Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About this Guide

This guide describes how to set up and use Panorama™ for centralized management; it is intended for administrators who want the basic framework to quickly set up the Panorama virtual appliance or the M-Series appliance for centralized administration of Palo Alto Networks firewalls.

If you have an M-Series appliance, this guide takes over after you finish rack mounting your M-Series appliance.

For more information, refer to the following sources:

- For information on how to configure other components in the Palo Alto Networks Next-Generation Security Platform, go to the Technical Documentation portal: https://docs.paloaltonetworks.com or search the documentation.
- For access to the knowledge base, complete documentation set, discussion forums, and videos, refer to https://live.paloaltonetworks.com.
- For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to https://www.paloaltonetworks.com/support/tabs/overview.html.
- For the most current PAN-OS and Panorama 7.1 release notes, go to https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-release-notes.

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panorama Overview</td>
<td>9</td>
</tr>
<tr>
<td>About Panorama</td>
<td>10</td>
</tr>
<tr>
<td>Panorama Platforms</td>
<td>11</td>
</tr>
<tr>
<td>Centralized Configuration and Deployment Management</td>
<td>13</td>
</tr>
<tr>
<td>Context Switch—Firewall or Panorama</td>
<td>13</td>
</tr>
<tr>
<td>Templates and Template Stacks</td>
<td>13</td>
</tr>
<tr>
<td>Device Groups</td>
<td>15</td>
</tr>
<tr>
<td>Centralized Logging and Reporting</td>
<td>19</td>
</tr>
<tr>
<td>Logging Options</td>
<td>19</td>
</tr>
<tr>
<td>Managed Collectors and Collector Groups</td>
<td>20</td>
</tr>
<tr>
<td>Caveats for a Collector Group with Multiple Log Collectors</td>
<td>20</td>
</tr>
<tr>
<td>Centralized Reporting</td>
<td>22</td>
</tr>
<tr>
<td>Panorama Commit and Validation Operations</td>
<td>24</td>
</tr>
<tr>
<td>Role-Based Access Control</td>
<td>25</td>
</tr>
<tr>
<td>Administrative Roles</td>
<td>25</td>
</tr>
<tr>
<td>Authentication Profiles and Sequences</td>
<td>26</td>
</tr>
<tr>
<td>Access Domains</td>
<td>27</td>
</tr>
<tr>
<td>Administrative Authentication</td>
<td>27</td>
</tr>
<tr>
<td>Panorama Recommended Deployments</td>
<td>29</td>
</tr>
<tr>
<td>Panorama for Centralized Management and Reporting</td>
<td>29</td>
</tr>
<tr>
<td>Panorama in a Distributed Log Collection Deployment</td>
<td>30</td>
</tr>
<tr>
<td>Plan Your Deployment</td>
<td>31</td>
</tr>
<tr>
<td>Deploy Panorama: Task Overview</td>
<td>33</td>
</tr>
<tr>
<td>Set Up Panorama</td>
<td>35</td>
</tr>
<tr>
<td>Determine Panorama Log Storage Requirements</td>
<td>36</td>
</tr>
<tr>
<td>Set Up the Panorama Virtual Appliance</td>
<td>38</td>
</tr>
<tr>
<td>Setup Prerequisites for the Panorama Virtual Appliance</td>
<td>38</td>
</tr>
<tr>
<td>Install the Panorama Virtual Appliance</td>
<td>39</td>
</tr>
<tr>
<td>Perform Initial Configuration of the Panorama Virtual Appliance</td>
<td>42</td>
</tr>
<tr>
<td>Expand Log Storage Capacity on the Panorama Virtual Appliance</td>
<td>45</td>
</tr>
<tr>
<td>Increase CPUs and Memory on the Panorama Virtual Appliance</td>
<td>47</td>
</tr>
<tr>
<td>Complete the Panorama Virtual Appliance Setup</td>
<td>48</td>
</tr>
<tr>
<td>Set Up the M-Series Appliance</td>
<td>50</td>
</tr>
<tr>
<td>Perform Initial Configuration of the M-Series Appliance</td>
<td>51</td>
</tr>
<tr>
<td>Set up the M-Series Appliance as a Log Collector</td>
<td>54</td>
</tr>
<tr>
<td>Increase Storage on the M-Series Appliance</td>
<td>60</td>
</tr>
<tr>
<td>Register Panorama and Install Licenses</td>
<td>68</td>
</tr>
<tr>
<td>Register Panorama</td>
<td>68</td>
</tr>
<tr>
<td>Activate a Panorama Support License</td>
<td>69</td>
</tr>
<tr>
<td>Activate/Retrieve a Firewall Management License on the Panorama Virtual Appliance</td>
<td>69</td>
</tr>
</tbody>
</table>

© Palo Alto Networks, Inc.  Panorama 7.1 Administrator’s Guide • 3
Activate/Retrieve a Firewall Management License on the M-Series Appliance ....... 70

Install Content and Software Updates for Panorama .................................................. 72
Panorama, Log Collector, and Firewall Version Compatibility ...................................... 72
Install Updates for Panorama in an HA Configuration ................................................ 73
Install Updates for Panorama with an Internet Connection ........................................ 74
Install Updates for Panorama without an Internet Connection .................................... 78

Transition to a Different Panorama Platform ............................................................... 82
  Migrate from a Panorama Virtual Appliance to an M-Series Appliance .............. 82
  Migrate from an M-Series Appliance to a Panorama Virtual Appliance .............. 84
  Migrate from an M-100 Appliance to an M-500 Appliance ................................. 87

Access and Navigate Panorama Management Interfaces ............................................. 91
  Log in to the Panorama Web Interface ...................................................................... 91
  Navigate the Panorama Web Interface .................................................................... 91
  Log in to the Panorama CLI .................................................................................... 92

Set Up Administrative Access to Panorama .................................................................. 94
  Configure an Admin Role Profile ............................................................................ 94
  Configure an Access Domain .................................................................................. 94
  Configure Administrative Accounts and Authentication ......................................... 95
  Configure an Administrative Account .................................................................... 96
  Configure an Administrator with Kerberos SSO, External, or Local Authentication .... 96
  Configure an Administrator with Certificate-Based Authentication for the Web Interface . 97
  Configure an Administrator with SSH Key-Based Authentication for the CLI ........... 98
  Configure RADIUS Vendor-Specific Attributes for Administrator Authentication .... 99

Manage Firewalls ........................................................................................................... 101
  Add a Firewall as a Managed Device .................................................................... 102

Manage Device Groups ................................................................................................. 103
  Add a Device Group .............................................................................................. 103
  Create a Device Group Hierarchy ......................................................................... 104
  Create Objects for Use in Shared or Device Group Policy ..................................... 105
  Revert to Inherited Object Values ......................................................................... 107
  Manage Unused Shared Objects ............................................................................ 107
  Manage Precedence of Inherited Objects ............................................................... 108
  Move or Clone a Policy Rule or Object to a Different Device Group ..................... 108
  Select a URL Filtering Vendor on Panorama .......................................................... 109
  Push a Policy Rule to a Subset of Firewalls ............................................................. 113
  Manage the Rule Hierarchy .................................................................................... 114

Manage Templates and Template Stacks ...................................................................... 116
  Template Capabilities and Exceptions .................................................................. 116
  Add a Template ..................................................................................................... 116
  Configure a Template Stack .................................................................................. 118
  Override a Template Setting ................................................................................. 119
  Disable/Remove Template Settings ....................................................................... 120

Transition a Firewall to Panorama Management .......................................................... 121
  Plan the Transition to Panorama Management ...................................................... 121
  Migrate a Firewall to Panorama Management ...................................................... 122
  Migrate a Firewall HA Pair to Panorama Management ......................................... 126
## Table of Contents

- Load a Partial Firewall Configuration into Panorama ........................................... 129
- Use Case: Configure Firewalls Using Panorama .................................................. 132
  - Device Groups in this Use Case ........................................................................ 133
  - Templates in this Use Case ................................................................................. 133
  - Set Up Your Centralized Configuration and Policies ........................................ 134

### Manage Log Collection .................................................................................. 141
- Configure a Managed Collector ............................................................................. 142
- Manage Collector Groups ......................................................................................... 146
  - Configure a Collector Group ............................................................................. 146
  - Move a Log Collector to a Different Collector Group ........................................... 149
  - Remove a Firewall from a Collector Group .......................................................... 151
- Configure Log Forwarding to Panorama ................................................................. 152
- Verify Log Forwarding to Panorama .................................................................... 155
- Modify Log Forwarding and Buffering Defaults ..................................................... 156
- Configure Log Forwarding from Panorama to External Destinations .................. 158
- Log Collection Deployments .................................................................................. 160
  - Plan a Log Collection Deployment ................................................................... 160
  - Deploy Panorama with Dedicated Log Collectors .............................................. 162
  - Deploy Panorama with Default Log Collectors .................................................. 169
  - Deploy Panorama Virtual Appliances with Local Log Collection .................... 175

### Manage Licenses and Updates ...................................................................... 177
- Manage Licenses on Firewalls Using Panorama .................................................... 178
- Deploy Updates to Firewalls and Log Collectors Using Panorama ...................... 179
  - Supported Updates ............................................................................................. 179
  - Schedule a Content Update Using Panorama ...................................................... 180
  - Deploy an Update to Log Collectors when Panorama is Internet-connected .......... 181
  - Deploy an Update to Log Collectors when Panorama is not Internet-connected .... 184
  - Deploy an Update to Firewalls when Panorama is Internet-connected ................ 187
  - Deploy an Update to Firewalls when Panorama is not Internet-connected .......... 187

### Monitor Network Activity .............................................................................. 193
- Use Panorama for Visibility ................................................................................... 194
  - Monitor the Network with the ACC and AppScope ........................................... 194
  - Analyze Log Data ............................................................................................... 196
  - Generate, Schedule, and Email Reports .............................................................. 196
- Use Case: Monitor Applications Using Panorama ................................................ 199
- Use Case: Respond to an Incident Using Panorama .............................................. 202
  - Incident Notification .......................................................................................... 202
  - Review the Widgets in the ACC ......................................................................... 203
  - Review Threat Logs ............................................................................................ 203
  - Review WildFire Logs ......................................................................................... 204
  - Review Data Filtering Logs ................................................................................. 204
  - Update Security Rules ......................................................................................... 205
# Table of Contents

## Panorama High Availability
- Panorama HA Prerequisites
- Priority and Failover on Panorama in HA
- Failover Triggers
  - HA Heartbeat Polling and Hello Messages
  - HA Path Monitoring
- Logging Considerations in Panorama HA
  - Logging Failover on a Panorama Virtual Appliance
  - Logging Failover on an M-Series Appliance
- Synchronization Between Panorama HA Peers
- Manage a Panorama HA Pair
  - Set Up HA on Panorama
  - Test Panorama HA Failover
  - Switch Priority after Panorama Failover to Resume NFS Logging
  - Restore the Primary Panorama to the Active State

## Administer Panorama
- Preview, Validate, or Commit Configuration Changes
- Manage Panorama and Firewall Configuration Backups
  - Schedule Export of Configuration Files
  - Back Up Panorama and Firewall Configurations
  - Restore a Panorama Configuration
  - Configure the Maximum Number of Configuration Backups on Panorama
  - Load a Configuration Backup on a Managed Firewall
- Compare Changes in Panorama Configurations
- Manage Locks for Restricting Configuration Changes
- Add Custom Logos to Panorama
- Use the Panorama Task Manager
- Manage Storage Quotas and Expiration Periods for Logs and Reports
  - Log and Report Storage
  - Log and Report Expiration Periods
  - Configure Storage Quotas and Expiration Periods for Logs and Reports
- Monitor Panorama
  - Panorama System and Configuration Logs
  - Monitor Panorama and Log Collector Statistics Using SNMP
- Reboot or Shut Down Panorama
- Configure Panorama Password Profiles and Complexity

## Troubleshooting
- Troubleshoot Panorama System Issues
  - Generate Diagnostic Files for Panorama
  - Diagnose Panorama Suspended State
  - Monitor the File System Integrity Check
  - Manage Panorama Storage for Software and Content Updates
  - Recover from Split Brain in Panorama HA Deployments
# Table of Contents

Troubleshoot Log Storage and Connection Issues .................................................. 245  
Verify Panorama Port Usage .................................................................................. 245  
Resolve Zero Log Storage for a Collector Group ...................................................... 246  
Replace a Failed Disk on an M-Series Appliance ..................................................... 246  
Replace the Virtual Disk on an ESXi Server ............................................................ 247  
Replace the Virtual Disk on vCloud Air .................................................................. 247  
Migrate Logs to a New M-Series Appliance in Log Collector Mode ....................... 248  
Migrate Logs to a New M-Series Appliance in Panorama Mode ............................... 252  
Migrate Log Collectors after Failure/RMA of Non-HA Panorama ......................... 257  
Regenerate Metadata for M-Series Appliance RAID Pairs ..................................... 260  
Replace an RMA Firewall ....................................................................................... 261  
Partial Device State Generation for Firewalls ....................................................... 261  
Before Starting RMA Firewall Replacement ......................................................... 261  
Restore the Firewall Configuration after Replacement ......................................... 263  
Troubleshoot Commit Failures ................................................................................ 265  
Troubleshoot Registration or Serial Number Errors .............................................. 266  
Troubleshoot Reporting Errors ............................................................................. 267  
View Task Success or Failure Status ..................................................................... 268
Panorama Overview

Panorama provides centralized monitoring and management of multiple Palo Alto Networks next-generation firewalls. It provides a single location from which you can oversee all applications, users, and content traversing your network, and then use this knowledge to create application enablement policies that protect and control the network. Using Panorama for centralized policy and firewall management increases operational efficiency in managing and maintaining a distributed network of firewalls.

▲ About Panorama
▲ Panorama Platforms
▲ Centralized Configuration and Deployment Management
▲ Centralized Logging and Reporting
▲ Panorama Commit and Validation Operations
▲ Role-Based Access Control
▲ Panorama Recommended Deployments
▲ Plan Your Deployment
▲ Deploy Panorama: Task Overview
About Panorama

Panorama provides centralized management of Palo Alto Networks next-generation firewalls, as the following figure illustrates:

Panorama allows you to effectively configure, manage, and monitor your Palo Alto Networks firewalls using central oversight with local control, as required. The three focal areas in which Panorama adds value are:

- **Centralized configuration and deployment**—To simplify central management and rapid deployment of the firewalls on your network, use Panorama to pre-stage the firewalls for deployment. You can then assemble the firewalls into groups, and create templates to apply a base network and device configuration and use device groups to administer globally shared and local policy rules. See Centralized Configuration and Deployment Management.

