Junos Pulse Secure Access Cluster Upgrade

How-to

This document covers the required steps to upgrade an Active/Active (A/A) or Active/Passive (A/P) Junos Pulse Secure Access Cluster.

Table of Contents

Note: This document applies to SA OS 7.0 and above.

Step 1: Confirming a Supported Upgrade Path

In order to ensure configuration and user data integrity after the upgrade, we strongly recommend that you follow the supported upgrade path documented in the first Release Notes (R1) for that branch. In the first Release Note for every branch, there is a section titled "Upgrading to this Release" where you can find this information. Subsequent Release Notes will only list branch fixes and limitations. If you are upgrading from a release which is not listed, then please upgrade to one of the listed releases first before proceeding to your chosen branch. For example, if you are currently running 6.0R3.1 and you would like to upgrade to 7.1R2, you would need to check the Secure Access Release Notes for Release version 7.1R1.

Step 2: Downloading the Service Package

You can install a different service package by first obtaining the software from the Juniper Support Web site. Package files are encrypted and signed so that the SA Series Appliance server accepts only valid packages issued by Juniper Networks. This measure prevents the SA Series Appliance server from accepting Trojan horse programs.

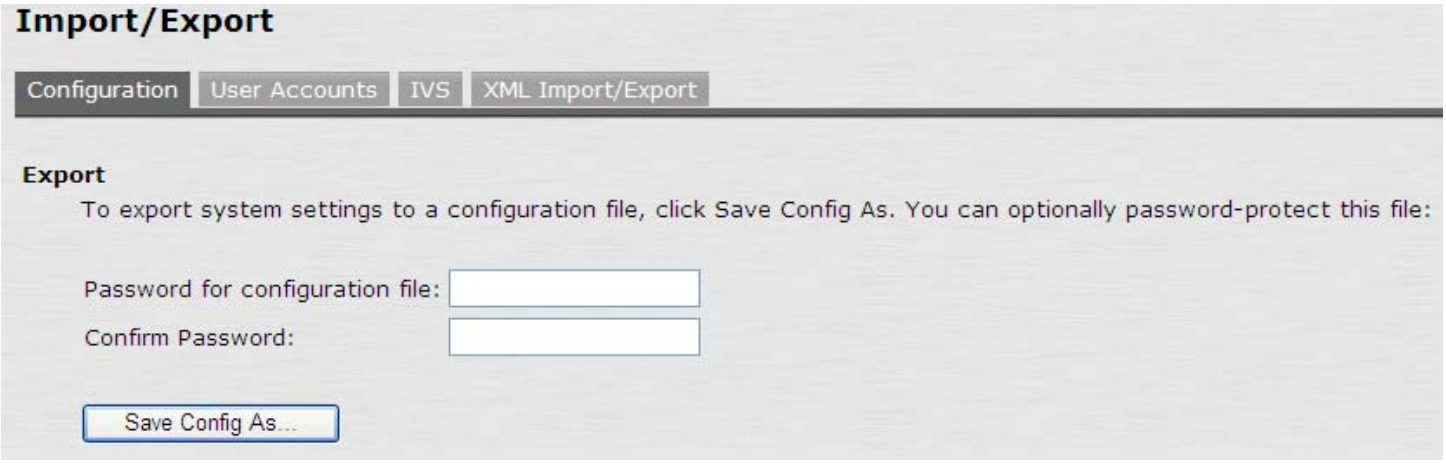
Step 3: Creating Backup Files

Before installing a new service package, please export your current system configuration, local user accounts, customized user settings, and role and policy information.

Step 3.1: Exporting a System Configuration File

Your System Configuration file contains Network, Cluster, License, and SNMP settings. To export an encrypted binary system configuration file:

1. In the admin console, choose **Maintenance > Import/Export > Configuration**.
2. Under **Export**, enter a password if you'd like to password-protect the configuration file.
3. Click **Save Config As** to create the **system.cfg** file.

