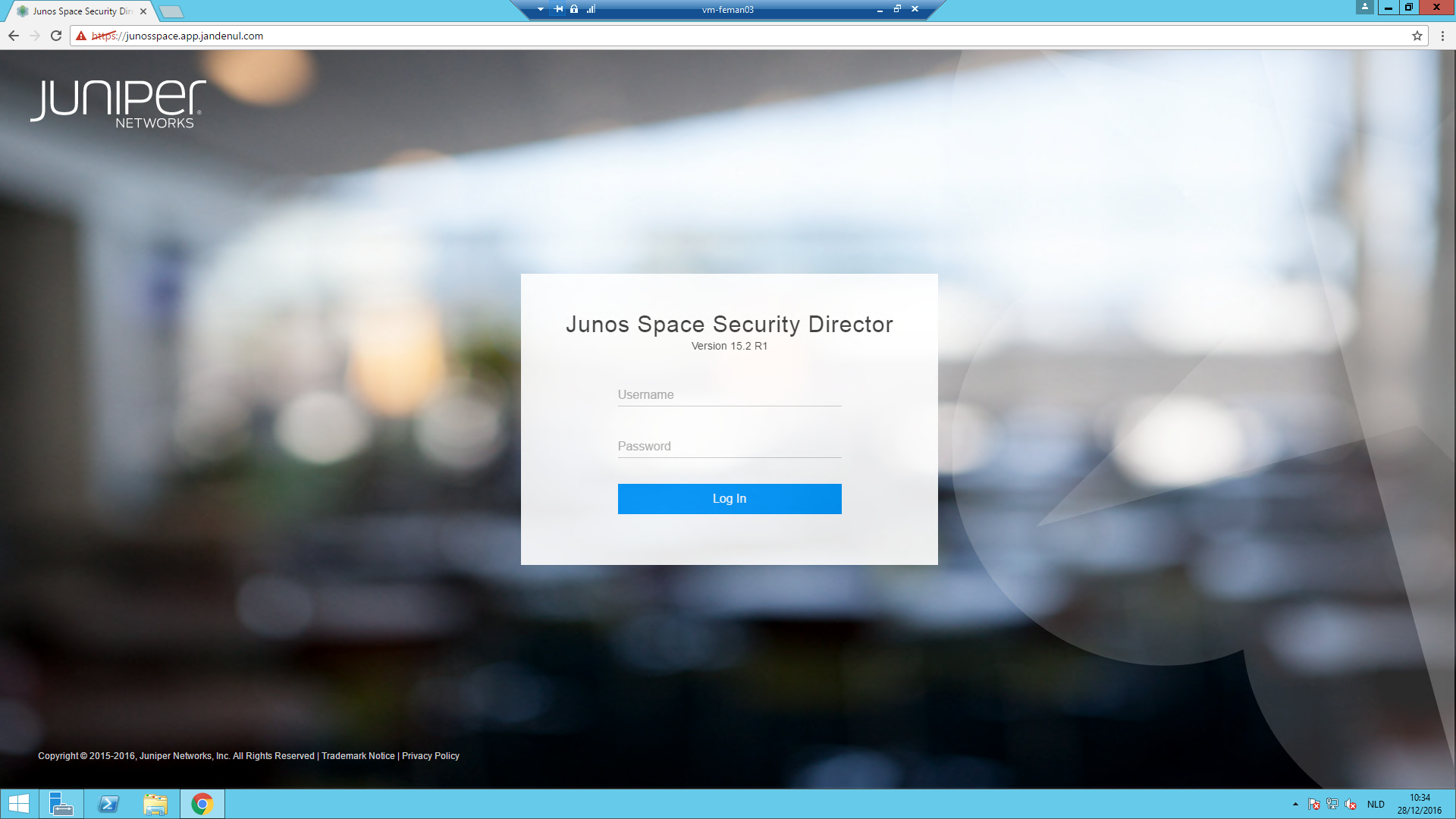
JUNOS SPACE TSE MANUAL

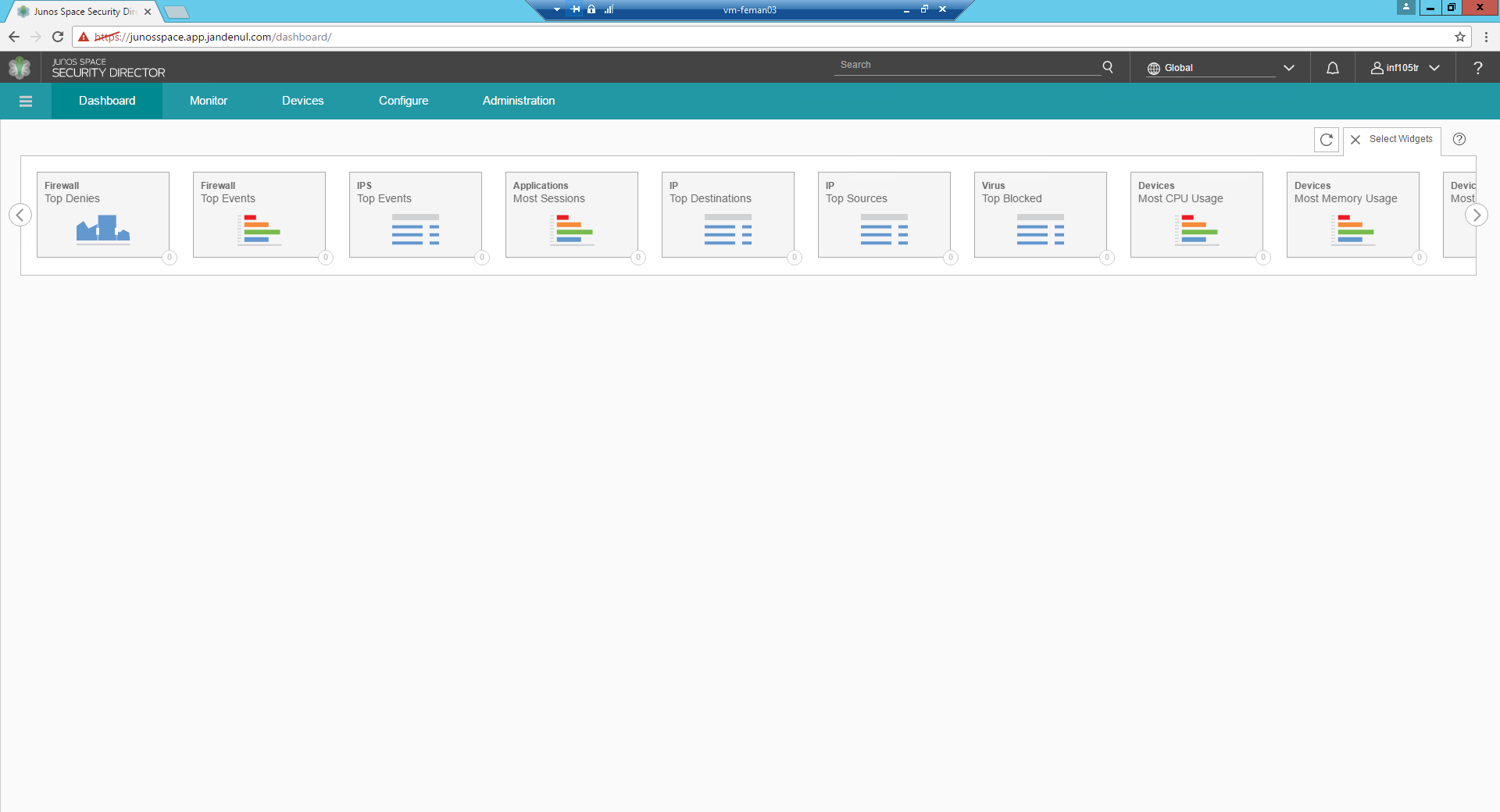
# Login into Junos Space

To login in Junos Space, you need to login into VM-FEMAN03 since it is only accessible from there. Once you are logged in, you can browse to <https://junosspace.app.jandenul.com> (best results with Google Chrome)