- **Aggregated logging with central oversight for analysis and reporting**—Collect information on activity across all the managed firewalls on the network and centrally analyze, investigate and report on the data. This comprehensive view of network traffic, user activity, and the associated risks empowers you to respond to potential threats using the rich set of policies to securely enable applications on your network. See Centralized Logging and Reporting.

- **Distributed administration**—Allows you to delegate or restrict access to global and local firewall configurations and policies. See Role-Based Access Control for delegating appropriate levels of access for distributed administration.

Panorama is available in two appliance types: a virtual appliance and a dedicated hardware appliance. For more information, see Panorama Platforms.
Panorama Platforms

Panorama is available in the following appliances, each of which supports firewall management licenses for managing up to 25, 100, or 1,000 firewalls:

- **Panorama virtual appliance**—You can install the Panorama virtual appliance on a VMware ESXi server or in VMware vCloud Air. The virtual appliance allows for simple installation and facilitates server consolidation for sites that need a virtual management appliance. By default, the Panorama virtual appliance has one disk partition for all data. Approximately 11GB of the partition is allocated to store the logs collected from firewalls and the logs that Panorama and Log Collectors generate. If you need more log storage, you can add a virtual disk of up to 8TB on vCloud Air or ESXi 5.5 and later versions. Earlier ESXi versions support a virtual disk of up to 2TB. If you need more than 8TB, you can mount Panorama to an NFS datastore but only on the ESXi server, not in vCloud Air. The Panorama virtual appliance works best in environments with logging rates of up to 10,000 logs per second. You can forward firewall logs directly to the Panorama virtual appliance (see Deploy Panorama Virtual Appliances with Local Log Collection) or use the Panorama virtual appliance to manage Dedicated Log Collectors that are M-Series appliances (see Deploy Panorama with Dedicated Log Collectors).

- **M-Series appliance**—The M-100 appliance and M-500 appliance are dedicated hardware models intended for large-scale deployments. In environments with high logging rates (over 10,000 logs per second) and log retention requirements, these appliances enables scaling of your log collection infrastructure. Both appliances use RAID drives to store firewall logs and support RAID 1 mirroring to protect against disk failures. Both appliances use an SSD to store the logs that Panorama and Log Collectors generate. Only the M-500 appliance has redundant, hot-swappable power supplies and front-to-back airflow. The M-500 appliance also has faster processors and greater memory for better performance (for example, faster commit times). These attributes make the M-500 appliance more suitable for datacenters than the M-100 appliance. You can deploy the M-Series appliance in the following modes to separate the central management function from the log collection function:
  - **Panorama mode**: The appliance performs both central management and log collection. This is the default mode. For configuration details, see Deploy Panorama with Default Log Collectors.
  - **Log Collector mode**: The appliance functions as a Dedicated Log Collector. If multiple firewalls forward large volumes of log data, the M-Series appliance in Log Collector mode provides increased scale and performance. In this mode, the appliance has no web interface for administrative access, only a command line interface (CLI). However, you can manage the appliance using the web interface of the Panorama management server (M-Series appliance in Panorama mode or a Panorama virtual appliance). CLI access to an M-Series appliance in Log Collector mode is only necessary for initial setup and debugging. For configuration details, see Deploy Panorama with Dedicated Log Collectors.

The log storage capacity and maximum log collection rate varies by appliance and mode, as described in the following table. For more details and specifications, see the M-100 and M-500 Hardware Reference Guides.

The best appliance for your network depends on whether you must deploy within a virtual infrastructure, your bandwidth resources (some networks benefit from deploying Log Collectors close to the firewalls), and your log storage requirements (see Determine Panorama Log Storage Requirements). The following table summarizes the logging capacities of each appliance.

<table>
<thead>
<tr>
<th>Appliance Capacities and Features</th>
<th>M-500 Appliance</th>
<th>M-100 Appliance</th>
<th>Virtual Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Logging Rate for Panorama management server (M-Series appliance in Panorama mode or Panorama virtual appliance)</td>
<td>20,000 logs/second</td>
<td>10,000 logs/second</td>
<td>10,000 logs/second</td>
</tr>
<tr>
<td>Appliance Capacities and Features</td>
<td>M-500 Appliance</td>
<td>M-100 Appliance</td>
<td>Virtual Appliance</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>--------------------------------------</td>
<td>--------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Maximum Logging Rate for Dedicated Log Collector</td>
<td>50,000 logs/second</td>
<td>30,000 logs/second</td>
<td>Not applicable: the Panorama virtual appliance cannot be a Dedicated Log Collector.</td>
</tr>
<tr>
<td>Maximum Log Storage</td>
<td>8TB (16 RAID drives)</td>
<td>4TB (8 RAID drives)</td>
<td>8TB (2TB for ESXi releases before v5.5)</td>
</tr>
<tr>
<td>Default Log Storage</td>
<td>4TB (8 drives)</td>
<td>1TB (2 drives)</td>
<td>~11GB</td>
</tr>
<tr>
<td>SSD Storage (for logs that M-Series appliances generate)</td>
<td>240GB</td>
<td>120GB</td>
<td>Not applicable</td>
</tr>
<tr>
<td>NFS Attached Log Storage</td>
<td>Not available</td>
<td>Not available</td>
<td>ESXi server only</td>
</tr>
</tbody>
</table>
Centralized Configuration and Deployment Management

Panorama uses *device groups* and *templates* to group firewalls into logical sets that require similar configuration. You use the device groups and templates to centrally manage all configuration elements, policies, and objects on the managed firewalls. Panorama also enables you to centrally manage licenses, software (PAN-OS software, SSL-VPN client software, GlobalProtect agent/app software), and content updates (Applications, Threats, WildFire, and Antivirus).

- **Context Switch—Firewall or Panorama**
- **Templates and Template Stacks**
- **Device Groups**

**Context Switch—Firewall or Panorama**

The Panorama web interface enables you to toggle between a Panorama-centric view and a firewall-centric view by using the Context drop-down at the top-left of every tab. You can set the Context to Panorama to manage firewalls centrally or switch context to the web interface of a specific firewall to configure it locally. The similarity of the Panorama and firewall web interfaces enables you to seamlessly move between them to administer and monitor firewalls.

The Context drop-down lists only the firewalls that are connected to Panorama. For a Device Group and Template administrator, the drop-down lists only the connected firewalls that are within the Access Domains assigned to that administrator. To search a long list, use the Filters within the drop-down.

For firewalls that have a high availability (HA) configuration, the icons have colored backgrounds to indicate HA state (as follows). Knowing the HA state is useful when selecting a firewall context. For example, you generally make firewall-specific configuration changes on the active firewall.

- Green—Active.
- Yellow—Passive or the firewall is initiating (the initiating state lasts for up to 60 seconds after boot up).
- Red—The firewall is non-functional (error state), suspended (an administrator disabled the firewall), or tentative (for a link or path monitoring event in an active/active HA configuration).

**Templates and Template Stacks**

You use templates to configure the settings that enable firewalls to operate on the network. Templates enable you to define a common base configuration using the Network and Device tabs on Panorama. For example, you can use templates to manage interface and zone configurations, server profiles for logging and syslog access, and network profiles for controlling access to zones and IKE gateways. When defining a template, consider assigning firewalls that are the same hardware model and require access to similar network resources, such as gateways and syslog servers.

If your network has groups of firewalls with some group-specific settings and some settings that are common across groups, you can simplify management by assigning the firewalls to a template stack for each group. A template stack is a combination of templates: the assigned firewalls inherit the settings from every template in the stack. This enables you to avoid the redundancy of adding every setting to every template. The following figure illustrates an example deployment in which you assign data center firewalls in the
Asia-Pacific (APAC) region to a stack that has one template with global settings, one template with APAC-specific settings, and one template with data center-specific settings. To manage firewalls in an APAC branch office, you can then re-use the global and APAC-specific templates by adding them to another stack that includes a template with branch-specific settings. Templates in a stack have a configurable priority order that ensures Panorama pushes only one value for any duplicate setting. Panorama evaluates the templates listed in a stack configuration from top to bottom, with higher templates having priority. The following figure illustrates a data center stack in which the data center template has a higher priority than the global template: Panorama pushes the idle timeout value from the data center template and ignores the value from the global template.

Figure: Template Stacks

To accommodate firewalls that have unique settings, you can use templates (single or stacked) to push a limited common base configuration to all firewalls, and in individual firewalls configure firewall-specific settings. Alternatively, you can push a broader common base configuration and in the individual firewalls override certain pushed settings with firewall-specific values. When you override a setting, the firewall saves that setting to its local configuration; Panorama no longer manages the setting. To restore template values after overriding them, you can use Panorama to force the template configuration onto a firewall. For example, after defining a common NTP server in a template and overriding the NTP server configuration on a firewall to accommodate its local time zone, you can later revert to the NTP server defined in the template.

You cannot use templates to set firewall modes: virtual private network (VPN) mode, multiple virtual systems mode (multi-vsys mode), and operational mode (normal, Federal Information Processing Standards [FIPS], or Common Criteria [CC]). For details, see Template Capabilities and Exceptions. However, you can assign firewalls that have non-matching modes to the same template or stack. In such cases, Panorama pushes mode-specific settings only to firewalls that support those modes. As an exception, you can configure Panorama to push the settings of the default vsys in a template to firewalls that don’t support virtual systems or have none configured.

For the relevant procedures, see Manage Templates and Template Stacks.
Device Groups

To use Panorama effectively, you have to group the firewalls in your network into logical units called device groups. A device group enables grouping based on network segmentation, geographic location, organizational function, or any other common aspect of firewalls that require similar policy configurations. Using device groups, you can configure policy rules and the objects they reference. You can organize device group hierarchically, with shared rules and objects at the top, and device group-specific rules and objects at subsequent levels. This enables you to create a hierarchy of rules that enforce how firewalls handle traffic. For example, you can define a set of shared rules as a corporate acceptable use policy. Then, to allow only regional offices to access peer-to-peer traffic such as BitTorrent, you can define a device group rule that Panorama pushes only to the regional offices (or define a shared security rule and target it to the regional offices). For the relevant procedures, see Manage Device Groups. The following topics describe device group concepts and components in more detail:

- Device Group Hierarchy
- Device Group Policies
- Device Group Objects

Device Group Hierarchy

You can Create a Device Group Hierarchy to nest device groups in a tree hierarchy of up to four levels, with lower-level groups inheriting the settings (policy rules and objects) of higher-level groups. At the bottom level, a device group can have parent, grandparent, and great-grandparent device groups (ancestors). At the top level, a device group can have child, grandchild, and great-grandchild device groups (descendants). All device groups inheriting settings from the Shared location—a container at the top of the hierarchy for configurations that are common to all device groups.

Creating a device group hierarchy enables you to organize firewalls based on common policy requirements without redundant configuration. For example, you could configure shared settings that are global to all firewalls, configure device groups with function-specific settings at the first level, and configure device groups with location-specific settings at lower levels. Without a hierarchy, you would have to configure both function- and location-specific settings for every device group in a single level under Shared.

Figure: Device Group Hierarchy

For details on the order in which firewalls evaluate policy rules in a device group hierarchy, see Device Group Policies. For details on overriding the values of objects that device groups inherit from ancestor device groups, see Device Group Objects.
Device Group Policies

Device groups provide a way to implement a layered approach for managing policies across a network of managed firewalls. A firewall evaluates policy rules by layer (shared, device group, and local) and by type (pre-rules, post-rules, and default rules) in the following order from top to bottom. When the firewall receives traffic, it performs the action defined in the first evaluated rule that matches the traffic and disregards all subsequent rules. To change the evaluation order for rules within a particular layer, type, and rulebase (for example, shared Security pre-rules), see Manage the Rule Hierarchy.

<table>
<thead>
<tr>
<th>Evaluation Order</th>
<th>Rule Scope and Description</th>
<th>Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared pre-rules</td>
<td>Panorama pushes shared pre-rules to all the firewalls in all device groups. Panorama pushes device group-specific pre-rules to all the firewalls in a particular device group and its descendant device groups. If a firewall inherits rules from device groups at multiple levels in the device group hierarchy, it evaluates pre-rules in the order of highest to lowest level. This means the firewall first evaluates shared rules and last evaluates the rules of device groups with no descendants. You can use pre-rules to enforce the acceptable use policy of an organization. For example, a pre-rule might block access to specific URL categories or allow Domain Name System (DNS) traffic for all users.</td>
<td>These rules are visible on firewalls but you can only manage them in Panorama.</td>
</tr>
<tr>
<td>Device group pre-rules</td>
<td></td>
<td>A local firewall administrator, or a Panorama administrator who switches to a local firewall context, can edit local firewall rules.</td>
</tr>
<tr>
<td>Local firewall rules</td>
<td>Local rules are specific to a single firewall or virtual system (vsys).</td>
<td>A local firewall administrator, or a Panorama administrator who switches to a local firewall context, can edit local firewall rules.</td>
</tr>
<tr>
<td>Device group post-rules</td>
<td>Panorama pushes shared post-rules to all the firewalls in all device groups. Panorama pushes device group-specific post-rules to all the firewalls in a particular device group and its descendant device groups. If a firewall inherits rules from device groups at multiple levels in the device group hierarchy, it evaluates post-rules in the order of lowest to highest level. This means the firewall first evaluates the rules of device groups with no descendants and last evaluates shared rules. Post-rules typically include rules to deny access to traffic based on the App-ID, User-ID, or service.</td>
<td>These rules are visible on firewalls but you can only manage them in Panorama.</td>
</tr>
<tr>
<td>Shared post-rules</td>
<td></td>
<td>A local firewall administrator, or a Panorama administrator who switches to a local firewall context, can edit local firewall rules.</td>
</tr>
</tbody>
</table>
Panorama Overview

Centralized Configuration and Deployment Management

Whether you view rules on a firewall or in Panorama, the web interface displays them in evaluation order. All the shared, device group, and default rules that the firewall inherits from Panorama are shaded orange. Local firewall rules display between the pre-rules and post-rules.