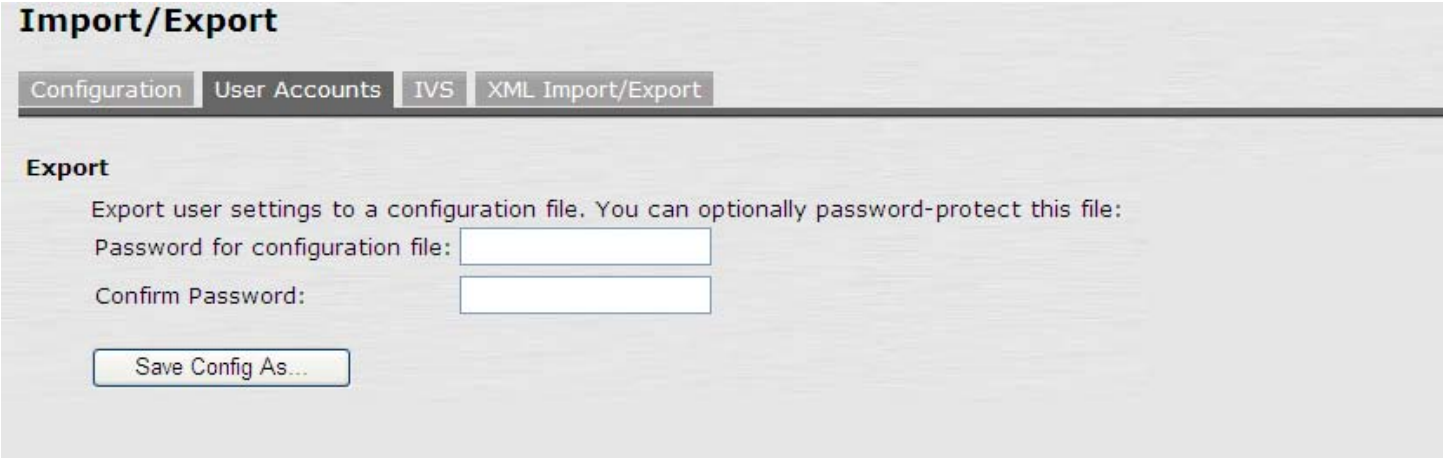


NOTE: When exporting an SA Series FIPS configuration file, note that information about the machine's security world or key store is included in the file. Therefore, you need an administrator card that is associated with the security world in order to successfully import the configuration file into another machine.

Step 3.2: Exporting a User Accounts File

The User Accounts file contains Sign in Settings (includes sign sing policies, sign in pages, and all authentication servers), Authentication Realms, Roles, Network Access, Resource policies, Resource Profiles, User accounts, and Meeting settings. To export an encrypted binary local user accounts file:

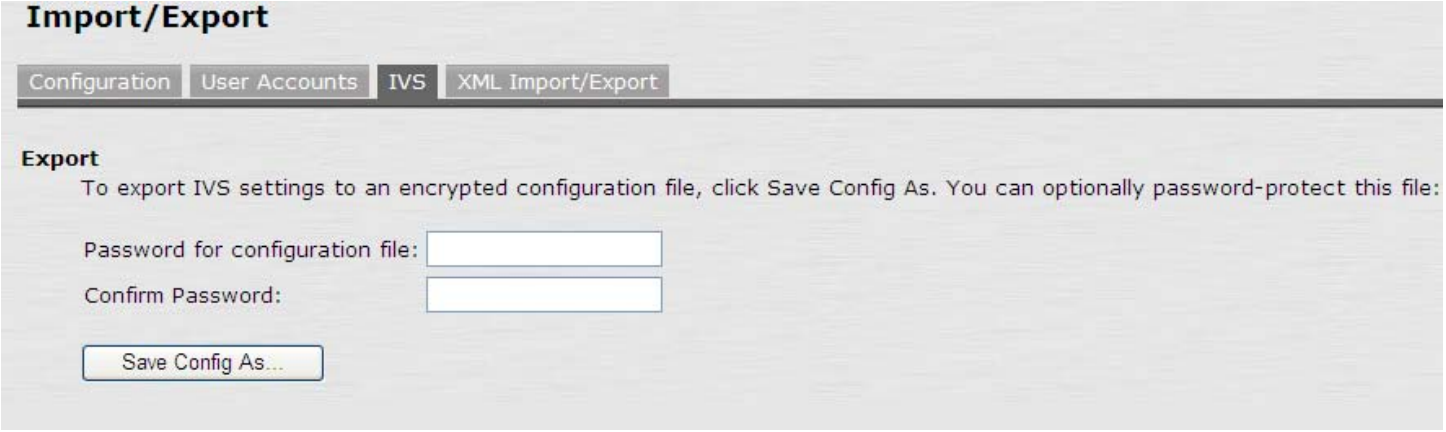
1. In the admin console, choose **Maintenance > Import/Export > Import/Export User Accounts**.
2. Under **Export**, enter a password if you'd like to password-protect the configuration file.
3. Click **Save Config As** to create the **user.cfg** file.



Step 3.3: Exporting an IVS Configuration File (Applies only to SA-x000 & x500 devices)

The Instant Virtual System (IVS) configuration file contains IVS Profiles, System, Authentication, Administrators, Administrators, Users, Resources Policies, and Maintenance settings. To export an encrypted binary IVS file:

1. In the admin console, choose **Maintenance > Import/Export > Import/Export IVS**.
2. Under **Export**, enter a password if you'd like to password-protect the configuration file.
3. Click **Save Config As** to create the **ivs.cfg** file.



