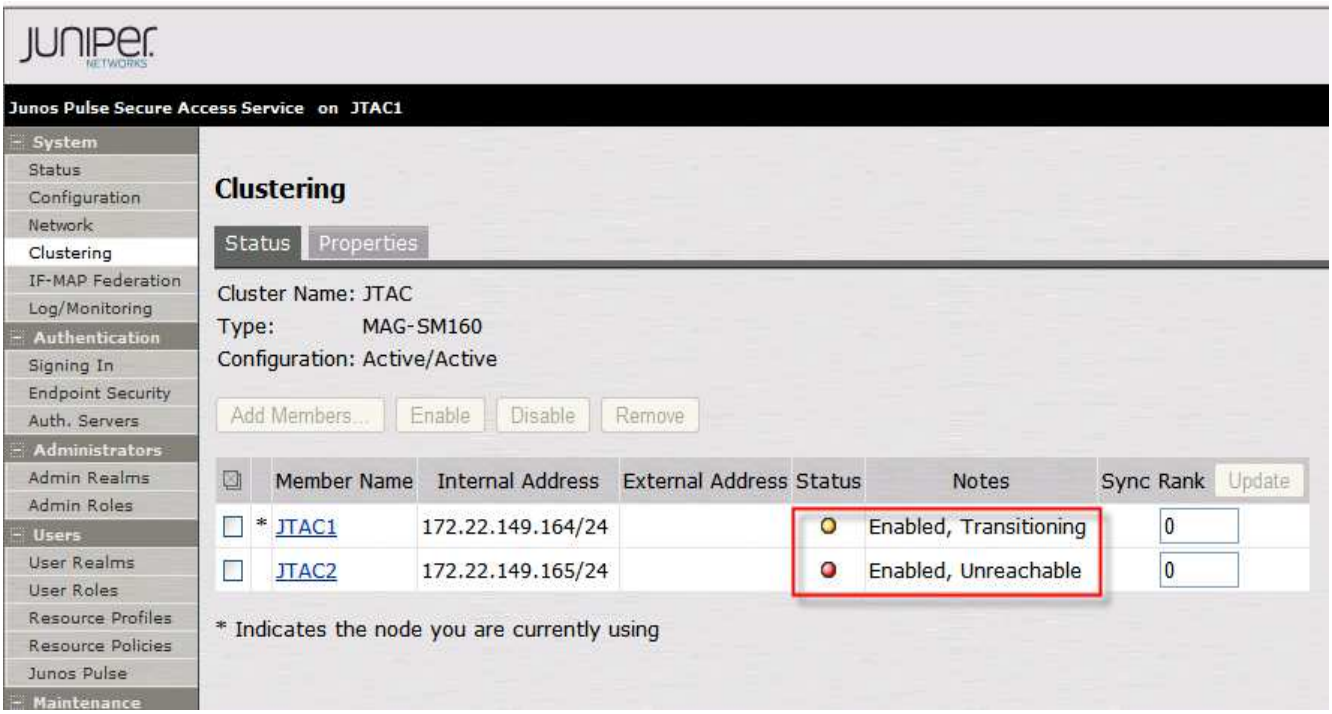
Enter member **node name** and **IP** and check **netmask** and **gateway**, then click **Add**:



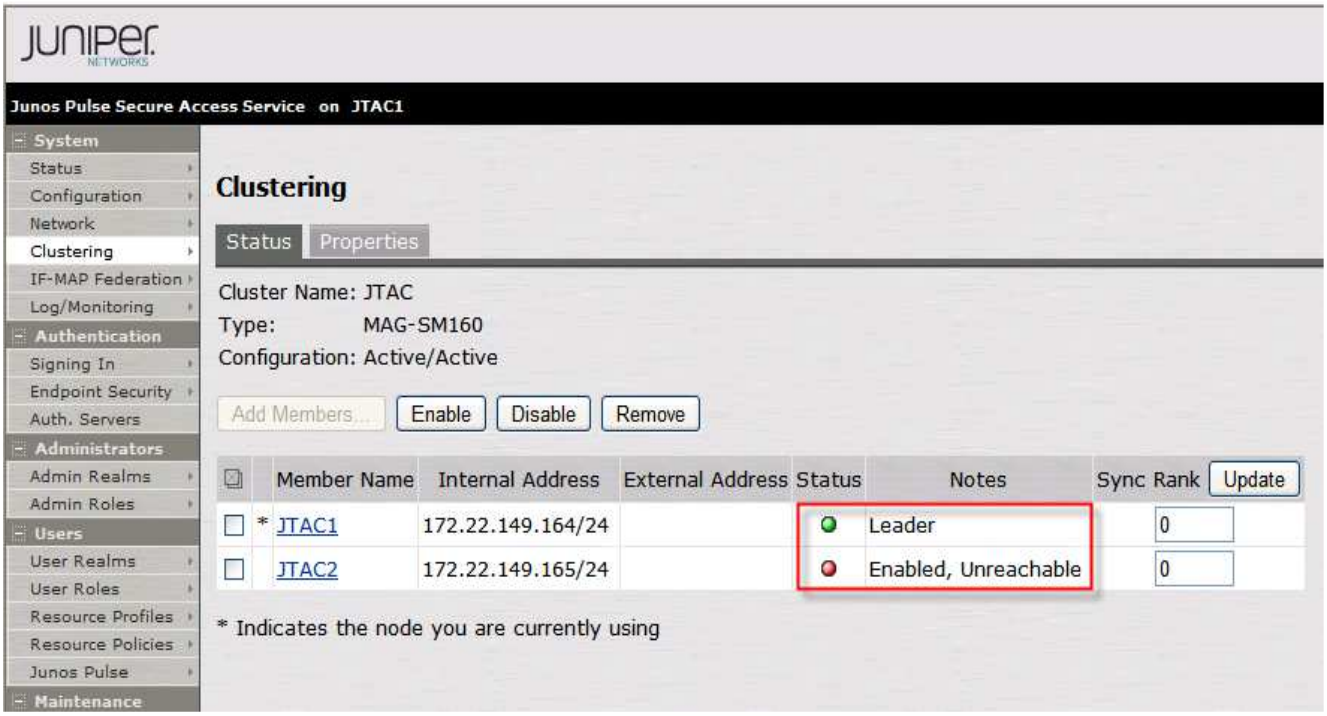
Save the changes by clicking **Save Changes**:



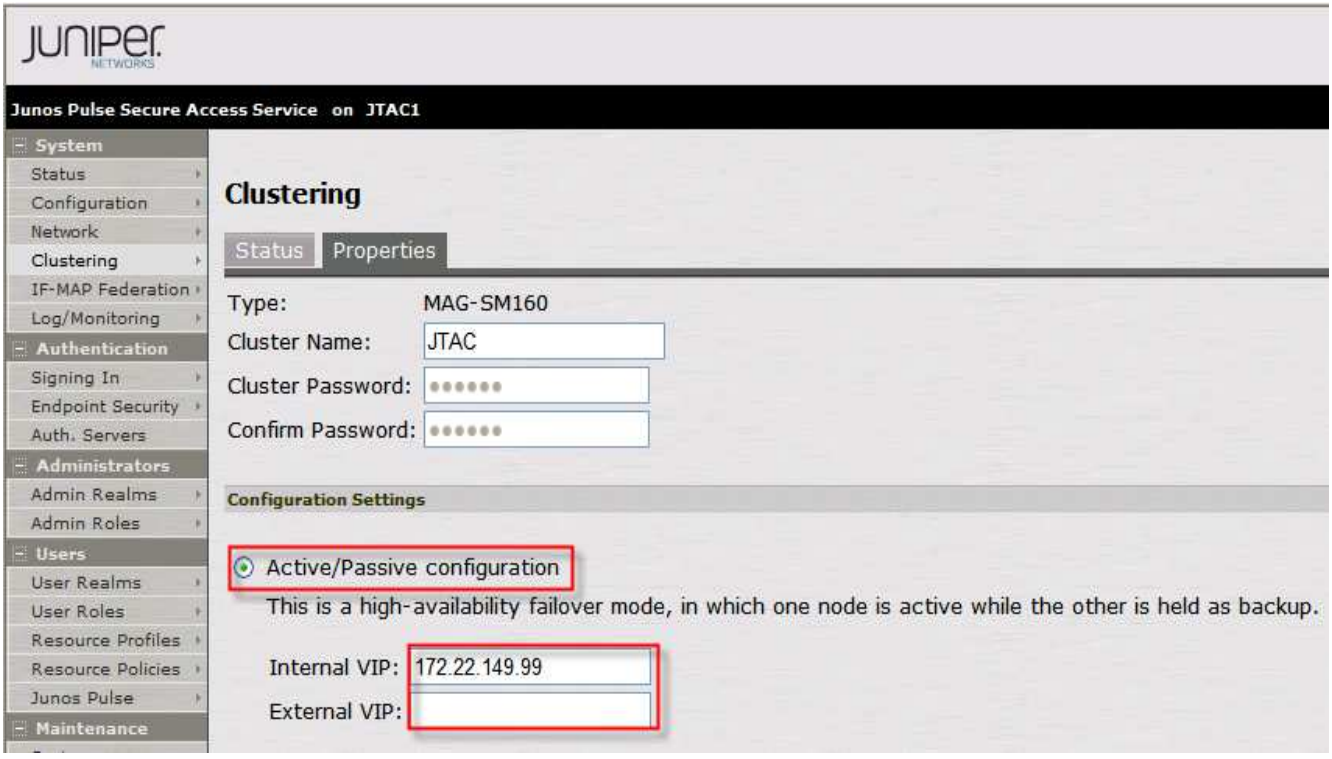
Check cluster **status**, it should go **transitioning** for short period:



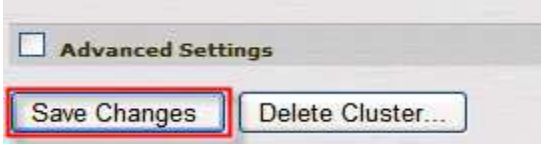
Then first node becomes enabled and status should be **Leader**, the second node remains **Enabled, Unreachable** until it joins the cluster:



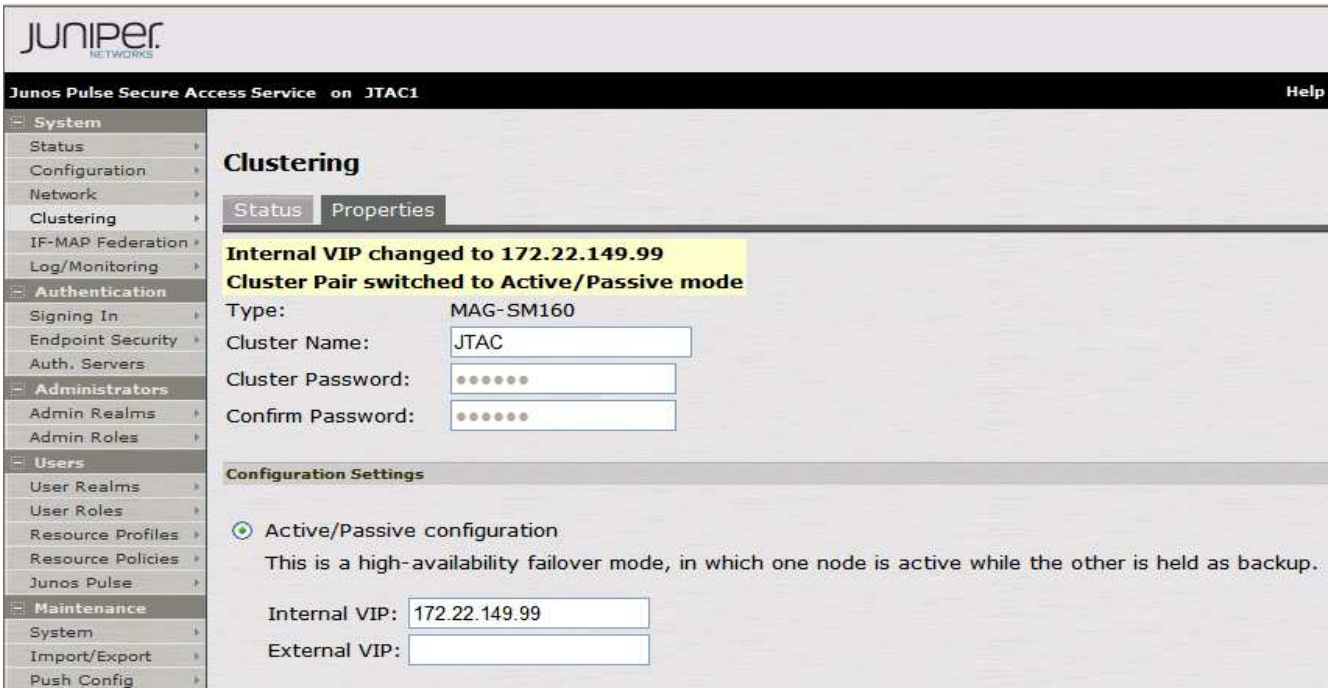
Change to A/P is needed by adding the cluster VIP address/es:



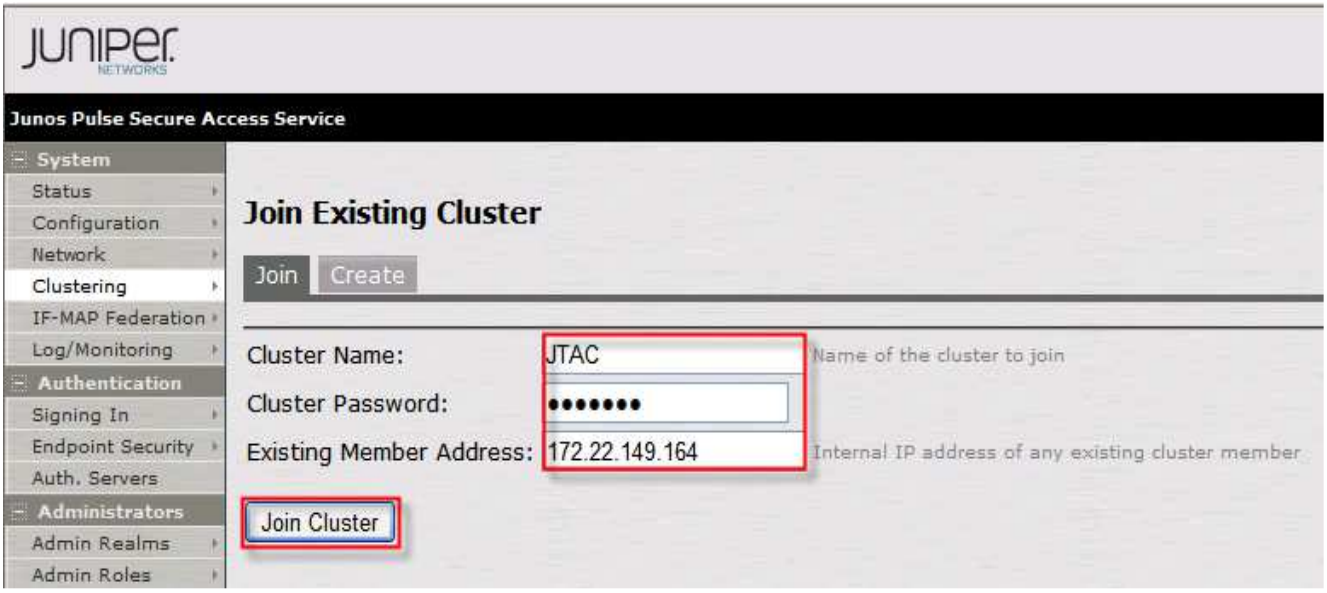
Save the cluster configuration settings:



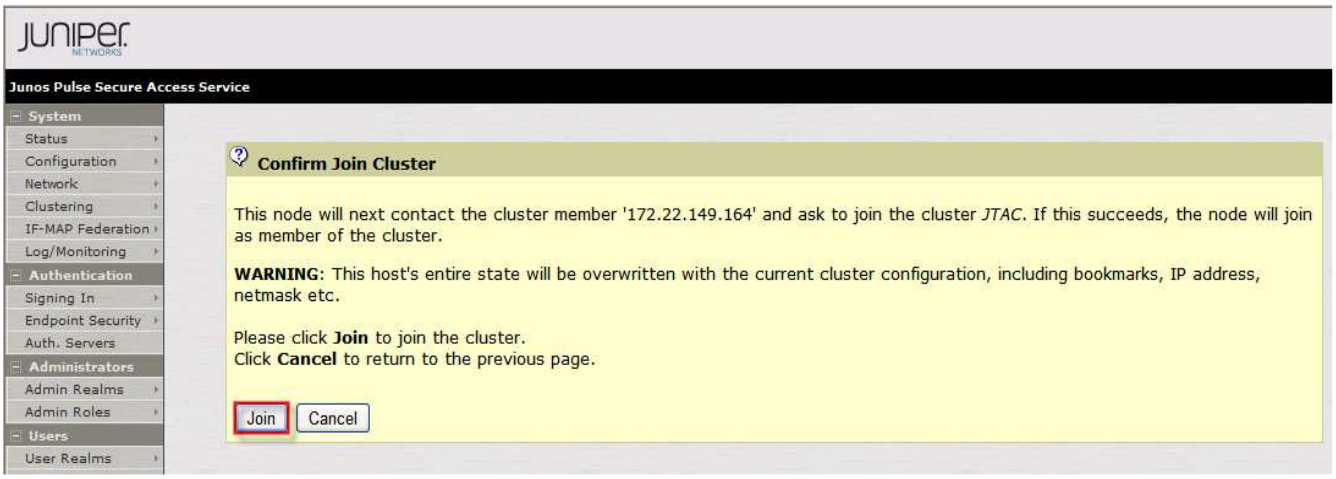
Change confirmation:



8. Login to the second MAG device and join this node to the cluster by **Clustering>Join Cluster**

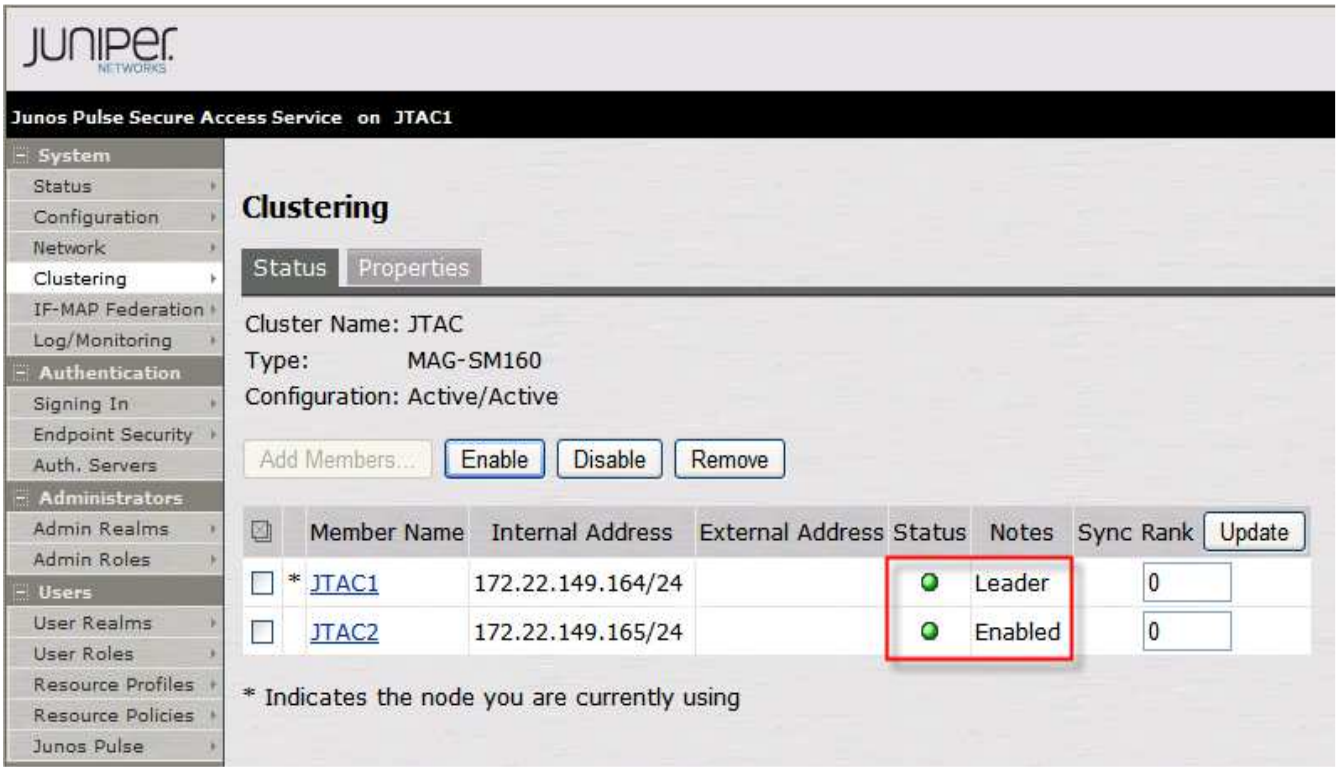


In confirmation page, click **Join**:



After successful join, admin session will be forced off the secondary node that just joined.

