Panorama Release Notes

Version 5.1

Panorama provides centralized management and visibility of Palo Alto Networks next-generation firewalls. These Release Notes include information on the list of new features, upgrade/downgrade procedures, issues addressed in this release, and the list of known issues in this release.

Before installing this version, please review the upgrade/downgrade procedures thoroughly to understand important changes in Panorama 5.1.

Contents

Panorama Features

The following new features were added in Panorama 5.1.0:

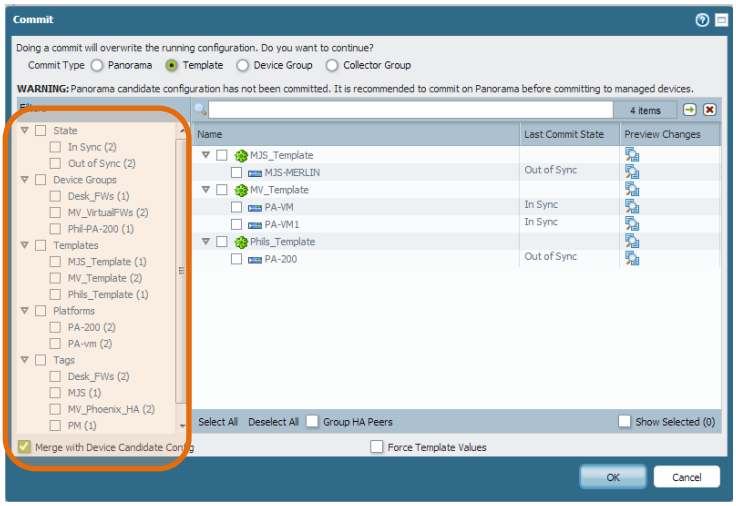
- **Support for device-specific metadata using tags—**The ability to find devices/virtual systems using tags has been added. This enhancement is especially useful in large deployments where several hundred devices are managed by Panorama; tags and predefined filters help to shorten the list of managed devices that display onscreen and allow you easily select the devices that you want to monitor or manage. For example, you can filter for all devices that use a specific template and push a new policy using a Device Group commit to only the devices to which the specified template was applied.

  Tags are user-defined and can be added or deleted using the 

button on the **Panorama > Managed Devices** tab. A tag is a text string that supports up to 31 characters in length; it may not contain empty spaces. Each device/virtual system supports up to 24 tags, and when you select multiple devices/virtual systems, you can see whether there are any common tags across the selected devices. All additions and modifications to tags are logged to the configuration log on Panorama.

  The new filtering attributes that are available are:

  - Device Groups (user-defined groups)
  - Templates (user-defined templates)
  - Tags (user-defined tags)
  - Platforms
  - State (in sync, out-of-sync, selected, not selected, active, completed)
  - Commit Status (sent, succeeded, succeeded with warnings, failed)
  - Result (pending, succeeded, failed)



  Filters are contextual and the filtering attributes that display vary based on the operation you are performing on Panorama. For example, the **State** filter displays when you commit a change to a template or to device groups, but not when you view the list of templates in the **Panorama > Templates** tab.

- **Workflow improvements to replace an RMA device**—To minimize the effort in restoring the configuration for a managed device on a Return Merchandise Authorization (RMA), a CLI-based workflow is available for the *superuser* and *panorama-admin* user roles. A new CLI command on Panorama allows you to replace the serial number of the old device

with that of the new/replacement device; swapping the serial number allows Panorama to recognize the replacement device as soon it comes online.

To then restore the configuration on the replacement device, on Panorama, you can generate a *partial* device state for managed devices running PAN-OS 5.0.4 and later versions. The partial device state replicates the configuration on the managed device with a few exceptions for Large Scale VPN (LSVPN) setups. It is created by combining two facets of the configuration:

- Local configuration on the device: Each time a configuration change is committed, each device sends a copy of its local configuration file to Panorama. This device configuration backup file is stored on Panorama.
- Centralized configuration managed by Panorama: Panorama maintains a snapshot of the shared policies and templates pushed from Panorama.

  Note: Some parts of the dynamic configuration relating to LSVPN, such as information on satellite and dynamic certificate status, are not available and cannot be migrated over to the device because these details are only available as runtime configuration on the device.

For information on the exceptions and for the detailed steps to complete this process, refer to the *Panorama Administrator's Guide*.

- **Remote versus local data source for the ACC and App Scope**—On the Application Command Center (**ACC**) and **App Scope** on Panorama, you now can select the *data source* for visibility into applications, users, and threats across all managed devices. You can choose between **Panorama** or **Remote Device Data**.

Panorama is now the default data source; this is a change in behavior from earlier releases. With **Panorama** as the data source, the logs are accessed from the local storage on Panorama or are fetched from the managed log collectors, when deployed in the distributed log architecture. Using **Panorama** as the data source offers better response time because the managed devices are not queried for the data.