Note: IVS is only available if you have an IVS license.

Step 4: Clearing your Logs

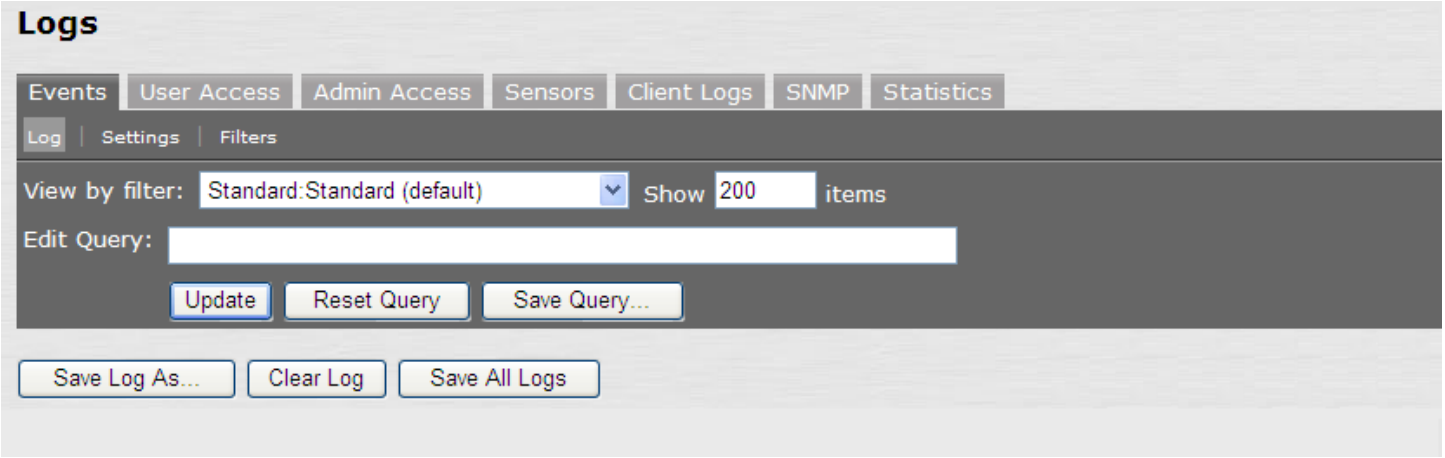
Installing a service package can take several minutes and requires the SA Series Appliance to reboot. Because existing system data is backed up during this process, you can decrease installation time by clearing your system logs before trying to install a service package. System log Files are text files stored on an SA Series Appliance to track system events. An SA Series Appliance produces an Events log, User Access log, Administrator Access log, Sensors log, Client Upload logs, and System Snapshot Files. These files will be preserved unless these files are deleted prior to upgrading.

Step 4.1: Deleting the System Log Files

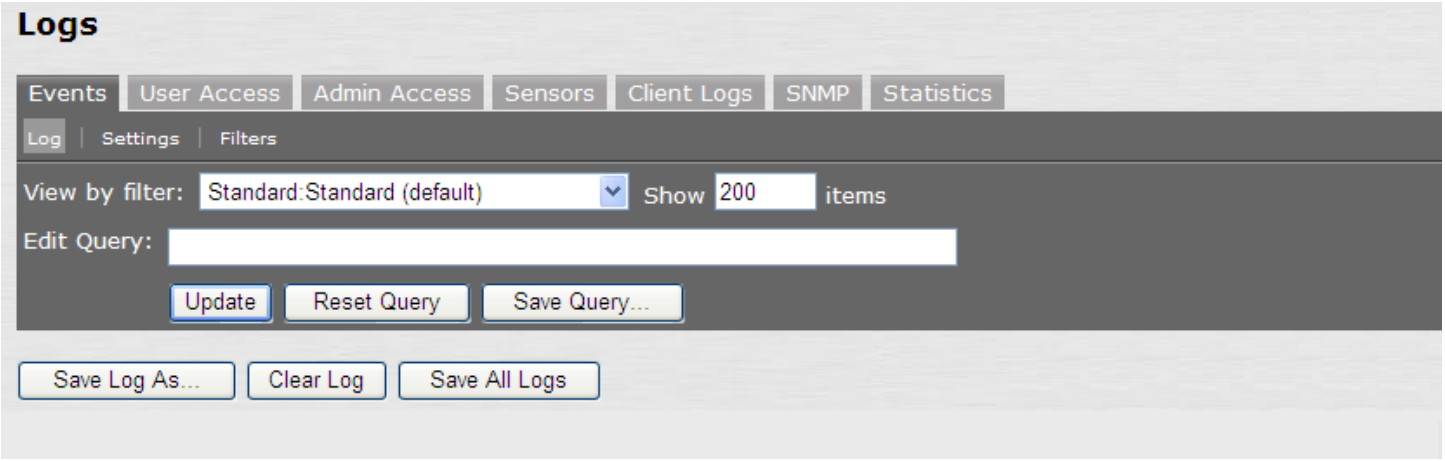
To delete the System Log Files:

1. In the admin console, choose **Log/Monitoring**.
2. Select **Events log**, **User Access log**, **Administrator Access log,** or **Sensors log**.
3. If you would like to save your System Logs before upgrading select **Save All Logs** to download your Events log, User Access log, Administrator Access log, and Sensors log in a single zip file.

4. Select **Clear Log**, and repeat for each remaining System Log.



5. Select **Clear Log**, and repeat for each remaining System Log.

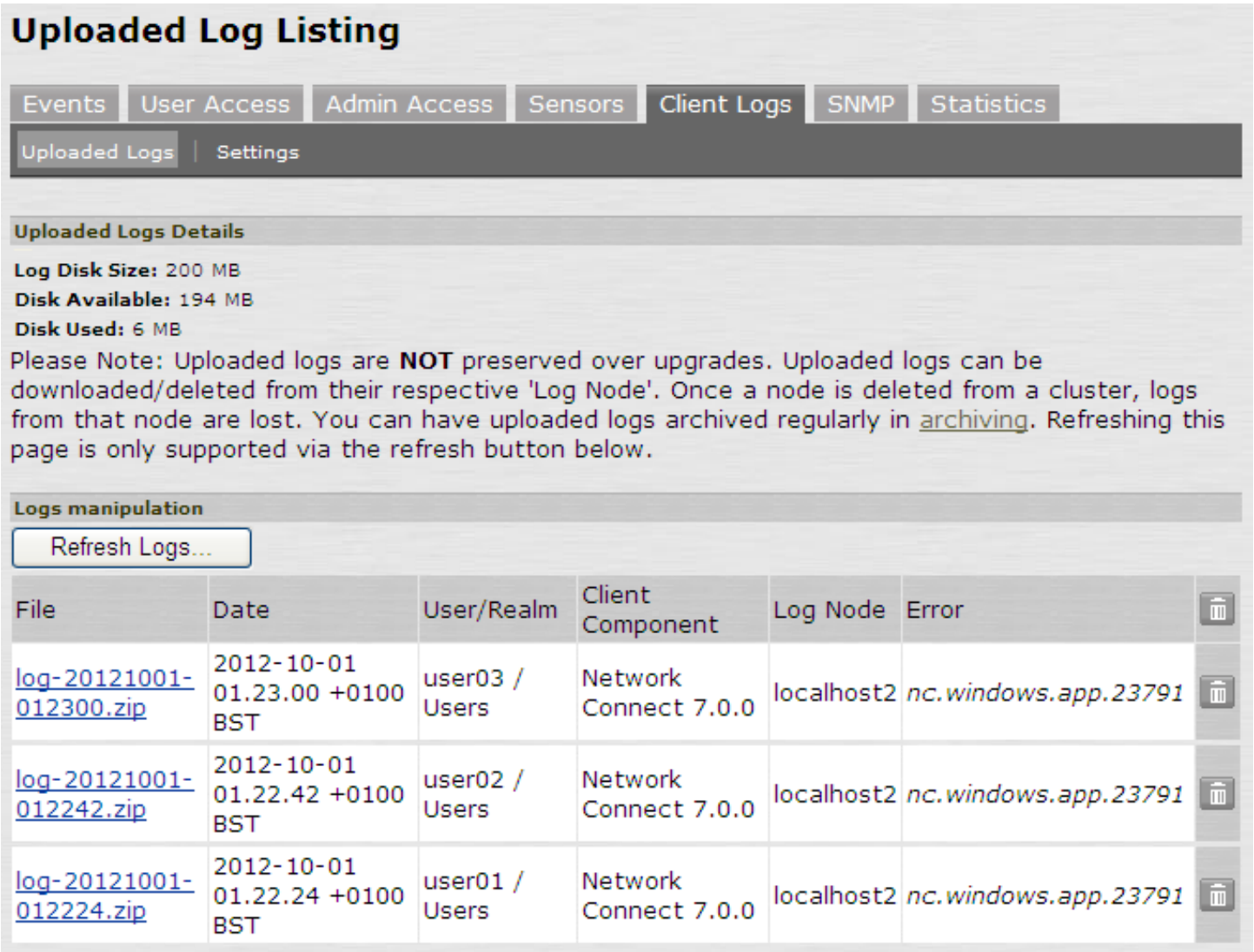


Step 4.2: Deleting the Client Upload logs

To delete the Client Upload logs:

1. In the admin console, choose **Log/Monitoring > Client Logs > Uploaded Logs**.
2. If you would like to save your Client Uploaded Logs before upgrading select **<Log-File-Name>.zip** to download each log file.