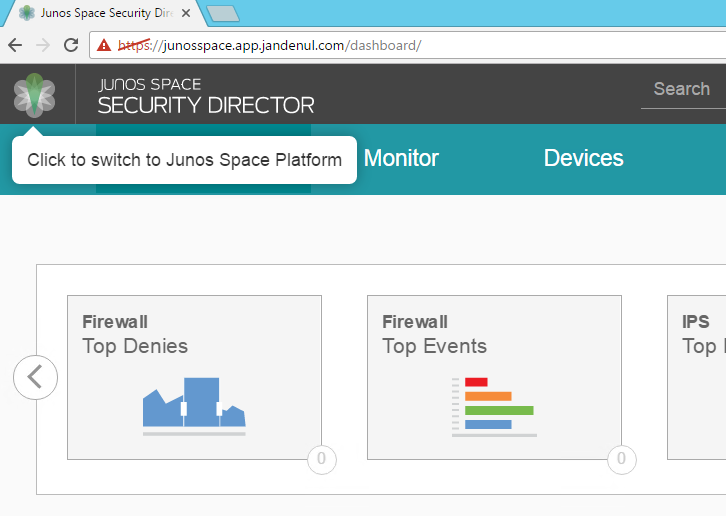
To login, use your ADL account. If you are not able to login, make sure your ADL account is member of security group JDN\_GSR\_RADIUS\_LOG\_ON\_JUNOS\_SPACE\_TSE.

After login, you will be shown the Junos Space Security director dashboard.