Figure: Rule Hierarchy

<table>
<thead>
<tr>
<th>Evaluation Order</th>
<th>Rule Scope and Description</th>
<th>Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>intrazone-default</td>
<td>The default rules apply only to the Security rulebase, and are predefined on Panorama (at the Shared level) and the firewall (in each vsys). These rules specify how PAN-OS handles traffic that doesn’t match any other rule. The intrazone-default rule allows all traffic within a zone. The interzone-default rule denies all traffic between zones. If you override default rules, their order of precedence runs from the lowest context to the highest: overridden settings at the firewall level take precedence over settings at the device group level, which take precedence over settings at the Shared level.</td>
<td>Default rules are initially read-only, either because they are part of the predefined configuration or because Panorama pushed them to firewalls. However, you can override the rule settings for tags, action, logging, and security profiles. The context determines the level at which you can override the rules: • Panorama—At the Shared or device group level, you can override default rules that are part of the predefined configuration. • Firewall—You can override default rules that are part of the predefined configuration on the firewall or vsys, or that Panorama pushed from the Shared location or a device group.</td>
</tr>
<tr>
<td>interzone-default</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Device Group Objects

Objects are configuration elements that policy rules reference, for example: IP addresses, URL categories, security profiles, users, services, and applications. Rules of any type (pre-rules, post-rules, default rules, and rules locally defined on a firewall) and any rulebase (Security, NAT, QoS, Policy Based Forwarding, Decryption, Application Override, Captive Portal, and DoS Protection) can reference objects. You can reuse an object in any number of rules that have the same scope as that object in the Device Group Hierarchy. For example, if you add an object to the Shared location, all rules in the hierarchy can reference that shared object because all device groups inherit objects from Shared. If you add an object to a particular device group, only the rules in that device group and its descendant device groups can reference that device group object. If object values in a device group must differ from those inherited from an ancestor device group, you can Override inherited object values. You can also Revert to Inherited Object Values at any time. When you Create Objects for Use in Shared or Device Group Policy once and use them many times, you reduce administrative overhead and ensure consistency across firewall policies.
You can configure how Panorama handles objects system-wide:

- **Pushing unused objects**—By default, Panorama pushes all objects to firewalls regardless of whether any shared or device group policy rules reference the objects. Optionally, you can configure Panorama to push only referenced objects. For details, see Manage Unused Shared Objects.

- **Precedence of ancestor and descendant objects**—By default, when device groups at multiple levels in the hierarchy have an object with the same name but different values (because of overrides, as an example), policy rules in a descendant device group use the object values in that descendant instead of object values inherited from ancestor device groups or Shared. Optionally, you can reverse this order of precedence to push values from Shared or the highest ancestor containing the object to all descendant device groups. For details, see Manage Precedence of Inherited Objects.
Centralized Logging and Reporting

Panorama aggregates data from all managed firewalls and provides visibility across all the traffic on the network. It also provides an audit trail for all policy modifications and configuration changes made to the managed firewalls. In addition to aggregating logs, Panorama can aggregate and forward Simple Network Management Protocol (SNMP) traps, email notifications, and syslog messages to an external destination.

The Application Command Center (ACC) on Panorama provides a single pane for unified reporting across all the firewalls. It enables you to centrally Monitor Network Activity, to analyze, investigate, and report on traffic and security incidents. On Panorama, you can view logs and generate reports from logs forwarded to Panorama or to the managed Log Collectors, if configured, or you can query the managed firewalls directly. For example, you can generate reports about traffic, threat, and/or user activity in the managed network based on logs stored on Panorama (and the managed collectors) or by accessing the logs stored locally on the managed firewalls.

If you choose not to Configure Log Forwarding to Panorama, you can schedule reports to run on each managed firewall and forward the results to Panorama for a combined view of user activity and network traffic. Although this view does not provide a granular drill-down on specific data and activities, it still provides a unified reporting approach.

- **Logging Options**
- **Managed Collectors and Collector Groups**
- **Caveats for a Collector Group with Multiple Log Collectors**
- **Centralized Reporting**

### Logging Options

Both the Panorama virtual appliance and M-Series appliance can collect logs that the managed firewalls forward. You can then Configure Log Forwarding from Panorama to External Destinations (syslog server, email server, or Simple Network Management Protocol [SNMP] trap server). The logging options vary on each Panorama appliance.

The PA-7000 Series firewall can’t forward logs to Panorama, only to external services directly. However, when you monitor logs or generate reports for a device group that includes a PA-7000 Series firewall, Panorama queries the firewall in real-time to display its log data.

<table>
<thead>
<tr>
<th>Panorama Appliance</th>
<th>Logging Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual appliance</td>
<td>Offers three logging options:</td>
</tr>
<tr>
<td></td>
<td>• Use the approximately 11GB of internal storage space allocated for logging as soon as you install the virtual appliance.</td>
</tr>
<tr>
<td></td>
<td>• Add a virtual disk. Panorama running on VMware vCloud Air or ESXi 5.5 and later versions can support a virtual disk of up to 8TB. Earlier versions of the ESXi server support a virtual disk of up to 2TB.</td>
</tr>
<tr>
<td></td>
<td>• Mount a Network File System (NFS) datastore in which you can configure the storage capacity that is allocated for logging.</td>
</tr>
</tbody>
</table>
Centralized Logging and Reporting

Managed Collectors and Collector Groups

A Log Collector can be local to an M-Series appliance in Panorama mode (default Log Collector) or can be an M-Series appliance in Log Collector mode (Dedicated Log Collector). Because you use Panorama to configure and manage Log Collectors, they are also known as managed collectors. An M-Series appliance in Panorama mode or a Panorama virtual appliance can manage Dedicated Log Collectors. To administer Dedicated Log Collectors using the Panorama web interface, you must add them as managed collectors. Otherwise, administrative access to a Dedicated Log Collector is only available through its CLI using the default administrative user (admin) account. Dedicated Log Collectors do not support additional administrative user accounts.

A Collector Group is 1 to 16 managed collectors that operate as a single logical log collection unit. If the group contains Dedicated Log Collectors, the logs are uniformly distributed across all the disks in each Log Collector and across all members in the Collector Group. This distribution maximizes the use of the available storage space. To manage a Log Collector, you must add it to a Collector Group. If you assign more than one Log Collector to a Collector Group, see Caveats for a Collector Group with Multiple Log Collectors.

The Collector Group configuration specifies which managed firewalls can send logs to the Log Collectors in the group. After you configure the Log Collectors and enable the firewalls to forward logs, each firewall forwards its logs to the assigned Log Collector.

Managed collectors and Collector Groups are integral to a distributed log collection deployment on Panorama. A distributed log collection deployment allows for easy scalability and incremental addition of Dedicated Log Collectors as your logging needs grow. The M-Series appliance in Panorama mode can log to its default Collector Group and then be expanded to a distributed log collection deployment with one or more Collector Groups that include Dedicated Log Collectors.

To configure Log Collectors and Collector Groups, see Manage Log Collection.

Caveats for a Collector Group with Multiple Log Collectors

You can Configure a Collector Group with multiple Log Collectors (up to 16) to ensure log redundancy, increase the log retention period, or accommodate logging rates that exceed the capacity of a single Log Collector (see Panorama Platforms for capacity information). All the Log Collectors in any particular Collector
Group must be the same model, such as all M-500 appliances or all M-100 appliances. For example, if a single managed firewall generates 16TB of logs, the Collector Group that receives those logs will require at least four Log Collectors that are M-100 appliances or two Log Collectors that are M-500 appliances.

A Collector Group with multiple Log Collectors uses the available storage space as one logical unit and uniformly distributes the logs across all its Log Collectors. The log distribution is based on the disk capacity of the Log Collectors (1TB to 8TB, depending on the number of disk pairs and the M-Series appliance) and a hash algorithm that dynamically decides which Log Collector owns the logs and writes to disk. Although Panorama uses a preference list to prioritize the list of Log Collectors to which a managed firewall can forward logs, Panorama does not necessarily write the logs to the first Log Collector specified in the preference list. For example, consider the following preference list:

<table>
<thead>
<tr>
<th>Managed Firewall</th>
<th>Log Forwarding Preference List Defined on a Collector Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW1</td>
<td>L1,L2,L3</td>
</tr>
<tr>
<td>FW2</td>
<td>L4,L5,L6</td>
</tr>
</tbody>
</table>

Using this list, FW1 will forward logs to L1, its primary Log Collector, but the hash algorithm could determine that the logs will be written on L2. If L2 becomes inaccessible or has a chassis failure, FW1 will not know about its failure because it is still able to connect to L1, its primary Log Collector.

In the case where a Collector Group has only one Log Collector and the Log Collector fails, the firewall stores the logs to its HDD/SSD (the available storage space varies by hardware model), and resumes forwarding logs to the Log Collector where it left off before the failure occurred as soon as connectivity is restored.

With multiple Log Collectors in a Collector Group, the firewall does not buffer logs to its local storage when it can connect to its primary Log Collector. Therefore, FW1 will continue sending logs to L1. Because L2 is unavailable, the primary Log Collector L1 buffers the logs to its HDD, which has 10GB of log space. If L2 remains unavailable and the logs pending for L2 exceed 10GB, L1 will overwrite the older log entries to continue logging. In such an event, loss of logs is a risk.
Palo Alto Networks recommends the following mitigations if using multiple Log Collectors in a Collector Group:

- Enable log redundancy when you Configure a Collector Group. This ensures that no logs are lost if any one Log Collector in the Collector Group becomes unavailable. Each log will have two copies and each copy will reside on a different Log Collector. Log redundancy is available only if each Log Collector in the Collector Group has the same number of logging disks.

  Because enabling redundancy creates more logs, this configuration requires more storage capacity. When a Collector Group runs out of space, it deletes older logs.

- Obtain an On-Site-Spare (OSS) to enable prompt replacement if a Log Collector failure occurs.

- In addition to forwarding logs to Panorama, configure forwarding to an external service as backup storage. The external service can be a syslog server, email server, or Simple Network Management Protocol (SNMP) trap server.

Centralized Reporting

Panorama aggregates logs from all managed firewalls and enables reporting on the aggregated data for a global view of application use, user activity, and traffic patterns across the entire network infrastructure. As soon as the firewalls are added to Panorama, the ACC can display all traffic traversing your network. With logging enabled, clicking into a log entry in the ACC provides direct access to granular details about the application.

For generating reports, Panorama uses two sources: the local Panorama database and the remote firewalls that it manages. The Panorama database refers to the local storage on Panorama that is allocated for storing both summarized logs and some detailed logs. If you have a distributed Log Collection deployment, the Panorama database includes the local storage on Panorama and all the managed Log Collectors. Panorama summarizes the information—traffic, application, threat—collected from all managed firewalls at 15-minute intervals. Using the local Panorama database allows for faster response times, however, if you prefer to not forward logs to Panorama, Panorama can directly access the remote firewall and run reports on data that is stored locally on the managed firewalls.

Panorama offers more than 40 predefined reports that can be used as is, or they can be customized by combining elements of other reports to generate custom reports and report groups that can be saved. Reports can be generated on demand, on a recurring schedule, and can be scheduled for email delivery.
These reports provide information on the user and the context so that you correlate events and identify patterns, trends, and potential areas of interest. With the integrated approach to logging and reporting, the ACC enables correlation of entries from multiple logs relating to the same event.

For more information, see Monitor Network Activity.
Panorama Commit and Validation Operations

When you are ready to activate changes that you made to the candidate configuration on Panorama or to push changes to the firewalls and Log Collectors that Panorama manages, you can Preview, Validate, or Commit Configuration Changes. For example, if you add a Log Collector to the Panorama configuration, firewalls cannot send logs to that Log Collector until you commit the change to Panorama and then commit to the Collector Group that contains the Log Collector. Panorama queues commit operations so that you can initiate a new commit while a previous commit is in progress. If the queue already has the maximum of ten administrator-initiated commits, Panorama must process a pending commit before you can initiate a new commit. You can also Use the Panorama Task Manager to cancel pending commits or to see details about commits that are pending, in progress, completed, or failed. To check which changes a commit will activate, you can run a commit preview.

When you initiate a commit, Panorama checks the validity of the changes before activating them. The validation output displays conditions that block the commit (errors) or that are important to know even though they don’t block the commit (warnings). For example, validation could indicate an invalid route destination that you need to fix for the commit to succeed. To identify and fix configuration errors before initiating a commit, you can validate changes without committing. A pre-commit validation displays the same errors and warnings as a commit, including reference errors, rule shadowing, and application dependency warnings. Pre-commit validations are useful if your organization allows commits only within certain time windows; you can find and fix errors before commit time to avoid failures that could cause you to miss a window.

For details on candidate and running configurations, see Manage Panorama and Firewall Configuration Backups. To prevent multiple administrators from making configuration changes during concurrent sessions, see Manage Locks for Restricting Configuration Changes.
Role-Based Access Control

Role-based access control (RBAC) enables you to define the privileges and responsibilities of administrative users (administrators). Every administrator must have a user account that specifies a role and authentication method. Administrative Roles define access to specific configuration settings, logs, and reports within Panorama and firewall contexts. For Device Group and Template administrators, you can map roles to Access Domains, which define access to specific device groups, templates, and firewalls (through context switching). By combining each access domain with a role, you can enforce the separation of information among the functional or regional areas of your organization. For example, you can limit an administrator to monitoring activities for data center firewalls but allow that administrator to set policies for test lab firewalls. By default, every Panorama appliance (virtual appliance or M-Series appliance) has a predefined administrative account (admin) that provides full read-write access (superuser access) to all functional areas and to all device groups, templates, and firewalls. For each administrator, you can define the minimum password complexity, a password profile, and an authentication profile that determines how Panorama verifies user access credentials.

Instead of using the default account for all administrators, it is a best practice to create a separate administrative account for each person who needs access to the administrative or reporting functions on Panorama. This provides better protection against unauthorized configuration changes and enables Panorama to log and identify the actions of each administrator.

- Administrative Roles
- Authentication Profiles and Sequences
- Access Domains
- Administrative Authentication

Administrative Roles

You configure administrator accounts based on the security requirements of your organization, any existing authentication services with which to integrate, and the required administrative roles. A role defines the type of system access that is available to an administrator. You can define and restrict access as broadly or granularly as required, depending on the security requirements of your organization. For example, you might decide that a data center administrator can have access to all device and networking configurations, but a security administrator can control only security policy definitions, while other key individuals can have limited CLI or XML API access. The role types are:

- **Dynamic Roles**—These are built-in roles that provide access to Panorama and managed firewalls. When new features are added, Panorama automatically updates the definitions of dynamic roles; you never need to manually update them. The following table lists the access privileges associated with dynamic roles.