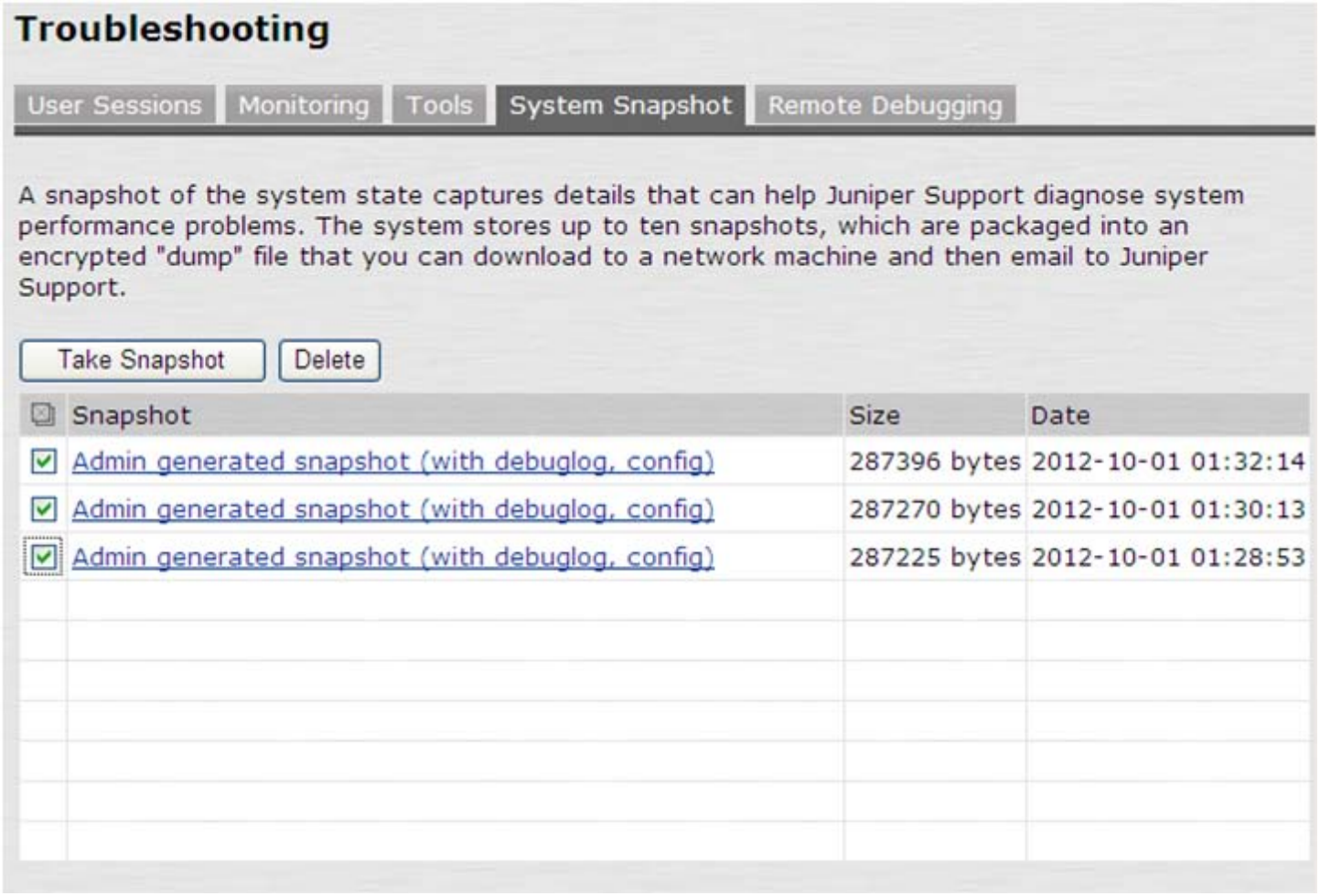
3. Select the **trash icon** to delete each file.