9. Login to primary node and check cluster status and it should stabilize in a few minutes.

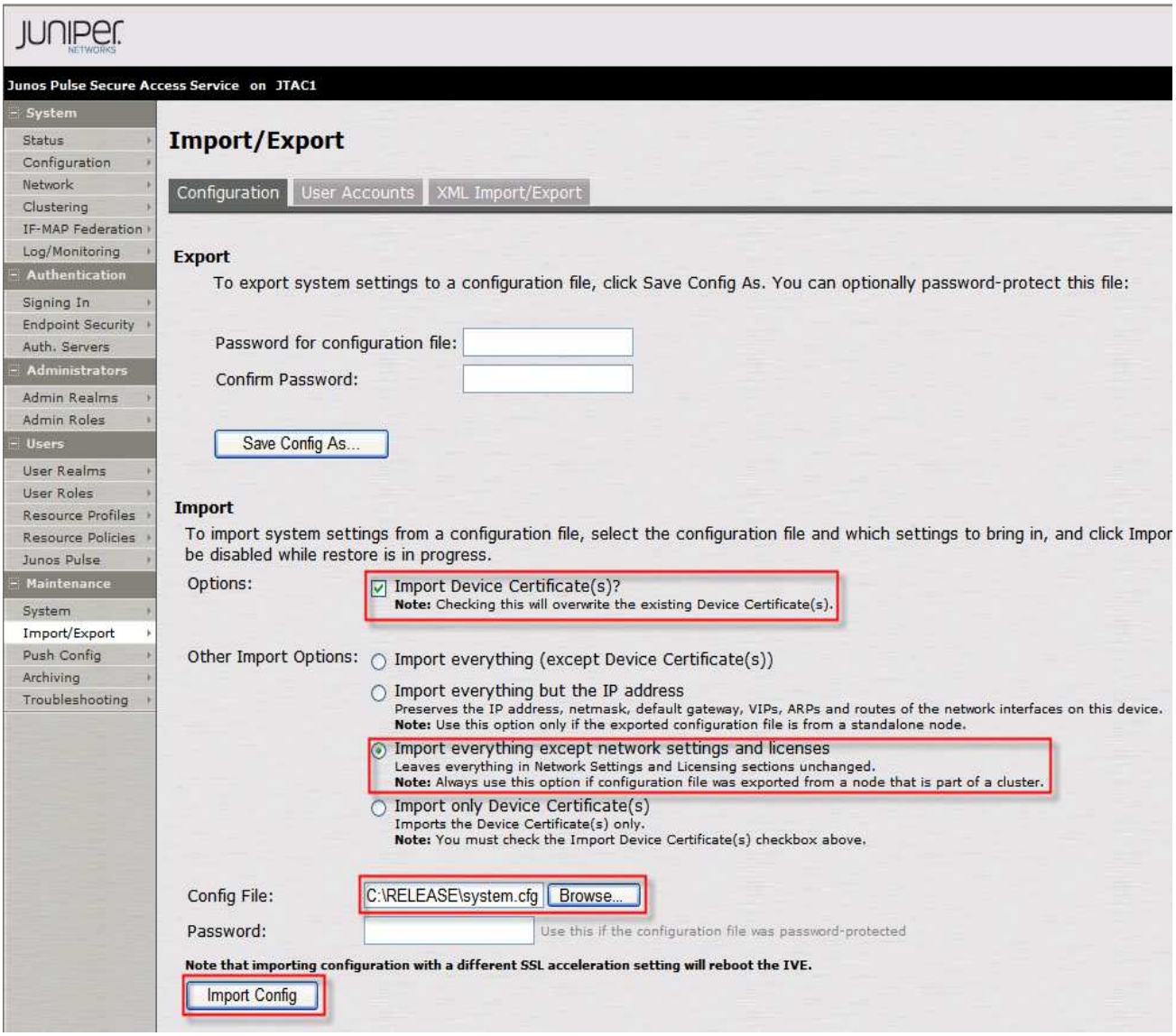


10. In the primary node of the new cluster, import the system.cfg (this is the same process in a standalone mode upgrade).

Note: This export process is the same for upgrading a standalone device)

To import the system configurations on the MAG device:

a. In the admin console, select **Maintenance** > **Import/Export** > **Configuration**.
b. Specify whether you want to import the Secure Access Service certificate. Note: The certificate is not imported unless you check the **Import Device Certificate(s)?** checkbox.
c. Select **Import everything except network settings and licenses** — This option imports all configuration settings except the network, cluster and license settings.
d. Browse to the configuration file, which is named **system.cfg** by default.
e. Enter the password you specified for the file. If you did not specify a password before exporting the file, then leave this field blank.
f. Click **Import Config**.