<table>
<thead>
<tr>
<th>Dynamic Role</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Superuser</td>
<td>Full read-write access to Panorama</td>
</tr>
<tr>
<td>Superuser (read-only)</td>
<td>Read-only access to Panorama</td>
</tr>
</tbody>
</table>
Role-Based Access Control

Panorama Overview

- **Admin Role Profiles**—To provide more granular access control over the functional areas of the web interface, CLI, and XML API, you can create custom roles. When new features are added to the product, you must update the roles with corresponding access privileges: Panorama does not automatically add new features to custom role definitions. You select one of the following profile types when you Configure an Admin Role Profile.

<table>
<thead>
<tr>
<th>Admin Role Profile</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panorama</td>
<td>For these roles, you can assign read-write access, read-only access, or no access to all the Panorama features that are available to the superuser dynamic role except the management of Panorama administrators and Panorama roles. For the latter two features, you can assign read-only access or no access, but you cannot assign read-write access. An example use of a Panorama role would be for security administrators who require access to security policy definitions, logs, and reports on Panorama.</td>
</tr>
</tbody>
</table>
| Device Group and Template   | For these roles, you can assign read-write access, read-only access, or no access to specific functional areas within device groups, templates, and firewall contexts. By combining these roles with Access Domains, you can enforce the separation of information among the functional or regional areas of your organization. Device Group and Template roles have the following limitations:  
  - No access to the CLI or XML API  
  - No access to configuration or system logs  
  - No access to VM information sources  
  - In the Panorama tab, access is limited to:  
    - Device deployment features (read-write, read-only, or no access)  
    - The device groups specified in the administrator account (read-write, read-only, or no access)  
    - The templates and managed firewalls specified in the administrator account (read-only or no access)  
  An example use of this role would be for administrators in your operations staff who require access to the device and network configuration areas of the web interface for specific device groups and/or templates. |

**Authentication Profiles and Sequences**

An authentication profile specifies the authentication service that validates the credentials of an administrator during login and defines how Panorama accesses the service. If you create a local administrator account on Panorama, you can authenticate the administrator to the local database, use an external service (RADIUS, TACACS+, LDAP, or Kerberos server), or use Kerberos single sign-on (SSO). If you use an external service, you must configure a server profile before you Configure an Admin Role Profile. If you want to use an external service for both account administration (instead of creating local accounts) and for authentication, you must Configure RADIUS Vendor-Specific Attributes for Administrator Authentication.
Some environments have multiple databases for different users and user groups. To authenticate to multiple authentication sources (for example, local database and LDAP), configure an authentication sequence. An authentication sequence is a ranked order of authentication profiles that an administrator is matched against when logging in. Panorama checks against the local database first, and then checks each profile in sequence until the administrator is successfully authenticated. The administrator is denied access to Panorama only if authentication fails for all the profiles defined in the authentication sequence.

Access Domains

Access domains control administrative access to specific device groups (to manage policies and objects) and templates (to manage network and device settings), and also control the ability to switch context to the web interface of managed firewalls. Access domains apply only to administrators with Device Group and Template roles. By combining access domains with Administrative Roles, you can enforce the separation of information among the functional or regional areas of your organization.

You can manage access domains locally or by using RADIUS Vendor-Specific Attributes (VSAs). To use RADIUS VSAs, your network requires an existing RADIUS server and you must configure a RADIUS server profile to define how Panorama accesses the server. On the RADIUS server, you define a VSA attribute number and value for each administrator. The value defined must match the access domain configured on Panorama. When an administrator tries to log in to Panorama, Panorama queries the RADIUS server for the administrator access domain and attribute number. Based on the response from the RADIUS server, the administrator is authorized for access and is restricted to the firewalls, virtual systems, device groups, and templates that are assigned to the access domain.

For the relevant procedures, see:
- Configure an Access Domain.
- Configure RADIUS Vendor-Specific Attributes for Administrator Authentication.

Administrative Authentication

The following methods are available to authenticate Panorama administrators:

- **Local administrator account with local authentication**—Both the administrator account credentials and the authentication mechanisms are local to Panorama. To further secure the local administrator account, create a password profile that defines a validity period for passwords and set Panorama-wide password complexity settings. For details on how to configure this type of administrative access, see Configure an Administrator with Kerberos SSO, External, or Local Authentication.

- **Local administrator account with certificate- or key-based authentication**—With this option, the administrator accounts are local to Panorama, but authentication is based on Secure Shell (SSH) keys (for CLI access) or client certificates/common access cards (for the web interface). For details on how to configure this type of administrative access, see Configure an Administrator with Certificate-Based Authentication for the Web Interface and Configure an Administrator with SSH Key-Based Authentication for the CLI.

- **Local administrator account with external authentication**—The administrator accounts are managed on Panorama, but existing external authentication services (LDAP, Kerberos, TACACS+, or RADIUS) handle the authentication functions. If your network supports Kerberos single sign-on (SSO), you can configure
external authentication as an alternative in case SSO fails. For details on how to configure this type of administrative access, see Configure an Administrator with Kerberos SSO, External, or Local Authentication.

- **External administrator account and authentication**—An external RADIUS server handles account administration and authentication. To use this option, you must define Vendor-Specific Attributes (VSAs) on your RADIUS server that map to the administrator roles and access domains. For a high-level overview of the process, see Configure RADIUS Vendor-Specific Attributes for Administrator Authentication. For details on how to configure this type of administrative access, refer to Radius Vendor-Specific Attributes (VSAs).
Panorama Recommended Deployments

A Panorama deployment comprises the Panorama management server (which has a browser-based interface), optional Log Collectors, and the Palo Alto Networks firewalls that Panorama manages. The recommended deployments are:

- Panorama for Centralized Management and Reporting
- Panorama in a Distributed Log Collection Deployment

For the procedures to configure the most typical log collection deployments, see Log Collection Deployments.

Panorama for Centralized Management and Reporting

The following diagram illustrates how you can deploy the Panorama virtual appliance or M-Series appliance in a redundant configuration for the following benefits:

- **Centralized management**—Centralized policy and firewall management that allows for rapid deployment and management of up to one thousand firewalls.
- **Visibility**—Centralized logging and reporting to analyze and report on user-generated traffic and potential threats.
- **Role-based access control**—Appropriate levels of administrative control at the firewall level or global level for administration and management.
Panorama in a Distributed Log Collection Deployment

You can deploy the hardware-based Panorama—the M-Series appliance—either as a Panorama management server that performs management and log collection functions or as a Dedicated Log Collector that provides a comprehensive log collection solution for the firewalls on your network. Using the M-Series appliance as a Log Collector allows for a more robust environment where the log collection process is offloaded to a dedicated appliance. Using a dedicated appliance in a distributed log collection (DLC) deployment provides redundancy, improved scalability, and capacity for longer term log storage.

In a DLC deployment, the Panorama management server (Panorama virtual appliance or an M-Series appliance in Panorama mode) manages the firewalls and the Log Collectors. Using Panorama, you configure the firewalls to send logs to one or more Log Collectors. You can then use Panorama to query the Log Collectors and provide an aggregated view of network traffic. In a DLC configuration, you can access the logs stored on the Log Collectors from both the primary and secondary Panorama peers in a high availability (HA) pair.

In the following topology, the Panorama peers in an HA configuration manage the deployment and configuration of firewalls. This solution provides the following benefits:

- Enables the Panorama management server to use more resources for management functions.
- Provides high-volume log storage on a dedicated hardware appliance.
- Enables higher logging rates.
- Provides horizontal scalability and redundancy with RAID 1 storage.
- Optimizes bandwidth resources in networks where more bandwidth is available for firewalls to send logs to nearby Log Collectors than to a remote Panorama management server.
- Enables you to meet regional regulatory requirements (for example, regulations might not allow logs to leave a particular region).
Plan Your Deployment

- Determine the management approach. Do you plan to use Panorama to centrally configure and manage the policies, to centrally administer software, content and license updates, and/or centralize logging and reporting across the managed firewalls in the network?

  If you already deployed and configured the Palo Alto Networks firewalls on your network, determine whether to transition the firewalls to centralized management. This process requires a migration of all configuration and policies from your firewalls to Panorama. For details, see Transition a Firewall to Panorama Management.

- Verify the Panorama and firewall software versions. Panorama can manage firewalls running PAN-OS versions that match the Panorama version or are earlier than the Panorama version. The exception is that Panorama 6.1 and later versions cannot push configurations to firewalls running PAN-OS 6.0.0 through 6.0.3. Panorama cannot manage firewalls that run a later PAN-OS version than the Panorama version. For example, Panorama 6.0 cannot manage firewalls running PAN-OS 7.0. For versions within the same feature release, although Panorama can manage firewalls running a later version of PAN-OS, we recommend that Panorama run the same version or a later version. For example, if Panorama runs 7.0.3, it is recommended that all managed firewalls run PAN-OS 7.0.3 or earlier versions.

- Plan to use the same URL filtering database (BrightCloud or PAN-DB) across all managed firewalls. If some firewalls are using the BrightCloud database and others are using PAN-DB, Panorama can only manage security rules for one or the other URL filtering database. URL filtering rules for the other database must be managed locally on the firewalls that use that database.

- Plan to use Panorama in a high availability configuration; set it up as an active/passive high availability pair. See Panorama High Availability.

- Estimate the log storage capacity your network needs to meet security and compliance requirements. Consider such factors as the network topology, number of firewalls sending logs, type of log traffic (for example, URL Filtering and Threat logs versus Traffic logs), the rate at which firewalls generate logs, and the number of days for which you want to store logs on Panorama. For details, see Determine Panorama Log Storage Requirements.

- For meaningful reports on network activity, plan a logging solution:
  - Do you need to forward logs to a syslog server, in addition to Panorama?
  - If you need a long-term storage solution, do you have a Security Information and Event Management (SIEM) solution, such as Splunk or ArcSight, to which you can forward logs?
  - Do you need redundancy in logging?

    With Panorama virtual appliances in HA, each peer can log to its virtual disk. The managed firewalls can send logs to both peers in the HA pair. This option provides redundancy in logging. Panorama running on VMware vCloud Air or ESXi 5.5 and later versions can support a virtual disk of up to 8TB. Earlier versions of the ESXi server support a virtual disk of up to 2TB.

    If you use Dedicated Log Collectors (M-Series appliances in Log Collector mode), you can enable redundancy to ensure that no logs are lost if any one Log Collector in the Collector Group becomes unavailable. Each log will have two copies and each copy will reside on a different Log Collector.

    Will you log to a Network File System (NFS)? Only the Panorama virtual appliance supports NFS. Consider using NFS if Panorama requires more than 8TB of log storage capacity and but doesn’t manage Dedicated Log Collectors. If using NFS, note that the managed firewalls can send logs only to the primary peer in the HA pair, and only the active-primary Panorama is mounted to the NFS and can write to it.

    If your logging solution includes M-Series appliances, by default they use the management (MGT) interface for configuration, log collection, and Collector Group communication. However, it is a best practice to use the Eth1 or Eth2 interfaces for log collection and Collector Group communication to...
improve security, control traffic prioritization, performance, and scalability. Determine whether your solution would benefit from using separate interfaces for these functions. For details, see Set Up the M-Series Appliance.

- Determine what access privileges, roles, and permissions administrators require to access to the managed firewalls and Panorama. See Set Up Administrative Access to Panorama.

- Plan the required Device Groups. Consider whether to group firewalls based on function, security policy, geographic location, or network segmentation. An example of a function-based device group is one that contains all the firewalls that a Research and Development team uses. Consider whether to create smaller device groups based on commonality, larger device groups to scale more easily, or a Device Group Hierarchy to simplify complex layers of administration.

- Plan a layering strategy for administering policies. Consider how firewalls inherit and evaluate policy rules within the Device Group Hierarchy, and how to best implement shared rules, device-group rules, and firewall-specific rules to meet your network needs. For visibility and centralized policy management, consider using Panorama for administering rules even if you need firewall-specific exceptions for shared or device group rules. If necessary, you can Push a Policy Rule to a Subset of Firewalls within a device group.

- Plan the organization of your firewalls based on how they inherit network configuration settings from Templates and Template Stacks. For example, consider assigning firewalls to templates based on hardware models, geographic proximity, and similar network needs for time zones, a DNS server, and interface settings.
Deploy Panorama: Task Overview

The following task list summarizes the steps to get started with Panorama. For an example of how to use Panorama for central management, see Use Case: Configure Firewalls Using Panorama.

<table>
<thead>
<tr>
<th>Deploy Panorama: Task Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
</tr>
<tr>
<td>Step 2</td>
</tr>
<tr>
<td>Step 3</td>
</tr>
<tr>
<td>Step 4</td>
</tr>
<tr>
<td>Step 5</td>
</tr>
<tr>
<td>Step 6</td>
</tr>
<tr>
<td>Step 7</td>
</tr>
<tr>
<td>Step 8</td>
</tr>
<tr>
<td>Step 9</td>
</tr>
</tbody>
</table>
Set Up Panorama

For centralized reporting and cohesive policy management across all the firewalls on your network, Panorama can be deployed as a virtual appliance or as a hardware appliance (the M-100 or M-500 appliance). The following topics describe how to set up Panorama on your network:

- Determine Panorama Log Storage Requirements
- Set Up the Panorama Virtual Appliance
- Set Up the M-Series Appliance
- Register Panorama and Install Licenses
- Install Content and Software Updates for Panorama
- Transition to a Different Panorama Platform
- Access and Navigate Panorama Management Interfaces
- Set Up Administrative Access to Panorama
Determine Panorama Log Storage Requirements

When you Plan Your Deployment, estimate how much log storage capacity Panorama requires to determine which Panorama Platforms to deploy, whether to expand the storage on those appliances beyond their default capacities, whether to deploy Dedicated Log Collectors, and whether to Configure Log Forwarding from Panorama to External Destinations. When Panorama reaches the maximum capacity, it automatically deletes older logs to create space for new ones. Therefore, to ensure that log retention meets your needs, you should configure any additional storage during the Panorama setup stage. To expand log storage capacity during or after setup, see Expand Log Storage Capacity on the Panorama Virtual Appliance or Increase Storage on the M-Series Appliance.

Perform the following steps to determine the approximate log storage that Panorama requires. For details and use cases, refer to Panorama Sizing and Design Guide.