Step 4.3: Deleting the System Snapshot Files

To delete the System Snapshot Files:

1. In the admin console, choose **Maintenance > Troubleshooting > System Snapshot**.
2. If you would like to save your System Snapshot files before upgrading select **<Snapshot-File-Name>** to download each snapshot.
3. Put a check each snapshot file you would like to delete and choose **Delete.**



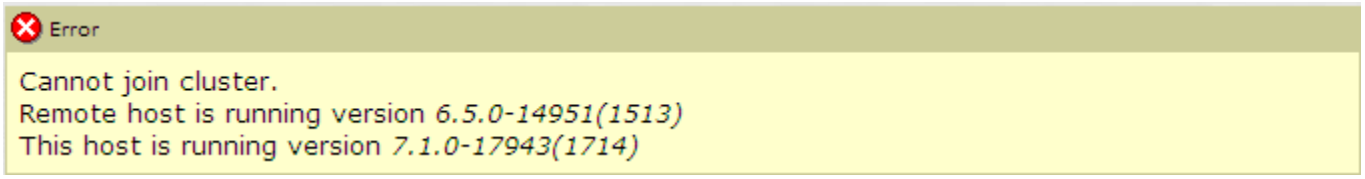
Step 5: Upgrading or Downgrading the Appliance

Note: Juniper Networks recommends to schedule a maintenance window when performing an upgrade or downgrade to a cluster. While each node is being upgraded, the SA device will transfer user sessions (core access, SAM, Network Connect or Junos Pulse) from one node to another. This will cause a short disconnect for SAM and Network Connect/Junos Pulse clients as these applications will automatically reconnect to the new node without any user interaction. Applications accessing resources through SAM and Network Connect/Junos Pulse will be required to automatically reconnect to the backend resources through the tunnel.

The SA Series Appliance offers the ability to easily upgrade every node in a cluster. When installation of a newer service package on one cluster node has completed, it will automatically push the service package to the rest of the cluster nodes.

If you disable or remove any cluster nodes, then upgrade the cluster, these devices will be automatically upgraded by the existing node in the cluster when they are re-enabled or re-joined to the cluster.

If you disable or remove any nodes and then roll back the cluster to an older version, the following error will be observed until the joining or disabled cluster members have also been rolled back or downgraded to same version or a lower version than what is already running on the Cluster.



In short, if the joining or disabled device is on a higher version than what is running on the cluster, then you will receive the error above when you try to re-enable or join it. If the joining member is on a lower version that what is running on the cluster, then it will be automatically upgraded by the existing cluster member once it is re-enabled or re-joined.

The admin console lets you install a new service package immediately or stage the service package. For clusters, we recommend you stage the service package at each cluster node, especially for “slower” networks. This reduces the upgrade time by allowing each node to upgrade simultaneously instead of having one node push the upgrade process to each of the other cluster’s nodes. Note, however, that the service package revision at the node where you first start the installation process overwrites the service package revision at the other cluster’s nodes if they are different.

For example, suppose you stage service packages at clusterNode1, clusterNode2 and clusterNode3. Now start the upgrade process on clusterNode3. The service pack revision on clusterNode1 is compared to clusterNode3. If it is different, then the service package on clusterNode3 is pushed to clusterNode1 before clusterNode1 starts its upgrade. If the revisions are the same, then clusterNode3 does not push its service package to clusterNode1. Similarly for clusterNode2.

Step 5.a: Install Service Package

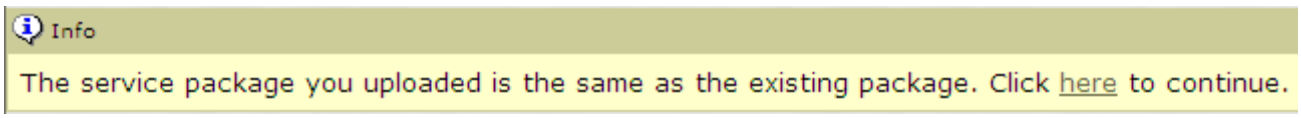
This feature is typically used to upgrade to newer versions of the system software, but you can also use this process to downgrade to a previous version or to delete all your current configuration settings and start from a “clean slate.” If needed, you may also roll back to a previous system state through the serial console or the web admin console.

To install a service package:

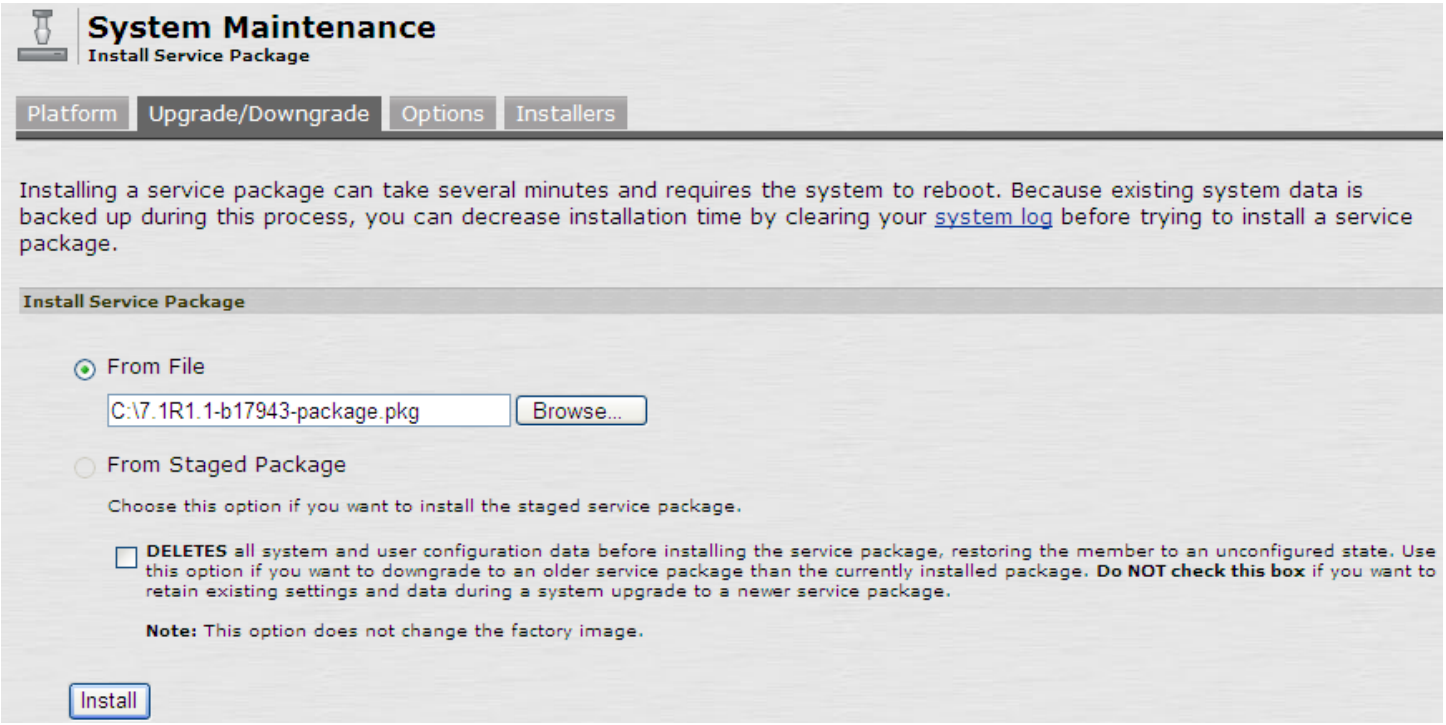
1. In the admin console, select **Maintenance > System > Upgrade/Downgrade**.
2. Under Section Install Service Package, select **Browse** to find the service package on your hard drive that you obtained from the Juniper Networks Customer Support Center.
3. Alternately, if you are downgrading to an older service package or deleting your configuration settings, you will need to select **Delete all system and user data**.

   WARNING: The option to **delete all system and user data** is only required if you are downgrading you’re an appliance to a version which is lower than the version which is currently running on your system. Selecting the option to **delete all system and user data** will restore your appliance to an un-configured state, and you will have to reestablish network connectivity before reconfiguring the system. **Do NOT check this box** if you wish to retain existing settings and data during a system upgrade to a newer service package. Please note that if your appliance is an SA Series FIPS, then choosing this option will delete your existing security world or key store, and also your certificates.

   Note: If you want to delete your current configuration settings but continue to use the same SA Series Appliance version, choose the service package that is currently installed on your appliance and select **Delete all system and user data**. If you do not choose **Delete all system and user data**, then you will receive the following error below:



4. Select the service package file and click **Install Now**.



Step 5.b: Manage Staged Service Package

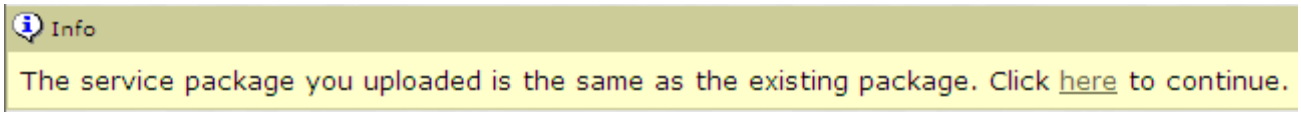
Staging lets you to push the package to a directory on the SA Series Appliance before the planned maintenance time and then install the package during the maintenance window. Note that staging does not provide the ability to schedule the installation of the stored service package. It only pushes the service package to the device without installing it. You must still manually start the installation process.