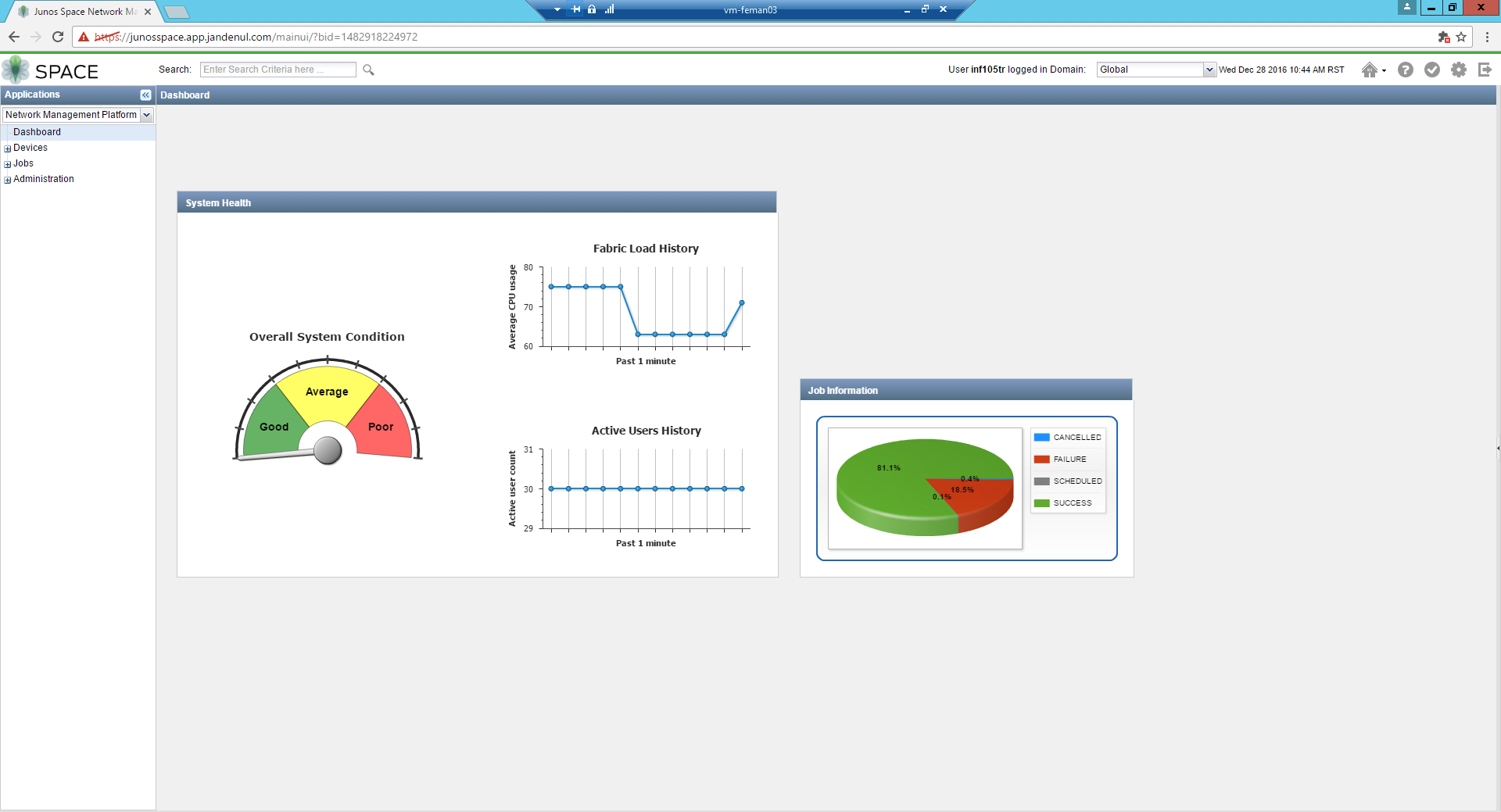


# Check if a device is in sync

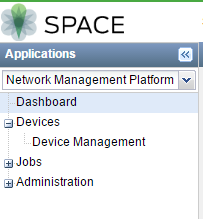
To check if a device is in sync with Junos Space, go to the Junos Space network management platform by clicking the Junos logo in the upper left corner of the page.



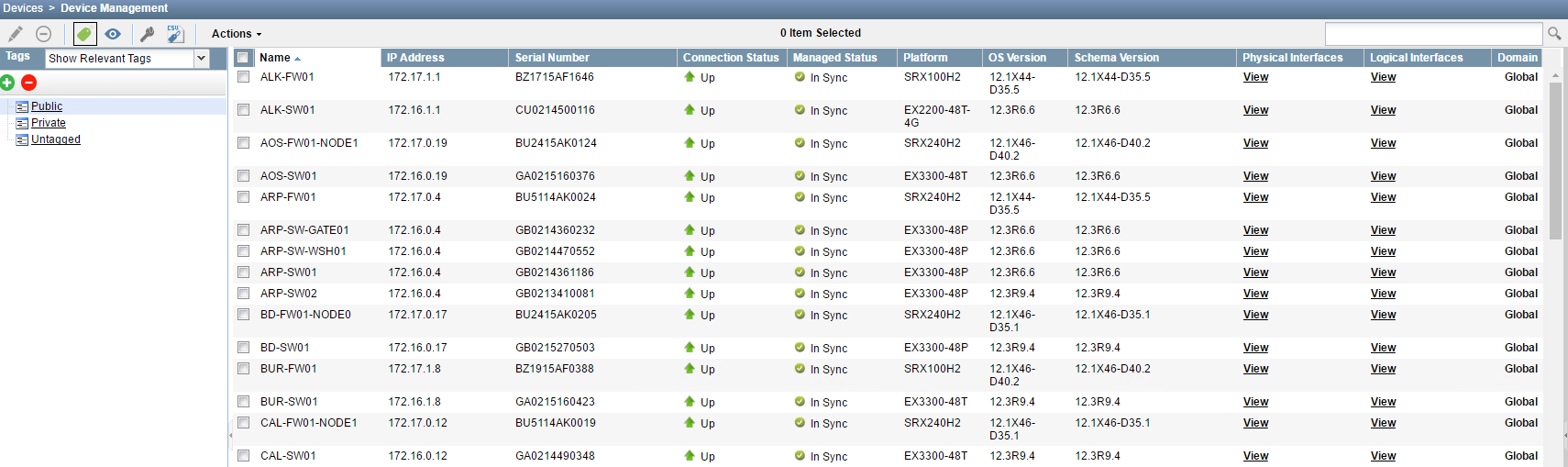
After clicking the Junos logo, you should see the Junos space network management dashboard.



To see the devices overview, open the **Devices** menu and click **Device Management** in the menu bar on the left.



After clicking device management, you will receive a list of all firewalls & switches configured in Junos Space.



When a device is in sync, the **Connection status** should be **UP** and **Managed Status** should be **In Sync**



Other states that are frequently seen, but which are not sufficient to pass a quality check:

* **Connection Status** is **Down** and **Management** **Status** is **In Sync**



Cause: The device was imported in space and in sync but at this time, there is no connectivity from the device to the central management station.

* **Connection Status** is **Down** and **Management** **Status** is **Device** **Changed**



Cause: The device was not in sync when it had connection to the central management station. At this time there is no connection between the device and central management.