### Determine Panorama Log Storage Requirements

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Step 1** | Determine the log retention requirements of your organization. Factors that affect log retention requirements include:  
- IT policy of your organization  
- Log redundancy—If you enable log redundancy when you Configure a Collector Group, each log will have two copies, which doubles your required log storage capacity.  
- Regulatory requirements, such as those specified by the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act, and Health Insurance Portability and Accountability Act (HIPAA)  
If your organization requires the removal of logs after a certain period, you can set the expiration period for each log type. You can also set a storage quota for each log type as a percentage of the total space if you need to prioritize log retention by type. For details, see Manage Storage Quotas and Expiration Periods for Logs and Reports.  |
| **Step 2** | Determine the average daily logging rates.  
Do this multiple times each day at peak and non-peak times to estimate the average. The more often you sample the rates, the more accurate your estimate.  
1. Display the current log generation rate in logs per second:  
   - If Panorama is not yet collecting logs, access the CLI of each firewall, run the following command, and calculate the total rates for all the firewalls. This command displays the number of logs received in the last second.  
     ```
     > debug log-receiver statistics
     ```  
   - If Panorama is already collecting logs, run the following command at the CLI of each appliance that receives logs (Panorama management server or Dedicated Log Collector) and calculate the total rates. This command gives the average logging rate for the last five minutes.  
     ```
     > debug log-collector log-collection-stats show incoming-logs
     ```  
   You can also use an SNMP manager to determine the logging rates of M-Series appliances by monitoring the panLcLogRate object (OID 1.3.6.1.4.1.25461.2.3.30.1.1).  
2. Calculate the average of the sampled rates.  
3. Calculate the daily logging rate by multiplying the average logs-per-second by 86,400.  |
### Determine Panorama Log Storage Requirements (Continued)

**Step 3**  Estimate the required storage capacity.  
This formula provides only an estimate; the exact amount of required storage will differ from the formula result.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Estimate the required storage capacity.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This formula provides only an estimate; the exact amount of required storage will differ from the formula result.</td>
</tr>
</tbody>
</table>

**Use the formula:**

\[ \text{required_storage_duration} \times \text{average_log_size} \times \text{average_logging_rate} \]

The average log size varies considerably by log type. However, you can use 360 bytes as an approximate average log size.

For example, if Panorama must store logs for 30 days and the average total logging rate for all firewalls is 21,254,400 logs per day, then the required log storage capacity is: $30 \times 360 \times 21,254,400 = 229,547,520,000$ bytes (approximately 230GB).
Set Up the Panorama Virtual Appliance

The Panorama virtual appliance consolidates the Panorama management and logging functions into a single virtual machine. To enable the use of an existing VMware virtual infrastructure to centrally administer and monitor Palo Alto Networks firewalls, install Panorama on an ESXi server or in vCloud Air.

Setup Prerequisites for the Panorama Virtual Appliance

Complete the following tasks before you Install the Panorama Virtual Appliance:

- Use your browser to access the Palo Alto Networks Customer Support web site and Register Panorama. You will need the Panorama serial number that you received in the order fulfillment email. After registering Panorama, you can access the Panorama software downloads page.
- Review the supported Panorama hypervisors to verify the hypervisor meets the minimum version requirements to deploy Panorama.
- If you will install Panorama on a VMware ESXi server, verify that the server meets the following minimum system requirements. These requirements apply to Panorama 5.1 and later releases.
Set Up Panorama

Minimum System Requirements for Panorama on a VMware ESXi Server

- 64-bit kernel-based VMware ESXi 5.1, 5.5, 6.0, or 6.5. Panorama running on ESXi 5.5 and later versions supports a virtual disk of up to 8TB. Panorama running on an earlier ESXi version supports a virtual disk of up to 2TB. The minimum supported version of the virtual hardware family type (also known as the VMware virtual hardware version) on the ESXi server is vmx-09.
- A client computer with one of the following: VMware vSphere Client or VMware Infrastructure Client that is compatible with your ESXi server.
- Use the following guidelines for allocating CPU and memory:
  - 1–10 managed firewalls: 4 cores and 4GB.
  - 11–50 managed firewalls: 8 cores and 8GB.
  - 51-1,000 managed firewalls: 8 cores and 16GB.
- 52GB disk space.
  Panorama allocates approximately 11GB for log storage. Increasing the disk space doesn't increase the log storage capacity. To Expand Log Storage Capacity on the Panorama Virtual Appliance, you must add another virtual disk or set up access to a Network File System (NFS) datastore.

Install the Panorama Virtual Appliance

Before installation, complete the Setup Prerequisites for the Panorama Virtual Appliance.

- ▲ Install Panorama on an ESXi Server
- ▲ Install Panorama in vCloud Air
- ▲ Support for VMware Tools on the Panorama Virtual Appliance

Install Panorama on an ESXi Server

Use these instructions to install a new Panorama virtual appliance on a VMware ESXi server. If you are upgrading your existing Panorama virtual appliance, skip to Install Content and Software Updates for Panorama.

Install Panorama on an ESXi Server

Step 1 Download the Panorama base image
Open Virtual Appliance (OVA) file.

1. Use your browser to access the Palo Alto Networks software downloads site. (If you can't log in, go to the Palo Alto Networks Customer Support web site for assistance.)
2. In the Panorama Base Images section, Download column, click the link for the desired release to download the OVA file.
**Install Panorama on an ESXi Server (Continued)**

**Step 2** Install Panorama.

1. Launch the VMware vSphere Client and connect to the VMware server.
2. Select **File > Deploy OVF Template**.
3. **Browse** to select the Panorama OVA file and click **Next**.
4. Confirm that the product name and description match the downloaded version, and click **Next**.
5. Enter a descriptive name for the Panorama virtual appliance, and click **Next**.
6. Select a **Datastore Location** on which to install the Panorama image, and click **Next**.
   Regardless of the disk size, Panorama uses approximately 11GB for log storage. Increasing the disk size doesn’t increase the log storage capacity. To **Expand Log Storage Capacity on the Panorama Virtual Appliance**, you must add another virtual disk or set up access to a Network File System (NFS) datastore.
7. Select your preferred **Disk Provisioning** disk format, and click **Next**.
   Consider your business needs when selecting the disk provisioning format. For more information, regarding the disk provisioning performance considerations, refer to the **VMware Thick vs Thin Disks and All Flash Arrays** document, or additional VMware documentation.
8. Specify which networks in the inventory to use for the Panorama virtual appliance.
9. Confirm the selected options and click **Finish** to start the installation process.
10. When the installation completes, right-click the Panorama virtual appliance and **Edit Settings** as follows:
   a. Select the **Hardware** tab and allocate **Memory** based on how many firewalls Panorama will manage:
      - 1–10 firewalls: 4GB
      - 11–50 firewalls: 8GB
      - 51–1,000 firewalls: 16GB
   b. Set the **SCSI Controller** to **LSI Logic Parallel**.
   c. Click **OK** to save your changes.

**Step 3** Power on the Panorama virtual appliance.

In the vSphere Client, right-click the Panorama virtual appliance and select **Power > Power On**.
When the Panorama virtual appliance boots, the installation process is complete. You are then ready to **Perform Initial Configuration of the Panorama Virtual Appliance**.

**Install Panorama in vCloud Air**

Use these instructions to install a new Panorama virtual appliance in VMware vCloud Air. If you are upgrading a Panorama virtual appliance deployed in vCloud Air, skip to **Install Content and Software Updates for Panorama**.
### Install Panorama in vCloud Air

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Download the Panorama base image Open Virtual Appliance (OVA) file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Go to the <a href="https://www.paloaltonetworks.com/support/downloads/#/">Palo Alto Networks software downloads site</a>. (If you can't log in, go to the <a href="https://www.paloaltonetworks.com/support/">Palo Alto Networks Customer Support web site</a>.)</td>
</tr>
<tr>
<td>2.</td>
<td>In the Panorama Base Images section, Download column, click the link for the desired release to download the OVA file.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Import the Panorama image to the vCloud Air catalog.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For details on these steps, refer to the <a href="https://www.vmware.com/support/pubs/ovf_tool_user_guide.html">OVF Tool User’s Guide</a>.</td>
</tr>
<tr>
<td>1.</td>
<td>Install the OVF Tool on your client system.</td>
</tr>
<tr>
<td>2.</td>
<td>Access the client system CLI.</td>
</tr>
<tr>
<td>3.</td>
<td>Navigate to the OVF Tool directory.  For example: C:\Program Files\VMware\VMware OVF Tool</td>
</tr>
<tr>
<td>4.</td>
<td>Convert the OVA file to an OVF package:  <code>ovftool.exe &lt;OVA-file-pathname&gt; &lt;OVF-file-pathname&gt;</code></td>
</tr>
<tr>
<td>5.</td>
<td>Use a browser to access the vCloud Air web console, select your Virtual Private Cloud OnDemand location, and record the browser URL. You will use the URL information to complete the next step. The URL format is:  <code>https://&lt;virtual-cloud-location&gt;.vchs.vmware.com/compute/cloud/org/&lt;vCloud-account-number&gt;/#/#/catalogVAppTemplateList?catalog=&lt;catalog-ID&gt;</code>.</td>
</tr>
<tr>
<td>6.</td>
<td>Import the OVF package, using the information from the vCloud Air URL to complete the <code>&lt;virtual-cloud-location&gt;</code>, <code>&lt;vCloud-account-number&gt;</code>, and <code>&lt;catalog-ID&gt;</code> variables. The other variables are your vCloud Air username and domain <code>@&lt;domain&gt;</code>, a virtual data center <code>&lt;datacenter&gt;</code>, and a vCloud Air template <code>&lt;template&gt;</code>.  <code>ovftool.exe -st=&quot;OVF&quot; &quot;&lt;OVF-file-pathname&gt;&quot; &quot;vcloud://&lt;user&gt;@&lt;domain&gt;:password@&lt;virtual-cloud-location&gt;.vchs.vmware.com?vdc=&lt;datacenter&gt;&amp;org=&lt;vCloud-account-number&gt;&amp;vappTemplate=&lt;template&gt;.ovf&amp;catalog=default-catalog&quot;</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Install Panorama.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Access the vCloud Air web console and select your Virtual Private Cloud OnDemand region.</td>
</tr>
</tbody>
</table>
| 2.     | Create a Panorama virtual machine. For the steps, refer to [Add a Virtual Machine from a Template](https://www.vmware.com/support/pubs/vcloud_ondemand_virtual_machine_tutorials.html) in the vCloud Air Documentation Center. Configure the CPU, Memory and Storage as follows:  
  - Set the CPU and Memory based on how many firewalls Panorama will manage:  
    - 1-10 firewalls—4 CPUs and 4GB memory  
    - 11-50 firewalls—8 CPUs and 8GB memory  
    - 50-1,000 firewalls—8 CPUs and 16GB memory  
  - Set the Storage to at least 52GB. For better logging and reporting performance, select the SSD-Accelerated option. Panorama uses approximately 11GB for log storage. Increasing the disk size doesn’t increase the log storage capacity. To increase the log storage capacity, [Add a Virtual Disk to Panorama in vCloud Air](https://www.vmware.com/support/pubs/vcloud_ondemand_virtual_machine_tutorials.html). |
### Support for VMware Tools on the Panorama Virtual Appliance

VMware Tools is bundled with the software image (ovf) for the Panorama virtual appliance. The support for VMware Tools allows you to use the vSphere environment—vCloud Director and vCenter server—for the following:

- View the IP address assigned to the Panorama management interface.
- View resource utilization metrics on hard disk, memory, and CPU. You can use these metrics to enable alarms or actions on the vCenter server or vCloud Director.
- Graceful shutdown and restart of Panorama using the power off function on the vCenter server or vCloud Director.
- Enables a heartbeat mechanism between the vCenter server and Panorama for verifying that Panorama is functioning, or if the firewall/Panorama is rebooting. If the firewall goes into maintenance mode, heartbeats are disabled so that the vCenter server does not shut down the firewall. Disabling heartbeats allows the firewall to stay operational in maintenance mode when it cannot not send heartbeats to the vCenter server.

### Perform Initial Configuration of the Panorama Virtual Appliance

Depending on your platform, use the VMware vSphere Client or vCloud Air web console to set up network access to the Panorama virtual appliance. For unified reporting, consider using Greenwich Mean Time (GMT) or Coordinated Universal Time (UTC) as the uniform time zone across Panorama and all the managed firewalls and Log Collectors.
## Perform Initial Configuration of the Panorama Virtual Appliance

### Step 1  Gather the required information from your network administrator.
- IP address for the management (MGT) interface
- Netmask
- Default gateway
- DNS server IP address

### Step 2  Access the console of the Panorama virtual appliance.
1. Access the console.
   - On an ESXi server:
     a. Launch the VMware vSphere Client.
     b. Select the **Console** tab for the Panorama virtual appliance and press enter to access the login screen.
   - On vCloud Air:
     a. Access the vCloud Air web console and select your Virtual Private Cloud OnDemand region.
     b. Select the **Virtual Machines** tab, right-click the Panorama virtual machine, and select **Open In Console**.
2. Enter your username and password to log (default is admin for both).
3. Enter **configure** to switch to Configuration mode.

### Step 3  Configure the network access settings for the MGT interface.
Panorama uses the MGT interface for management traffic, high availability synchronization, log collection, and communication within Collector Groups.
1. Enter the following command, where `<Panorama-IP>` is the IP address you want to assign to the Panorama management interface, `<netmask>` is the subnet mask, `<gateway-IP>` is the IP address of the network gateway, and `<DNS-IP>` is the IP address of the DNS server:
   ```
   set deviceconfig system ip-address <Panorama-IP>
   netmask <netmask>
   default-gateway <gateway-IP>
   dns-setting servers primary <DNS-IP>
   ```
2. Enter **commit** to commit your changes.
3. Enter **exit** to exit Configuration mode.
4. Use the ping utility to verify network access to external services required for firewall management, such as the default gateway, DNS server, and the Palo Alto Networks Update Server, as shown in the following example:
   ```
   admin@Panorama-Corp> ping host updates.paloaltonetworks.com
   PING updates.paloaltonetworks.com (67.192.236.252) 56(84) bytes of data.
   64 bytes from 67.192.236.252: icmp_seq=1 ttl=243 time=40.5 ms
   64 bytes from 67.192.236.252: icmp_seq=1 ttl=243 time=53.6 ms
   64 bytes from 67.192.236.252: icmp_seq=1 ttl=243 time=79.5 ms
   After verifying connectivity, press Ctrl+C to stop the pings.
   ```
### Perform Initial Configuration of the Panorama Virtual Appliance (Continued)

**Step 4**  Configure the general settings.

1. Using a secure connection (HTTPS) from a web browser, log in to the Panorama web interface using the IP address and password you assigned to the management interface (https://<IP address>).
2. Select Panorama > Setup > Management and edit the General Settings.
3. Enter a Hostname for the server and enter the network Domain name. The domain name is just a label; Panorama doesn’t use it to join the domain.
4. Align the clock on Panorama and the managed firewalls to use the same Time Zone, for example GMT or UTC. Timestamps are recorded when Panorama receives the logs and the managed firewalls generate the logs. Aligning the time zones on Panorama and the firewalls ensures that the timestamps are synchronized and the process of querying logs and generating reports on Panorama is harmonious.
5. Enter the Latitude and Longitude to enable accurate placement of the Panorama management server on the world map.
6. Enter the Serial Number you received in the order fulfillment email.
7. Click OK to save your changes.