To install a service package:

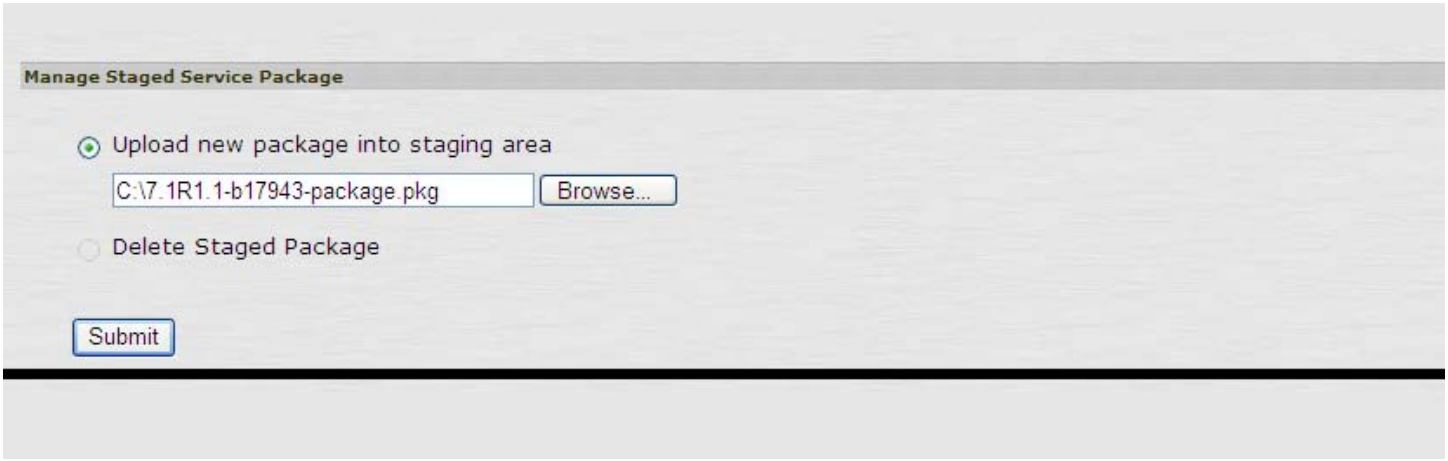
1. In the admin console, select **Maintenance > System > Upgrade/Downgrade**.
2. Under Section Manage Staged Service Package, select **Browse** to find the service package on your hard drive that you obtained from the Juniper Networks Customer Support Center.
3. Alternately, if you are downgrading to an older service package or deleting your configuration settings, select **Delete all system and user data**.

   WARNING: The option to **delete all system and user data** is only required if you are downgrading you're an appliance to a version which is lower than the version which is currently running on your system. Selecting the option to **delete all system and user data** will restore your appliance to an un-configured state, and you will have to reestablish network connectivity before reconfiguring the system. **Do NOT check this box** if you wish to retain existing settings and data during a system upgrade to a newer service package. Please note that if your appliance is an SA Series FIPS, then choosing this option will delete your existing security world or key store, and also your certificates.

   Note: If you want to delete your current configuration settings but continue to use the same SA Series Appliance version, choose the service package that is currently installed on your appliance and select **Delete all system and user data**. If you do not choose **Delete all system and user data**, then you will receive the following error below:



4. Select **Submit** to upload new package into staging area



NOTE: If you choose to revert to delete all system and user data from the appliance using this option, you will have to reestablish network connectivity before reconfiguring the system. Also note that you cannot roll back to a version lower than 3.1.

5. Under Section Install Service Package, select **From Staged Package <SA Version and Build>**.

Active/Passive scenario

Note: The term “passive node” used in this example to describe the node that does NOT own the VIP. Please check the VIP owner on **Clustering > Status** page.

To reduce the number of reconnection attempts due to VIP failover, Juniper Networks recommends to upgrade the passive node first. Once the upgrade is complete, the passive node will push the service package to the active node and cause the VIP to failover to the passive node. All existing user session will be automatically transferred to the

passive node. When the active node has completed the upgrade process, the passive node will remain the VIP owner. If you would like the active node to own the VIP again, a manual failover is required.

Juniper components will be upgraded only for new user sessions. Existing session will not be affected.

Active/Active scenario

Note: Active/Active example is assuming a load balancer with health check is handling traffic to the SA cluster.

When the upgrade process begins on the initial device, the initial device will become unresponsive and the load balancer will send traffic to the other nodes in the cluster. Once the initial device has completed the upgrade process, it will push the service package to the other nodes in the cluster. When upgrade process begins in the additional nodes, these nodes will become unresponsive. The load balancer will send traffic to the initial device to handle traffic until the upgrade process has completed on the additional nodes.

Juniper components will be upgraded only for new user sessions. Existing sessions will not be affected.

For any questions or issues relating to the procedures outlined in this document, please contact support. For details on how to engage support, please refer to the following link: http://www.juniper.net/support/requesting-support.html