* **Connection Status** is **Up** and **Management** **Status** is **Device** **Changed**



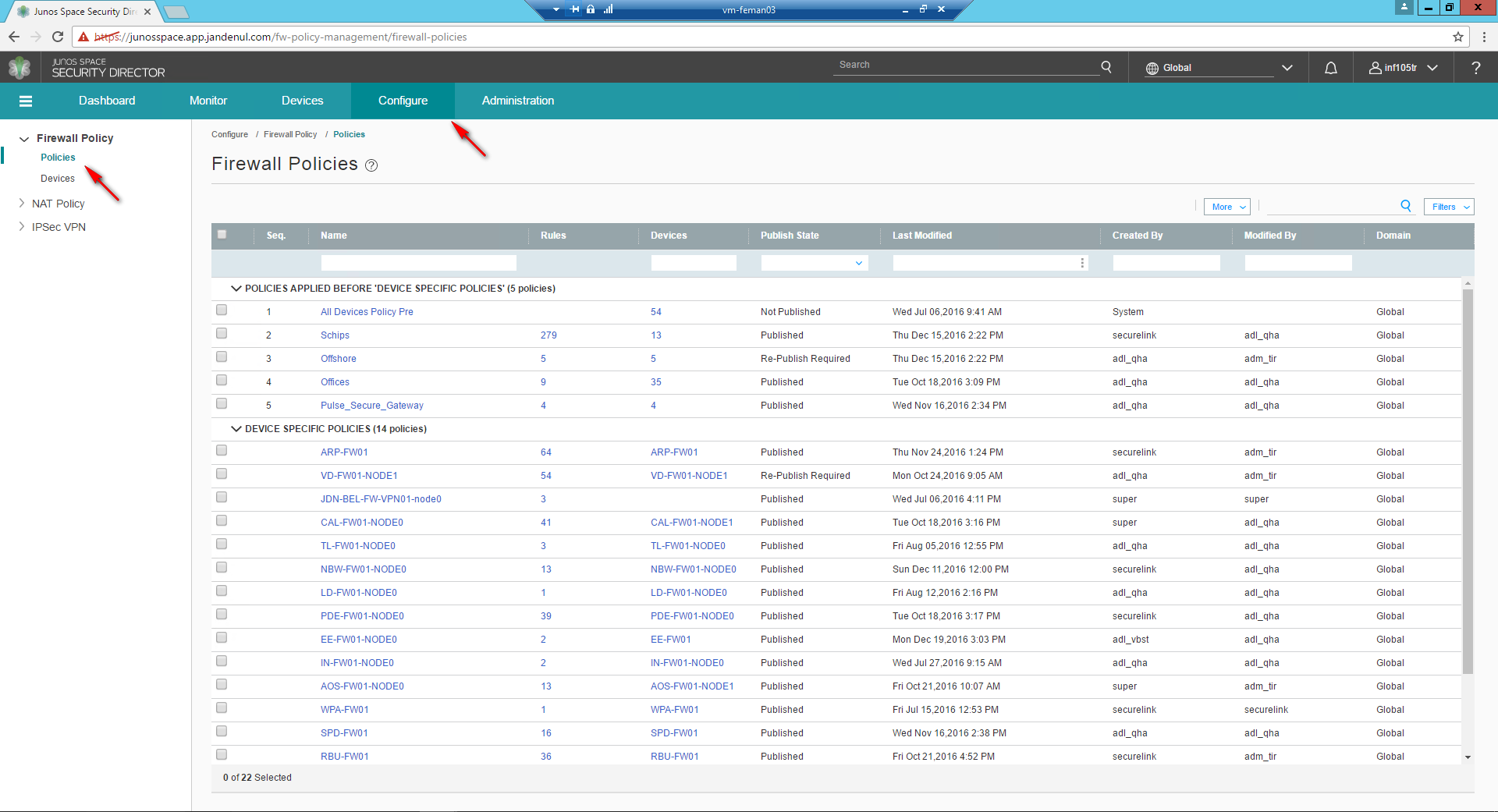
Cause: The device has connectivity to the central management station, but it is no longer in sync.

# Check if a device has Firewall policies assigned

Return to the Junos Space Security Director by selecting **Security Director** from the dropdown menu in the upper left corner in Network Management Platform.



In security Director click the **Configure** tab, and navigate to **Firewall Policy** >> **Policies** in the left-side menu.



Depending on the type of device, it should be assigned to specific policies.