**Step 5**  Change the default administrator password.

1. Click the admin link on the left side of the web interface footer.
2. Enter the Old Password and the New Password in the appropriate fields and record the new password in a safe location.
3. Click OK.

**Step 6**  (Optional) Modify the management interface settings.

1. Select Panorama > Setup > Management and edit the Management Interface Settings.
2. Select which management services to allow on the interface (for example, Secure Shell (SSH) access) As a best practice, don’t select Telnet or HTTP. These services use plaintext and are less secure than the other services.
3. Click OK.

**Step 7**  Save your configuration changes.

Click Commit, for the Commit Type select Panorama, and click Commit again.

**Step 8**  Next steps...

If necessary, Expand Log Storage Capacity on the Panorama Virtual Appliance. Best practice is to replace the default certificate that Panorama uses to secure HTTPS traffic over the management (MGT) interface. After completing these optional tasks, you can Complete the Panorama Virtual Appliance Setup.
Expand Log Storage Capacity on the Panorama Virtual Appliance

After you Perform Initial Configuration of the Panorama Virtual Appliance, it will have one disk partition for all data in which approximately 11GB is allocated for log storage. Increasing the disk size doesn't increase the log storage capacity. If you need up to 8TB of log storage, you can add a virtual disk to Panorama installed on a VMware ESXi server or in VMware vCloud Air. If you need more than 8TB, you can mount Panorama to an NFS datastore but only on the ESXi server, not in vCloud Air. For additional log storage, you can also forward firewall logs to Dedicated Log Collectors (see Configure a Managed Collector) or Configure Log Forwarding from Panorama to External Destinations.

Panorama can use only one virtual disk for logging. Therefore, if you add a virtual disk that is dedicated for logging, Panorama stops using the default 11GB log storage on the original disk and copies any existing logs to the new disk. (Panorama continues using the original disk for data other than logs.) Expanding the log storage capacity of an existing logging disk is not supported, and Panorama does not recognize the additional storage capacity. For example if you added a 2TB logging disk, and later expand that existing logging disk to 4TB, Panorama continues to recognize the logging disk as having 2TB of storage capacity and ignores the additional 2TB of storage capacity. If you replace an existing dedicated logging disk of up to 2TB storage capacity with a disk of up to 8TB, you will lose the logs on the existing disk. To preserve the logs, your choices are:

- Configure log forwarding to external destinations before you replace the virtual disk.
- Set up a new Panorama virtual appliance for the new 8TB disk and maintain access to the Panorama containing the old disk for as long as you need the logs. To forward firewall logs to the new Panorama virtual appliance, one option is to reconfigure the firewalls to connect with the new Panorama IP address (select Device > Setup > Management and edit the Panorama Settings), add the firewalls as managed devices to the new Panorama, and Configure Log Forwarding to Panorama. To reuse the old Panorama IP address on the new Panorama, another option is to export the configuration of the old Panorama and then import and load the configuration on the new Panorama.
- Copy logs from the old disk to the new disk. Copying can take several hours, depending on how many logs the disk currently stores, and Panorama cannot collect logs during the process. Contact Palo Alto Networks Customer Support for instructions.

Before expanding log storage capacity, Determine Panorama Log Storage Requirements.

- Add a Virtual Disk to Panorama on an ESXi Server
- Add a Virtual Disk to Panorama in vCloud Air
- Mount the Panorama ESXi Server to an NFS Datastore

Add a Virtual Disk to Panorama on an ESXi Server

To expand log storage capacity beyond the approximately 11GB internal storage allocated by default on the Panorama virtual appliance, you can add another virtual disk. Panorama running on ESXi 5.5 and later versions supports a virtual disk of up to 8TB. Panorama running on earlier ESXi versions supports a virtual disk of up to 2TB.

If Panorama loses connectivity to the new virtual disk, Panorama might lose logs during the failure interval.

To allow for redundancy, use the virtual disk in a RAID configuration. RAID10 provides the best write performance for applications with high logging characteristics.

If necessary, you can Replace the Virtual Disk on an ESXi Server.
Add a Virtual Disk to Panorama on an ESXi Server

Step 1  Access the VMware vSphere Client and select Virtual Machines.

Step 2  Right-click the Panorama virtual appliance and select Power > Power Off.

Step 3  Right-click the Panorama virtual appliance and select Edit Settings.

Step 4  Click Add in the Hardware tab to launch the Add Hardware wizard.

Step 5  Select Hard Disk as the hardware type and click Next.

Step 6  Create a new virtual disk and click Next.

Step 7  Set the Disk Size to up to 8TB.

Step 8  Select the Disk Provisioning disk format and click Next.

Step 9  Select Store with the virtual machine as the Location and click Next.

Step 10  Select a SCSI Virtual Device Node (you can use the default selection) and click Next.

Step 11  Verify that the settings are correct and click Finish to exit the wizard. The new disk appears in the list of devices for the virtual appliance.

Step 12  Right-click the Panorama virtual appliance and select Power > Power On. The virtual disk initializes for first-time use. The size of the new disk determines how long initialization takes. After initialization, Panorama moves all existing logs on the internal storage to the new disk and writes all new entries to it.

Step 13  Log in to Panorama, select Panorama > Setup > Management and, in the Logging and Reporting Settings section, verify that the Log Storage capacity accurately displays the new disk capacity.

Add a Virtual Disk to Panorama in vCloud Air

To expand log storage capacity beyond the approximately 11GB internal storage allocated by default on the Panorama virtual appliance in vCloud Air, you can add another virtual disk of up to 8TB.

If Panorama loses connectivity to the new virtual disk, Panorama might lose logs during the failure interval. If necessary, you can Replace the Virtual Disk on vCloud Air.

Add a Virtual Disk to Panorama in vCloud Air

Step 1  Access the vCloud Air web console and select your Virtual Private Cloud OnDemand region.

Step 2  Select the Panorama virtual appliance in the Virtual Machines tab.

Step 3  Select Actions > Edit Resources and Add another disk.

Step 4  Set the Storage to up to 8TB and set the storage tier to Standard or SSD-Accelerated.

Step 5  Save your changes.
Add a Virtual Disk to Panorama in vCloud Air (Continued)

Step 6 Log in to Panorama, select Panorama > Setup > Management and, in the Logging and Reporting Settings section, verify that the Log Storage capacity accurately displays the new disk capacity.

Mount the Panorama ESXi Server to an NFS Datastore

When the Panorama virtual appliance runs on an ESXi server, mounting to a Network File System (NFS) datastore enables logging to a centralized location and expanding the log storage capacity beyond what a virtual disk supports. (ESXi 5.5 and later versions can support a virtual disk of up to 8TB. Earlier ESXi versions support a virtual disk of up to 2TB.) Before setting up an NFS datastore in a Panorama high availability (HA) configuration, see Logging Considerations in Panorama HA.

Mount the Panorama ESXi Server to an NFS Datastore

Step 1 Select Panorama > Setup > Operations and, in the Miscellaneous section, click Storage Partition Setup.

Step 2 Set the Storage Partition type to NFS V3.

Step 3 Enter the IP address of the NFS Server.

Step 4 Enter the Log Directory path for storing the log files. For example, export/panorama.

Step 5 For the Protocol, select TCP or UDP, and enter the Port for accessing the NFS server. To use NFS over TCP, the NFS server must support it. Common NFS ports are UDP/TCP 111 for RPC and UDP/TCP 2049 for NFS.

Step 6 For optimal NFS performance, in the Read Size and Write Size fields, specify the maximum size of the chunks of data that the client and server pass back and forth to each other. Defining a read/write size optimizes the data volume and speed in transferring data between Panorama and the NFS datastore.

Step 7 (Optional) Select Copy On Setup to copy the existing logs stored on Panorama to the NFS volume. If Panorama has a lot of logs, this option might initiate the transfer of a large volume of data.

Step 8 Click Test Logging Partition to verify that Panorama can access the NFS Server and Log Directory.

Step 9 Click OK and Commit, set the Commit Type to Panorama, and click Commit again. Until you reboot, the Panorama virtual appliance writes logs to the local storage disk.

Step 10 Select Panorama > Setup > Operations and select Reboot Panorama in the Device Operations section. After rebooting, Panorama starts writing logs to the NFS datastore.

Increase CPUs and Memory on the Panorama Virtual Appliance

When you Perform Initial Configuration of the Panorama Virtual Appliance, you specify the memory and number of CPUs based on how many firewalls Panorama will manage:

- 1–10 firewalls—4 CPUs and 4GB memory
- 11–50 firewalls—8 CPUs and 8GB memory
- 51–1,000 firewalls—8 CPUs and 16GB memory

If you increase the number of firewalls that Panorama manages, you must also increase the memory and CPUs.
Increase CPUs and Memory for Panorama on an ESXi Server

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Access the VMware vSphere Client and select Virtual Machines.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Right-click the Panorama virtual appliance and select Power &gt; Power Off.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Right-click the Panorama virtual appliance and select Edit Settings.</td>
</tr>
</tbody>
</table>
| Step 4 | Select Memory and enter the new Memory Size based on the number of firewalls that Panorama manages:  
  • 1-10 firewalls—4GB memory  
  • 11–50 firewalls—8GB memory  
  • 51–1,000 firewalls—16GB memory |
| Step 5 | Select CPUs and specify the number of CPUs (the Number of virtual sockets multiplied by the Number of cores per socket) based on the number of firewalls that Panorama manages:  
  • 1–10 firewalls—4 CPUs  
  • 11–50 firewalls—8 CPUs  
  • 51–1,000 firewalls—8 CPUs |
| Step 6 | Click OK to save your changes. |
| Step 7 | Right-click the Panorama virtual appliance and select Power > Power On. |

Increase CPUs and Memory for Panorama on vCloud Air

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Access the vCloud Air web console and select your Virtual Private Cloud OnDemand region.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Virtual Machines tab, select the Panorama virtual machine and Power Off.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Actions &gt; Edit Resources.</td>
</tr>
</tbody>
</table>
| Step 4 | Set the CPU and Memory based on the number of firewalls that Panorama manages:  
  • 1–10 firewalls—4 CPUs and 4GB memory  
  • 11–50 firewalls—8 CPUs and 8GB memory  
  • 51–1,000 firewalls—8 CPUs and 16GB memory |
| Step 5 | Save your changes. |
| Step 6 | Select the Panorama virtual machine and Power On. |
Complete the Panorama Virtual Appliance Setup

After you Perform Initial Configuration of the Panorama Virtual Appliance, continue with the following tasks for additional configuration:

- Activate a Panorama Support License
- Activate/Retrieval a Firewall Management License on the Panorama Virtual Appliance
- Install Content and Software Updates for Panorama
- Access and Navigate Panorama Management Interfaces
- Set Up Administrative Access to Panorama
- Manage Firewalls
Set Up the M-Series Appliance

The M-Series appliance is a high performance hardware appliance that you can deploy in Panorama mode or Log Collector mode. When you Perform Initial Configuration of the M-Series Appliance, you can configure the following interfaces. The M-100 and M-500 Appliance Hardware Reference Guides explain where to attach cables for these interfaces.

The M-Series appliance does not support Link Aggregation Control Protocol (LACP) for aggregating these interfaces.

The Eth1 and Eth2 interfaces are available only if the M-Series appliance runs Panorama 6.1 or a later release and the managed firewalls run PAN-OS 5.0 or a later release.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management (MGT)</td>
<td>You must use the MGT interface for management and configuration of the firewalls, Log Collectors, and Panorama. By default, Panorama also uses MGT for log collection and communication within Collector Groups, though you can reassign these functions to the Eth1 and Eth2 interfaces.</td>
</tr>
<tr>
<td>Eth1</td>
<td>You can configure the M-Series appliance to use Eth1 or Eth2 for log collection and Collector Group communication. Each interface can support either or both of these functions—for example, you can configure Eth1 for both log collection and Collector Group communication. You cannot, however, assign multiple interfaces for the same function—for example, you cannot configure both Eth1 and Eth2 for log collection. To reduce the traffic load on MGT and improve security for management traffic, use Eth1 and/or Eth2 for log collection and Collector Group communication.</td>
</tr>
<tr>
<td>Eth3</td>
<td>Reserved for future use.</td>
</tr>
</tbody>
</table>

Use the following workflows for setting up an M-Series appliance:

<table>
<thead>
<tr>
<th>M-Series Appliance in Panorama Mode</th>
<th>M-Series Appliance in Log Collector Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Rack mount the M-Series appliance. Refer to the M-100 or M-500 Appliance Hardware Reference Guide for instructions.</td>
<td><strong>Step 1</strong> Rack mount the M-Series appliance. Refer to the M-100 or M-500 Appliance Hardware Reference Guide for instructions.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Perform Initial Configuration of the M-Series Appliance</td>
<td><strong>Step 2</strong> Perform Initial Configuration of the M-Series Appliance</td>
</tr>
<tr>
<td><strong>Step 3</strong> Register Panorama and Install Licenses</td>
<td><strong>Step 3</strong> Register Panorama and Install Licenses</td>
</tr>
<tr>
<td><strong>Step 4</strong> Install Content and Software Updates for Panorama</td>
<td><strong>Step 4</strong> Install Content and Software Updates for Panorama</td>
</tr>
<tr>
<td><strong>Step 5</strong> Configure each array. This task is required to make the RAID disks available for logging. Optionally, you can add disks to Increase Storage on the M-Series Appliance.</td>
<td><strong>Step 5</strong> Configure each array. This task is required to make the RAID disks available for logging. Optionally, you can add disks to Increase Storage on the M-Series Appliance.</td>
</tr>
<tr>
<td><strong>Step 6</strong> Set Up Administrative Access to Panorama</td>
<td><strong>Step 6</strong> Set up the M-Series Appliance as a Log Collector</td>
</tr>
<tr>
<td><strong>Step 7</strong> Manage Firewalls</td>
<td><strong>Step 7</strong> Manage Log Collection</td>
</tr>
<tr>
<td><strong>Step 8</strong> Manage Log Collection</td>
<td></td>
</tr>
</tbody>
</table>
Perform Initial Configuration of the M-Series Appliance

By default, Panorama has an IP address of 192.168.1.1 and a username/password of admin/admin. For security reasons, you must change these settings before continuing with other configuration tasks. You must perform these initial configuration tasks either from the Management (MGT) interface or using a direct serial port connection to the console port on the M-100 or M-500 appliance.