To fetch and display an aggregated view of the data from the managed devices, you can switch the source from **Panorama** to **Remote Device Data**. The web interface shows the progress of the query; an icon displays the status on the total number of managed devices, number of devices that have responded, number of devices skipped, and number that are not connected, if any. This change in preference is also retained for future queries.

When deployed in a high availability configuration, you can select the preferred data source only on the primary Panorama peer. The secondary Panorama peer does not display the **Panorama** option.

- **Upgrade to a 64-bit OS on the Panorama Virtual Appliance—**The Panorama virtual appliance is upgraded to a 64-bit OS; it is no longer released in a 32-bit OS format. When you deploy the OVF template to install a new Panorama virtual appliance, a 64-bit kernel-based VM is installed.

  Minimum system requirements for optimal performance on Panorama 5.1:

  - VMware ESX(i) 4.1 or later with support for 64-bit OS
  - Quad Core CPU (2 GHz); use 3GHz if you have 10 or more firewalls
  - 4GB RAM; 16GB recommended if have 10 or more firewalls
  - 40GB disk space

  Important: For currently deployed Panorama virtual appliances, on an upgrade, the OS will be migrated from a 32-bit to a 64-bit kernel-based VM. Therefore, you must verify that the hardware supports a 64-bit OS before installing or upgrading Panorama 5.1 to prevent Panorama from becoming unresponsive. For details, see Upgrading Panorama.

  For details on installing a new virtual appliance, refer to the *Panorama Administrator's Guide*.

- **Improvements in Performance—**To improve the user experience when using Panorama, some backend architecture improvements were effected. The observable changes are:
  - Faster commit times, and quicker response time when using Panorama for performing content and PAN-OS software updates on managed devices. This improvement was achieved by adding multi-threaded event and job processing systems.
  - Increased support for concurrent administrators by adding support for dedicated processes that handle reports, logs, and configuration changes. To ensure that conflicts do not occur when an administrator makes changes, the user interface is auto-updated to reflect the changes.
  - Improved response time in switching context from Panorama to a managed device. To handle context switching, a dedicated process was introduced, and the caching capability was added to enable quicker response time in subsequent context switches.

- **Support for Viewing Detailed Reports on WildFire Submissions**—Each time a firewall forwards a file to WildFire for analysis, WildFire sends the results of the analysis back to the firewall's WildFire logs. If WildFire log forwarding to Panorama is enabled on the firewalls, the aggregated logs can be viewed in the **Monitor > Logs > WildFire Submissions** tab on Panorama. These logs now contain links to detailed analysis reports that are hosted on the WildFire server. To enable Panorama to link to the reports, you must make sure that Panorama is configured to access the proper WildFire server. By default, Panorama is configured to link to reports on the WildFire cloud. However, if your firewalls are forwarding files to a local WF-500 WildFire appliance, you must configure Panorama to point to the appliance instead. You configure this setting on the **Panorama > Setup > WildFire** tab. Panorama can only be configured to point to one WildFire server.

- **Dedicated Panorama Documentation**—The all new Panorama Administrator's Guide provides comprehensive conceptual and procedural information for setting up Panorama—a virtual appliance or an M-100 appliance—setting up dedicated log collection, and for adding, managing, and monitoring your distributed Palo Alto Networks next-generation firewalls. It includes detailed use-case examples for planning and implementing a central management strategy and for using the aggregated reporting features to monitor and respond to activity and threats on your network.

Changes to Default Behavior

The following lists changes to the default behavior in Panorama 5.1:

- In earlier releases of Panorama, the Application Command Center (ACC) and the App Scope fetched data from the managed devices to represent the trends in network traffic. Now, by default, Panorama uses the **Panorama** data source that stores logs forwarded to it by the managed devices. The only exception to this behavior is in a high availability configuration, where the secondary Panorama peer accesses **Remote Device Data** and fetches data directly from the managed devices.

- **Important**: On upgrade to Panorama 5.1, Panorama is migrated from a 32-bit OS to a 64-bit OS. If you have a Panorama virtual appliance, make sure that your ESX(i) server supports a 64-bit OS before you upgrade. For other modifications and recommendations for optimal performance on the 64-bit OS, see the upgrade procedure.

Upgrade/Downgrade Procedures

The following sections provide upgrade/downgrade procedures.

Upgrading the Panorama Software Version

Important In order to upgrade to Panorama 5.1.0, you must be running Panorama 5.0.0 or later. Attempts to upgrade to Panorama 5.1.0 from earlier releases will be blocked.

For upgrading a Panorama virtual appliance, you must have VMware ESX(i) 4.1 or later with support for 64-bit OS. Ensure that 64-bit support is enabled in the system BIOS of the ESX(i) server that hosts the Panorama virtual appliance. For example, the CPU Information section in Dell systems includes the option for 64-bit support.