Ship:

* Ships
* SHIPS\_POST

Offshore Ship:

* Ships
* Offshore
* SHIPS\_POST

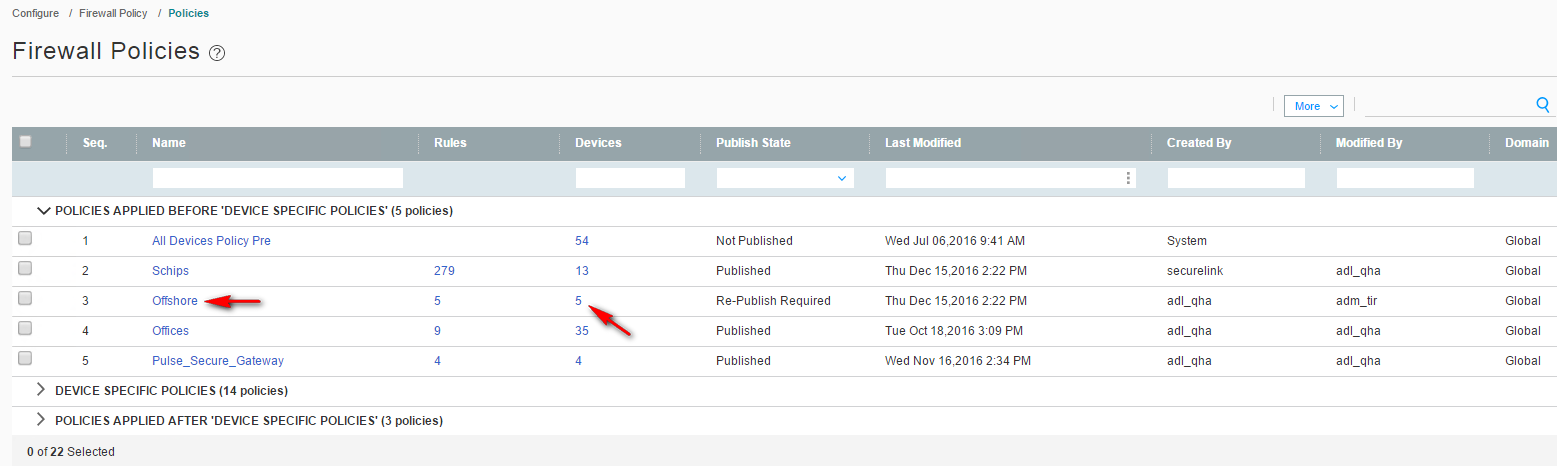
Office:

* Offices
* OFFICES\_POST

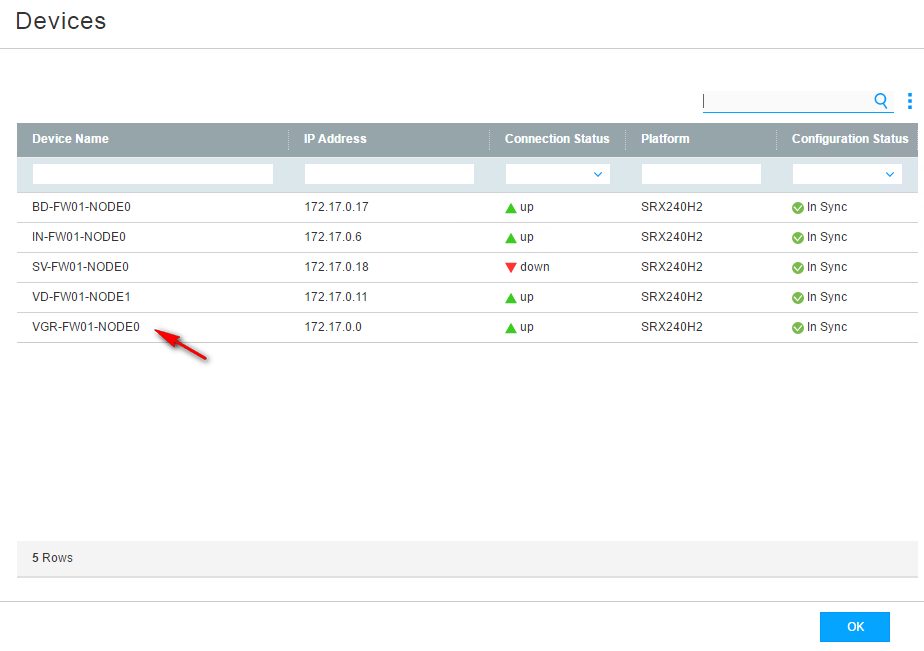
Office with MAG installed:

* Offices
* Pulse\_Secure\_Gateway
* OFFICES\_POST

To check if a device is assigned to the correct policies, click the number of assigned devices under the policy you need to check.



If the device which you are quality checking is in the pop-up list, the policy is assigned to the device.