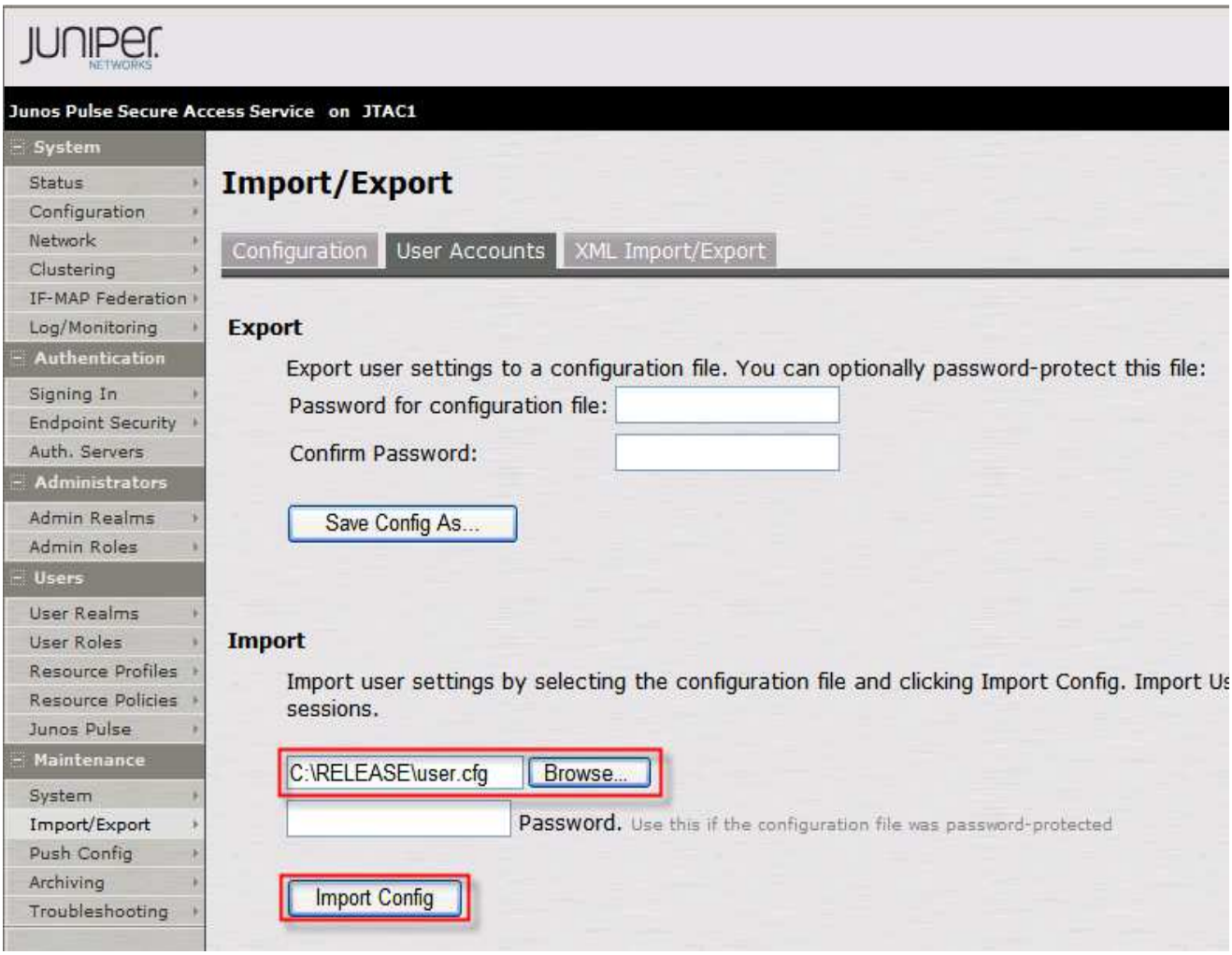


11. In the same primary node, import the user.cfg binary file.

To import the system configurations on the MAG device:

a. In the admin console, select **Maintenance > Import/Export > User Accounts**.
b. Browse to the configuration file, which is named **user.cfg** by default.

c. Enter the password you specified for the file. If you did not specify a password before exporting the file, then leave this field blank.
d. Click **Import Config**.



12. After importing system and user.cfg files, check and/or modify remaining local settings and other settings such as:

    a. **Network>Overview** settings (set in cluster or individual nodes)
    b. **Network>Routes** (for internal, external and other ports)
    c. **Network>Hosts** (set in cluster or individual nodes)
    d. **Network>Internal Port/ External Port>Virtual Ports** (if clustered, set this up in cluster "Entire Cluster")
    e. **Network>VLANs** (if clustered, set this up in cluster "Entire Cluster")
    f. **Nework>VPN Tunneling** (set in cluster or individual nodes)
    g. **Log/Monitoring>SNMP** (set in cluster or individual nodes)
    h. **Configuration>Certificates>Device Certificates** (and its ports bindings)
    i. **Resource Policies>VPN Tunneling>Connection Profiles** (if configured)
    j. **Auth Servers>**ACE Auth server, if used (check the node secret file status)
    k. **Configuration>Licensing** - License client-server settings (if used as license client in Enterprise Licensing Server environment), proper licenses installed

13. Check cluster status (if clustered) and test operation by logging in to the cluster VIPs (or the standalone MAG device IP). Test the authentication using AD, ACE, etc, and all other functionalities enabled, such as NC or Pulse.
14. This completes the hardware platform upgrade.

REFERENCES:

Junos Pulse Secure Access Service Administration Guide:

http://www.juniper.net/techpubs/software/ive/admin/j-sa-sslvpn-7.3-adminguide.pdf

Page 929: Clustering
Page 934: Defining and Initializing a Cluster
Page 935: Joining an Existing Cluster
Page 854: Importing and Exporting Secure Access Service Configuration Files

KB discussing supported network type for clustering:

http://kb.juniper.net/kb26035

MAG Series Devices Setup video:

http://youtu.be/nF-1KPk_ZoU