If you upgrade to 5.1 on an ESX(i) host that does not support a 64-bit OS, Panorama will stop functioning.

Step 1: Get Content Updates

Panorama must be running content update 320 or later to upgrade to Panorama 5.1.0. Use the following steps to perform a dynamic content update, which consists of App-ID updates as well as threat updates. Panorama must be registered for the following steps to work. Please go to https://support.paloaltonetworks.com to register Panorama.

1. Navigate to the **Panorama > Dynamic Updates** tab in the web interface.
2. Click **Check Now** to retrieve the currently available updates that can be installed.
3. Click the **Download** link in the **Action** column corresponding to the latest update.
4. After the download completes, click the **Install** link to initiate the update.

Step 2: Upgrade the Software

Use the following steps to perform a software upgrade to this release:

1. Navigate to the **Panorama > Software** tab in the web interface.
2. Click **Check Now** to retrieve the currently available releases that can be installed.
3. Locate the latest release and click the **Download** link for the version.
4. After the download completes, click the **Install** link to perform the upgrade. To complete the upgrade process, you must reboot Panorama.
   Important: If you are upgrading a Panorama virtual appliance, do not reboot. Instead, select **Panorama > Setup > Operations** and click **Shutdown** and then proceed to Step 5 below.

5. (Required only on the Panorama virtual appliance) Modify the settings on the virtual appliance.
    a. Power off the Panorama virtual appliance on the ESX(i) server.
    b. Select the Panorama virtual machine, and right-click. Select **Edit Settings...** and make the following changes:
        i. On the **Hardware** tab, change the **SCSI Controller Type** from **BusLogic Parallel** to **LSI Logic Parallel**.
        ii. (Optimal performance recommendation) Increase resource allocation for RAM and CPU based on the following minimum system requirements for Panorama 5.1:
            - Quad Core CPU (2 GHz); use 3GHz if you have 10 or more firewalls
            - 4GB RAM; use 16GB if have 10 or more firewalls
            - 40GB disk space
        iii. On the **Options** tab, change the **Guest Operating System** for the virtual appliance from **Other Linux (32-bit)** to **Other Linux (64-bit)**.
    c. Power on the Panorama virtual appliance.

Downgrading the Panorama Software

When downgrading from a major release, for example Panorama 5.1 to 5.0 or from 5.0 to 4.1, for best results use the configuration backup that you had created before the upgrade or use the auto-saved configuration file that was created during the upgrade. If you choose to use the running configuration for the downgrade, the configuration file might be pared down. This paring down occurs because portions of the configuration may have been migrated to new formats or to a new internal schema during the upgrade process; these changes can make the current configuration unsuitable for a downgrade.

1. Save a backup of the current configuration file.
    a. Navigate to the **Panorama > Setup > Operations** tab.
    b. Click **Export named configuration snapshot**, select **running-config.xml** and click **OK** to save the configuration file. Rename the file. This backup can be used to restore the configuration if you have problems with the downgrade and need to perform a factory reset.
2. Downgrade the software version.
    a. Navigate to the **Panorama > Software** tab. The software page lists all the Panorama software versions available for download.
    b. Locate the desired release and click the **Download** link for that version. If you have previously downloaded the version, the link displays as **Install** instead of **Download**.
    c. After the download completes, click the **Install** link to perform the downgrade. If downgrading to an earlier major release, on clicking **Install** you will be prompted

to select a configuration file. For best results, Palo Alto Networks recommends using the configuration file backup that you had created before the upgrade or the auto-saved configuration file that was automatically created and saved when you upgraded to a major release.

d. To complete the downgrade process, you must reboot Panorama. On a reboot, the software version and running configuration will be switched to the version you selected.
   Important: If you are downgrading a Panorama virtual appliance, do not reboot. Instead, select **Panorama > Setup > Operations** and click **Shutdown Panorama** and then proceed to Step 3 below.
   To reboot, click **OK** when prompted, or select **Panorama > Setup > Operations**, and click **Reboot Panorama**.

3. (Required only on the Panorama virtual appliance) After you complete installing the version of your choice, modify the virtual appliance settings on the ESX(i) server.
   a. Verify that the Panorama virtual appliance is powered off on the ESX(i) server.
   b. Select the Panorama virtual appliance. Right click and select **Edit Settings…** and make the following changes:
      i. On the **Hardware** tab, change the **SCSI Controller Type** and click **Change Type**. Change it from **LSI Logic Parallel** to **BusLogic Parallel**. Click **OK** to save the change.
      ii. On the **Options** tab, change the **Guest Operating System** for the virtual appliance from **Other Linux (64-bit)** to **Other Linux (32-bit)**. Click **OK** to save the change.
   c. Power on the Panorama virtual appliance on the ESX(i) server.
   d. Access the Panorama web interface. On the **Dashboard**, confirm that Panorama is now running the software version to which you just downgraded.