### Perform Initial Configuration of the M-100 or M-500 Appliance

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Gather the required interface and server information from your network administrator.</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>Gather the IP address, netmask (for IPv4) or prefix length (for IPv6), and default gateway for each interface that you plan to configure (MGT, Eth1, and/or Eth2). Only the MGT interface is mandatory.</td>
</tr>
<tr>
<td>🔄</td>
<td>If you plan to use the appliance as a Panorama management server, Palo Alto Networks recommends that you configure the Eth1 and/or Eth2 interfaces for log collection and Collector Group communication (see Set Up the M-Series Appliance). You can improve the security of management traffic by defining a separate subnet for the MGT interface that is more private than the Eth1 and Eth2 subnets.</td>
</tr>
<tr>
<td>🔄</td>
<td>Gather the IP addresses of the DNS servers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Access the M-Series appliance from your computer.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Connect to the M-Series appliance in one of the following ways:</td>
</tr>
<tr>
<td></td>
<td>• Attach a serial cable from a computer to the Console port on the M-Series appliance and connect using terminal emulation software (9600-8-N-1).</td>
</tr>
<tr>
<td></td>
<td>• Attach an RJ-45 Ethernet cable from a computer to the MGT port on the M-Series appliance. From a browser, go to <a href="https://192.168.1.1">https://192.168.1.1</a>. Enabling access to this URL might require changing the IP address on the computer to an address in the 192.168.1.0 network (for example, 192.168.1.2).</td>
</tr>
<tr>
<td>2.</td>
<td>When prompted, log in to the appliance using the default username and password (admin/admin). The appliance starts initializing.</td>
</tr>
</tbody>
</table>
### Perform Initial Configuration of the M-100 or M-500 Appliance (Continued)

**Step 3** Configure the network access settings for each interface that Panorama will use for configuration, log collection, and Collector Group communication.

1. Select **Panorama > Setup > Management**.
2. Edit the Interface Settings of each interface that Panorama will use. Only the MGT interface is required. The Eth1 and Eth2 interfaces are optional and apply only if you plan to use the M-Series appliance as a Panorama management server.
   a. Complete one or both of the following field sets based on the IP protocols of your network:
      - IPv4—**IP Address**, **Netmask**, and **Default Gateway**
      - IPv6—**IPv6 Address/Prefix Length** and **Default IPv6 Gateway**
   b. (Optional) Select the check boxes for the management services to allow on the interface. **Ping** is the only option for Eth1 and Eth2. As a best practice, clear the **Telnet** and **HTTP** check boxes for the MGT interface; these services use plaintext and so are less secure than others.
   c. Click **OK** to save your changes.

**Step 4** Configure the hostname, time zone, and general settings.

1. Select **Panorama > Setup > Management** and edit the General Settings.
2. Align the clock on Panorama and the managed firewalls to use the same **Time Zone**, for example GMT or UTC. The firewall records timestamps when it generate logs and Panorama records timestamps upon receiving the logs. Aligning the time zones ensures that the timestamps are synchronized and that the process of querying logs and generating reports on Panorama is harmonious.
3. Enter a **Hostname** for the server. Panorama uses this as the display name/label for the appliance. For example, this is the name that appears at the CLI prompt. It also appears in the Collector Name field if you add the appliance as a managed collector on the **Panorama > Managed Collectors** page.
4. (Optional) Enter the **Latitude** and **Longitude** to enable accurate placement of the M-Series appliance on the world map. The **App Scope > Traffic Maps** and **App Scope > Threat Maps** use these values.
5. Click **OK** to save your entries.

**Step 5** Configure the DNS servers and Palo Alto Networks Update Server.

1. Select **Panorama > Setup > Services** and edit the settings.
2. Enter the IP address of the **Primary DNS Server** and (optionally) of the **Secondary DNS Server**.
3. Enter the **URL or static address** of the **Update Server** (default updates.paloaltonetworks.com).
   - Select **Verify Update Server Identity** if you want Panorama to verify that the Update Server from which it downloads software or content packages has an SSL certificate that a trusted authority signed. This option adds an additional level of security for communication between the Panorama management server and Update Server.
4. Click **OK** to save your entries.
<table>
<thead>
<tr>
<th>Perform Initial Configuration of the M-100 or M-500 Appliance (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong> Change the default admin password.</td>
</tr>
<tr>
<td>1. Click the admin link in the lower left of the web interface.</td>
</tr>
<tr>
<td>2. Enter the Old Password, New Password, and Confirm New Password, and then click OK. Store the new password in a safe location.</td>
</tr>
<tr>
<td>To ensure that the MGT interface remains secure, configure Minimum Password Complexity settings (select Panorama &gt; Setup &gt; Management) and specify the interval at which administrators must change their passwords.</td>
</tr>
<tr>
<td>Click OK and Commit, set the Commit Type to Panorama, and click Commit again.</td>
</tr>
<tr>
<td>If you plan to use the M-Series appliance as a Panorama management server and you configured the Eth1 or Eth2 interfaces, you must assign them to the Device Log Collection or Collector Group Communication functions when you Configure a Managed Collector. To make the interfaces operational, you must then Configure a Collector Group for the managed collector and perform a Collector Group commit.</td>
</tr>
</tbody>
</table>
Set Up the M-Series Appliance

Set up the M-Series Appliance as a Log Collector

If you want a dedicated appliance for log collection, configure an M-100 or M-500 appliance in Log Collector mode. To do this, you first perform the initial configuration of the appliance in Panorama mode, which includes licensing, installing software and content updates, and configuring the management (MGT) interface. You then switch the M-100 or M-500 appliance to Log Collector mode and complete the Log

Perform Initial Configuration of the M-100 or M-500 Appliance (Continued)

Step 8  Verify network access to external services required for Panorama management, such as the Palo Alto Networks Update Server.

1. Connect to the M-Series appliance in one of the following ways:
   - Attach a serial cable from your computer to the Console port on the M-Series appliance. Then use terminal emulation software (9600-8-N-1) to connect.
   - Use terminal emulation software such as PuTTY to open an SSH session to the IP address that you specified for the MGT interface of the M-Series appliance during initial configuration.
2. Log in to the CLI when prompted. Use the default admin account and the password that you specified during initial configuration.
3. Use the ping utility to verify network connectivity to the Palo Alto Networks Update Server as shown in the following example. Verify that DNS resolution occurs and the response includes the IP address for the Update Server (10.101.16.13, in this example); the Update Server does not respond to a ping request.
   > ping host updates.paloaltonetworks.com
   PING updates.paloaltonetworks.com (10.101.16.13) 56(84) bytes of data.
   After verifying DNS resolution, press Ctrl+C to stop the ping request.
4. Use the following CLI command to retrieve information on the support entitlement for Panorama from the Update Server:
   > request support check
   If you have connectivity, the Update Server responds with the support status for Panorama. Because Panorama is not registered, the Update Server returns the following message:
   Contact Us
   https://www.paloaltonetworks.com/company/contact-us.html
   Support Home
   https://www.paloaltonetworks.com/support/tabs/overview.html
   Device not found on this update server

Step 9  Next steps...

1. Register Panorama and Install Licenses.
2. Install Content and Software Updates for Panorama.
   As a best practice, replace the default certificate that Panorama uses to secure HTTPS traffic over the MGT interface.
Collector configuration. Additionally, if you want to use dedicated interfaces (recommended) instead of the MGT interface for log collection and Collector Group communication, you must first configure the interfaces for the Panorama management server, then configure them for the Log Collector, and then perform a Panorama commit followed by a Collector Group commit.

Perform the following steps to set up a new M-Series appliance as a Log Collector or to convert an existing M-Series appliance that was previously deployed as a Panorama management server.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Set up the Panorama management server that will manage the Log Collector if you have not already done so.</th>
<th>Perform one of the following tasks:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Set Up the Panorama Virtual Appliance</td>
</tr>
</tbody>
</table>

| Step 2 | Record the management IP addresses of the Panorama management server. If you deployed Panorama in a high availability (HA) configuration, you need the IP address of each HA peer. | 1. Log in to the web interface of the Panorama management server. |
|        |                                                                                                                                  | 2. Record the IP Address of the solitary (non-HA) or active (HA) Panorama by selecting Panorama > Setup > Management and checking the Management Interface Settings. |
|        |                                                                                                                                  | 3. For an HA deployment, record the Peer HA IP Address of the passive Panorama by selecting Panorama > High Availability and checking the Setup section. |

| Step 3 | Set up the M-Series appliance that will serve as a Dedicated Log Collector. If you previously deployed this appliance as a Panorama management server, you can skip this step because the MGT interface is already configured and the licenses and updates are already installed. | The M-Series appliance in Log Collector mode does not have a web interface for configuration tasks, only a CLI. Therefore, before changing the mode on the M-Series appliance, use the web interface in Panorama mode to: |
|        |                                                                                                                                  | 1. Perform Initial Configuration of the M-Series Appliance. |
|        |                                                                                                                                  | 2. Register Panorama and Install Licenses. |
|        |                                                                                                                                  | 3. Install Content and Software Updates for Panorama. |

| Step 4 | Access the CLI of the M-Series appliance. | 1. Connect to the M-Series appliance in one of the following ways: |
|        |                                                                                                                                  | • Attach a serial cable from your computer to the Console port on the M-Series appliance. Then use terminal emulation software (9600-8-N-1) to connect. |
|        |                                                                                                                                  | • Use terminal emulation software such as PuTTY to open an SSH session to the IP address that you specified for the MGT interface of the M-Series appliance during initial configuration. |
|        |                                                                                                                                  | 2. Log in to the CLI when prompted. Use the default admin account and the password that you specified during initial configuration. |
### Set up the M-100 or M-500 Appliance as a Log Collector (Continued)

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Switch from Panorama mode to Log Collector mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Switch to Log Collector mode by entering the following command:</td>
</tr>
<tr>
<td></td>
<td><code>&gt; request system system-mode logger</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter <code>Y</code> to confirm the mode change. The M-Series appliance reboots. If the reboot process terminates your terminal emulation software session, reconnect to the M-Series appliance to see the Panorama login prompt.</td>
</tr>
<tr>
<td></td>
<td><img src="https://example.com" alt="CMS Login" /> If you see a CMS Login prompt, this means the Log Collector has not finished rebooting. Press Enter at the prompt without typing a username or password.</td>
</tr>
<tr>
<td>3.</td>
<td>Log back in to the CLI.</td>
</tr>
<tr>
<td>4.</td>
<td>Verify that the switch to Log Collector mode succeeded:</td>
</tr>
<tr>
<td></td>
<td>`&gt; show system info</td>
</tr>
<tr>
<td></td>
<td>If the mode change succeeded, the output displays:</td>
</tr>
<tr>
<td></td>
<td><code>system-mode: logger</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Configure the logging disks as RAID1 pairs.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If you previously deployed the appliance as a Panorama management server, you can skip this step because the disk pairs are already configured and available.</td>
</tr>
<tr>
<td></td>
<td><img src="https://example.com" alt="Note" /> The time required to configure the drives varies from several minutes to a couple of hours, based on the amount of data on the drives.</td>
</tr>
<tr>
<td>1.</td>
<td>Determine which disk pairs are present for configuring as RAID pairs on the M-Series appliance:</td>
</tr>
<tr>
<td></td>
<td><code>&gt; show system raid detail</code></td>
</tr>
<tr>
<td></td>
<td>Perform the remaining steps to configure each disk pair that has present disks. This example uses disk pair A1/A2.</td>
</tr>
<tr>
<td>2.</td>
<td>To add the first disk in the pair, enter the following command and enter <code>y</code> when prompted to confirm the request:</td>
</tr>
<tr>
<td></td>
<td><code>&gt; request system raid add A1</code></td>
</tr>
<tr>
<td></td>
<td>Wait for the process to finish before adding the next disk in the pair. To monitor the progress of the RAID configuration, re-enter:</td>
</tr>
<tr>
<td></td>
<td><code>&gt; show system raid detail</code></td>
</tr>
<tr>
<td></td>
<td>After the process finishes for the first disk, the output displays the disk pair status as <strong>Available</strong> but <strong>degraded</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>Add the second disk in the pair:</td>
</tr>
<tr>
<td></td>
<td><code>&gt; request system raid add A2</code></td>
</tr>
<tr>
<td>4.</td>
<td>Verify that the disk setup is complete:</td>
</tr>
<tr>
<td></td>
<td><code>&gt; show system raid detail</code></td>
</tr>
<tr>
<td></td>
<td>After the process finishes for the second disk, the output displays the disk pair status as <strong>Available and clean</strong>.</td>
</tr>
<tr>
<td></td>
<td><code>Disk Pair A</code></td>
</tr>
<tr>
<td></td>
<td><code>Status</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Record the serial number of the Log Collector.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>You need the serial number to add the Log Collector as a managed collector on the Panorama management server.</td>
</tr>
<tr>
<td>1.</td>
<td>At the Log Collector CLI, enter the following command to display its serial number.</td>
</tr>
<tr>
<td></td>
<td>`&gt; show system info</td>
</tr>
<tr>
<td>2.</td>
<td>Record the serial number.</td>
</tr>
</tbody>
</table>
### Set up the M-100 or M-500 Appliance as a Log Collector (Continued)