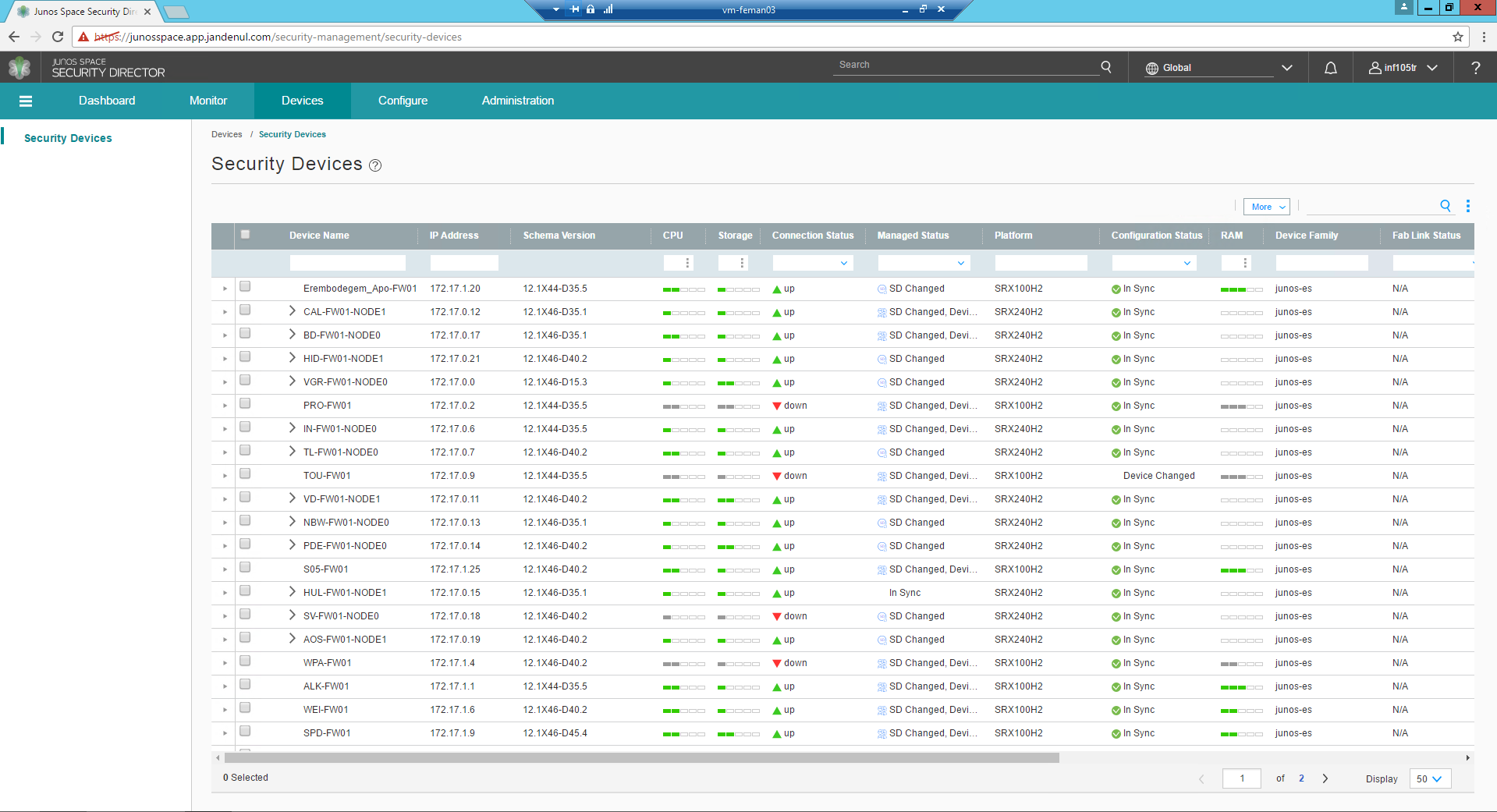


Repeat this step for all policies that should be assigned to the device.

Exceptions (Devices specific policies) should only exists if there are additions to the standard policy base.

# Check if the device received the last version of the assigned Firewall policies

In security Director click the **Devices** tab. You will see all firewalls which are configured in Junos Space.



To check if a device has the latest policies, scroll to the right and verify is the firewall has no **Pending Services**. If there are any other pending firewall services, the firewall does not have the latest policies.

NOTE: NAT policies are also shown; NAT policies have nothing to do with firewall policies.