New CLI Commands

List of new CLI commands introduced in Panorama 5.1:

Replace the serial number of a managed device on Panorama

- To swap the serial number of an old device that was sent for RMA with that of the new replacement device:
  replace device old [old SN#] **new** [new SN#]

Support for tags

- To add a tag to a device:
  set mgt-config devices [device_serial_number] **vsys** [vsys#] **tags** [tagname1 tagname2]

- To view tags assigned to a specific device:
  show mgt-config devices [device_serial_number] **vsys** [vsys#]

- To view tags for all managed devices:
  show mgt-config devices

- To delete a tag from a device:
  delete mgt-config devices [device_serial_number] **vsys** [vsys#] **tags** [tagname]

Known Issues

The following is a list of known unresolved issues in this release:

- 33612 — Attempts to reset the Master Key from the web interface (**Panorama > Master Key and Diagnostics**) or the CLI on Panorama will fail. However, because it is not necessary for the keys to match when pushing configuration changes from Panorama to a managed device, this issue should not cause a problem in administering devices using Panorama.

- 37751 — When you use Panorama templates to schedule a log export (**Device > Scheduled Log Export**) to an SCP server, you must log in to each managed device and click the **Test SCP server connection** button after the template is pushed. The connection is not established until the firewall accepts the host key for the SCP server.

- 39543 — SSH host keys used for SCP log export are stored in the known hosts file on the firewall. In a High Availability (HA) configuration, the SCP log export configuration is synchronized with the peer device, but the known host file is not synchronized. So, when a failover occurs, the SCP log export fails.

  Workaround: Log in to each Panorama peer in HA, and click the **Test SCP server connection** button and confirm the host key so that SCP log forwarding continues to work upon failover.

- 45391 — Limitation in configuring a management IP address on an M-100 appliance configured as the secondary passive peer in a High Availability pair.

  Workaround: To set the IP address for the management interface, you must suspend the active Panorama peer, promote the passive peer to active, change the configuration on that peer, and then restore the other peer back to the active state.

- 45424— When you switch context from Panorama and access the web interface of a managed device, you might be unable to upgrade the PAN-OS software image.

  Workaround: Use the **Panorama > Device Deployment > Software** tab to deploy and install the software image on the managed device.

- 45464— On the Panorama virtual appliance, summary logs for traffic and threats are not written after issuing the `clear log` command. You must restart the management server to enable summary logs.

- 47901— When the same filter is repeatedly used to query the traffic logs in the **Monitor > Logs > Traffic** tab, on occasion the query results do not display.

  Workaround: Clear the filter, refresh the page, then add the filter and repeat the query.

- 50473—Administrative access using key-based authentication for SSH and certificate-based authentication for the web interface cannot be enabled.

  Workaround: Configure username and password-based authentication on administrative access.

- 50856—On the M-100 appliance in Distributed Log Collection architecture, a slight difference is noticed between the disk capacity available on the RAID disks and the available capacity identified in memory.

- 51693— Do not restore the M-100 appliance to factory defaults. When an M-100 appliance running Panorama 5.1.0 is restored to factory defaults (Factory Reset), on reboot the appliance may go into maintenance mode and end in a non-functional state. A fix for this issue is being implemented, tested, and will be available in an upcoming maintenance release.

  Workaround: Refer to this KB article: https://live.paloaltonetworks.com/docs/DOC-5096

Related Documentation

The following additional documentation is provided:

PANORAMA

- **Panorama Administrator's Guide**—Describes how to administer Panorama using the web interface. The guide is intended for system administrators responsible for deploying, operating, and maintaining Panorama.

- **M-100 Hardware Reference Guide**—Detailed reference containing the specifics of the M-100 hardware platform, including specifications, LED behaviors, and installation procedures.

- **Online Help System**—Detailed context-sensitive help system integrated with the web interface on Panorama.

PALO ALTO NETWORKS FIREWALL

- **Getting Started Guide**—This guide takes you through the initial configuration and basic set up of your Palo Alto Networks firewall. Use this guide to perform the initial configuration on the firewall, and then use the **Panorama Administrator's Guide** to administer the firewalls centrally using Panorama.

- **Palo Alto Networks Administrator's Guide**—Describes how to administer the Palo Alto Networks firewall using the device's web interface. The guide is intended for system administrators responsible for deploying, operating, and maintaining the firewall.

- **PAN-OS Command Line Interface Reference Guide**—Detailed reference explaining how to access and use the command line interface (CLI) on the firewall and on Panorama.

Requesting Support

For technical support, call 1-866-898-9087 or send email to support@paloaltonetworks.com.

Revision History

Date	Revision	Comment
5/14/2013	A	• Added information on 5.1.0