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Add the Log Collector as a managed collector to the Panorama management server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Select <strong>Panorama &gt; Managed Collectors</strong> and <strong>Add</strong> a managed collector.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>General</strong> tab, enter the serial number (<strong>Collector S/N</strong>) you recorded for the Log Collector.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Panorama Server IP</strong> field, enter the IP address or FQDN of the solitary (non-HA) or active (HA) Panorama. For HA deployments, enter the IP address or FQDN of the passive Panorama peer in the <strong>Panorama Server IP 2</strong> field.</td>
</tr>
<tr>
<td></td>
<td>4. Select <strong>Management</strong> and configure one or both of the following field sets for the MGT interface based on the IP protocols of your network.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IPv4</strong>—<strong>IP Address</strong>, <strong>Netmask</strong>, and <strong>Default Gateway</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>IPv6</strong>—<strong>IPv6 Address/Prefix Length</strong> and <strong>Default IPv6 Gateway</strong></td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>OK</strong> and <strong>Commit</strong>, set the <strong>Commit Type</strong> to <strong>Panorama</strong>, and <strong>Commit</strong> again. This step is required before you can enable logging disks.</td>
</tr>
<tr>
<td></td>
<td>6. Verify that the <strong>Panorama &gt; Managed Collectors</strong> page lists the Log Collector you added. The Connected column displays a check mark to indicate that the Log Collector is connected to Panorama. You might have to wait a few minutes before the page displays the updated connection status.</td>
</tr>
<tr>
<td></td>
<td>At this point, the Configuration Status column displays Out of Sync and the Run Time Status column displays disconnected. The status will change to In Sync and connected after you configure a Collector Group (Step 12).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Enable connectivity between the Log Collector and Panorama management server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enter the following commands at the Log Collector CLI, where <strong>&lt;IPaddress1&gt;</strong> is for the MGT interface of the solitary (non-HA) or active (HA) Panorama and <strong>&lt;IPaddress2&gt;</strong> is for the MGT interface of the passive (HA) Panorama, if applicable.</td>
</tr>
<tr>
<td></td>
<td><code>&gt; configure</code></td>
</tr>
<tr>
<td></td>
<td><code># set deviceconfig system panorama-server</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;IPaddress1&gt; panorama-server-2 </code>&lt;IPaddress2&gt;``</td>
</tr>
<tr>
<td></td>
<td><code># commit</code></td>
</tr>
<tr>
<td></td>
<td><code># exit</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Enable the logging disks.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Select <strong>Panorama &gt; Managed Collectors</strong> and edit the Log Collector.</td>
</tr>
<tr>
<td></td>
<td>2. Select <strong>Disks</strong> and <strong>Add</strong> each RAID disk pair.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>OK</strong> and <strong>Commit</strong>, set the <strong>Commit Type</strong> to <strong>Panorama</strong>, and <strong>Commit</strong> again.</td>
</tr>
</tbody>
</table>
Set up the M-100 or M-500 Appliance as a Log Collector (Continued)

Step 11 (Optional) Configure the Eth1 and/or Eth2 interfaces if the Panorama management server and Log Collector will use them for log collection and Collector Group communication.

If you previously deployed the Log Collector as a Panorama management server and configured the Eth1 and/or Eth2 interfaces, you must reconfigure those interfaces because switching to Log Collector mode (Step 5) would have deleted all configurations except the management access settings.

Palo Alto Networks recommends using Eth1 and/or Eth2 to reduce the traffic load on the MGT interface and to improve security for management traffic.

1. Configure Eth1 and/or Eth2 on the Panorama management server if you haven’t already:
   a. Select Panorama > Setup > Management.
   b. Edit the Eth1 Interface Settings and/or Eth2 Interface Settings. For each interface, complete one or both of the following field sets based on the IP protocols of your network:
      - IPv4—IP Address, Netmask, and Default Gateway
      - IPv6—I Pv6 Address/Prefix Length and Default IPv6 Gateway
   c. Click OK to save your changes.

2. Configure Eth1 and/or Eth2 on the Log Collector:
   a. Select Panorama > Managed Collectors and edit the Log Collector.
   b. Configure the network settings of the Eth1 and/or Eth2 interfaces. For each interface, select the corresponding tab and configure one or both of the following field sets based on the IP protocols of your network:
      - IPv4—IP Address, Netmask, and Default Gateway
      - IPv6—I Pv6 Address/Prefix Length and Default IPv6 Gateway
   c. Click OK and Commit, set the Commit Type to Panorama, and click Commit again. This step is required before you can assign the Eth1 and Eth2 interfaces to logging functions.
   d. Select the interfaces (MGT, Eth1, or Eth2) that the Log Collector will use for Device Log Collection and Collector Group Communication (default is MGT).
   e. Click OK to save your changes.
## Set up the M-100 or M-500 Appliance as a Log Collector (Continued)

<table>
<thead>
<tr>
<th>Step 12</th>
<th>Assign the Log Collector to a Collector Group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Configure a Collector Group.</strong> You must perform a Panorama commit and then a Collector Group commit to synchronize the Log Collector configuration with Panorama and to put the Eth1 and Eth2 interfaces (if you configured them) in an operational state on the Log Collector.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>All the Log Collectors for any particular Collector Group must be the same model: such as all M-100 appliances or all M-500 appliances. If you <strong>Enable log redundancy across collectors</strong> in the Collector Group, then each Log Collector also requires the same number of disks.</td>
<td></td>
</tr>
<tr>
<td>2. <strong>Select Panorama &gt; Managed Collectors</strong> to verify that the Log Collector configuration is synchronized with Panorama.</td>
<td></td>
</tr>
<tr>
<td>The Configuration Status column should display In Sync and the Run Time Status column should display connected.</td>
<td></td>
</tr>
<tr>
<td>3. Access the Log Collector CLI and enter the following command to verify that its interfaces are operational:</td>
<td></td>
</tr>
<tr>
<td>&gt; show interface all</td>
<td></td>
</tr>
<tr>
<td>The output displays the state as up for each interface that is operational.</td>
<td></td>
</tr>
<tr>
<td>4. If the Collector Group has multiple Log Collectors, verify they can communicate with each other by running the following command for each interface that the Log Collectors use (MGT, Eth1, and/or Eth2). For the <strong>source</strong> IP address, specify the interface of the Log Collector on which you run the command. For the <strong>host</strong> IP address, specify the matching interface of another Log Collector in the same Collector Group.</td>
<td></td>
</tr>
<tr>
<td>&gt; ping source &lt;IP-address&gt; host &lt;IP-address&gt;</td>
<td></td>
</tr>
<tr>
<td>For example, if a Collector Group contains Log Collector A with an MGT interface set to 192.0.2.1 and Log Collector B with an MGT interface set to 192.0.2.2, log in to Log Collector A and enter:</td>
<td></td>
</tr>
<tr>
<td>&gt; ping source 192.0.2.1 host 192.0.2.2</td>
<td></td>
</tr>
<tr>
<td>If the Log Collectors can communicate over their MGT interfaces, the output displays:</td>
<td></td>
</tr>
<tr>
<td>PING 192.0.2.2 (192.0.2.2) from 192.0.2.1:</td>
<td></td>
</tr>
<tr>
<td>56(84) bytes of data.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 13</th>
<th>Next steps...</th>
</tr>
</thead>
<tbody>
<tr>
<td>To enable the Log Collector to receive firewall logs:</td>
<td></td>
</tr>
<tr>
<td>1. <strong>Configure Log Forwarding to Panorama.</strong></td>
<td></td>
</tr>
<tr>
<td>2. <strong>Verify Log Forwarding to Panorama.</strong></td>
<td></td>
</tr>
</tbody>
</table>
Increase Storage on the M-Series Appliance

The M-100 appliance has eight drive bays and each drive pair (A1/A2 and B1/B2 for example) is in a separate RAID 1 array. By default, the M-100 appliance ships with 1TB drives installed in two bays (A1 and A2) or you can choose to order the M-100 appliance with 1TB drives installed in all eight drive bays (A1 through D2). The M-500 appliance has 24 drive bays but only the first 16 (A1 through H2) are configurable. By default, the M-500 appliance ships with four 2TB disk drives installed in drive bays A1 through B2. Each pair (A1/A2, B1/B2, C1/C2, and D1/D2) is configured in separate RAID 1 arrays.

After you Perform Initial Configuration of the M-Series Appliance, you can increase log storage capacity of the appliance by upgrading any existing 1TB drives (to 2TB drives) or by installing additional 1TB or 2TB drives in empty and configurable drive bays. For example, on an M-500 appliance, you can choose to upgrade the existing 1TB drives to 2TB drives or you can add 2TB drives to the empty drive bays (E1 through H2).

For information on replacing failed drives, refer to the M-100 or M-500 Hardware Reference Guide.

The following table shows the maximum log storage capacity for each appliance based on the number of drives installed and the size of each drive.

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Number of Drives</th>
<th>Log Storage Capacity Using 1TB Drives</th>
<th>Log Storage Capacity Using 2TB Drives</th>
<th>Log Storage Capacity Using 1TB and 2TB Drives</th>
</tr>
</thead>
<tbody>
<tr>
<td>M-100 Appliance</td>
<td></td>
<td>Minimum - 1TB</td>
<td>Minimum - 2TB</td>
<td>Minimum - 3TB</td>
</tr>
<tr>
<td></td>
<td>Minimum - 2</td>
<td>Maximum - 4TB</td>
<td>Maximum - 8TB</td>
<td>Maximum - 7TB</td>
</tr>
<tr>
<td>M-500 Appliance</td>
<td>Minimum - 8</td>
<td>Maximum - 12TB</td>
<td>Maximum - 24TB</td>
<td>Minimum - 3TB</td>
</tr>
<tr>
<td></td>
<td>Maximum - 24</td>
<td></td>
<td></td>
<td>Maximum - 23TB</td>
</tr>
</tbody>
</table>

Before expanding log storage capacity, Determine Panorama Log Storage Requirements.

If you need more log storage than a single M-Series appliance supports, you can add Dedicated Log Collectors (see Configure a Managed Collector) or you can Configure Log Forwarding from Panorama to External Destinations.

You don't need to take the M-Series appliance offline to expand the storage when adding drives to an M-Series appliance that is already deployed. When the additional drives are configurable and available, the M-Series appliance redistributes the logs among all available drives. This log redistribution process happens in the background and does not impact uptime or the availability of the M-Series appliance. However, the process does diminish the maximum logging rate. The Redistribution State column (Panorama > Collector Groups) indicates the completion status of the process as a percentage.

▲ Add Additional Drives to an M-Series Appliance
▲ Upgrade Existing Drives on a M-Series Appliance
Add Additional Drives to an M-Series Appliance

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Install the new drives in the appropriate drive bays.</th>
<th>Make sure to add the drives sequentially in the next open drive bays. For example, add drives to B1 and B2 before adding drives to C1 and C2.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Access the command line interface (CLI) on the M-Series appliance.</td>
<td>Connect to the M-Series appliance in one of two ways: • Connect a serial cable from your computer to the Console port and connect to the M-Series appliance using terminal emulation software (9600-8-N-1). • Use terminal emulation software (such as PuTTY) to open a Secure Shell (SSH) session to the IP address of the M-Series appliance.</td>
</tr>
<tr>
<td>Step 3</td>
<td>When prompted, log in to the appliance.</td>
<td>Use the default administrator account and the assigned password.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure each array.</td>
<td>The time required to mirror the data on the drive may vary from several minutes to a few hours, depending on the amount of data on the drive.</td>
</tr>
</tbody>
</table>

The following example uses the drives in bays B1 and B2.

1. Enter the following commands and confirm the request when prompted:
   - `request system raid add B1`
   - `request system raid add B2`

2. To monitor the progress of the RAID configuration, enter the following command:
   - `show system raid detail`

When the RAID set up is complete, the following response displays:

```plaintext
Disk Pair A Available
  Status clean
  Disk id A1 Present
    model : ST91000640NS
    size : 953869 MB
    status : active sync
  Disk id A2 Present
    model : ST91000640NS
    size : 953869 MB
    status : active sync
Disk Pair B Available
  Status clean
  Disk id B1 Present
    model : ST91000640NS
    size : 953869 MB
    status : active sync
  Disk id B2 Present
    model : ST91000640NS
    size : 953869 MB
    status : active sync
```
**Upgrade Drives on M-Series Appliances Running Panorama 7.0.8 or a Later Release**

- **Step 1** Access the command line interface (CLI) on the M-Series appliance.
  - Connect to the M-Series appliance in one of two ways:
    - Connect a serial cable from your computer to the Console port and connect to the M-Series appliance using terminal emulation software (9600-8-N-1).
    - Use terminal emulation software (such as PuTTY) to open a Secure Shell (SSH) session to the IP address of the M-Series appliance.

- **Step 2** When prompted, log in to the appliance.
  - Use the default administrator account and the assigned password.
Step 3 Verify that the RAID 1 status for the installed drives shows there are at least two functioning RAID 1 arrays. During the upgrade, you will upgrade one RAID 1 array at a time and there must be at least one other RAID 1 array that is available to the appliance. The appliance will show an abort error if you try to remove the only functioning array from the configuration.

Enter the following command to view RAID status:

```bash
show system raid detail
```

For example, the following shows an output from an M-500 appliance with two available arrays (Disk Pair A and Disk Pair B). If there is only one available array, you must add a second array as described in Add Additional Drives to an M-Series Appliance before you upgrade the drives.

```
Disk Pair A                                          Available
  Status                         clean
  Disk id A1
    model        : ST91000640NS
    size         : 953869 MB
    status       : active sync
  Disk id A2
    model        : ST91000640NS
    size         : 953869 MB
    status       : active sync
Disk Pair B                                          Available
  Status                         clean
  Disk id B1
    model        : ST91000640NS
    size         : 953869 MB
    status       : active sync
  Disk id B2
    model        : ST91000640NS
    size         : 953869 MB
    status       : active sync
```
### Step 4: Remove the first 1TB drive and replace it with a 2TB drive.

1. To remove the first drive from the RAID 1 array configuration (A1 in this example), enter the following command and enter `y` when prompted to confirm the request:
   ```
   > request system raid remove A1
   ```
2. Physically remove the first drive from the drive bay. Press the ejector button on the drive carrier in drive bay A1 to release the ejector handle. Then pull the handle toward you and slide the drive out of the appliance.
3. Remove a 2TB drive from its packaging and place the drive on a table next to the drive you just removed. Take note of how the drive is installed in the carrier because you will install the 2TB drive in this same carrier.
4. Remove the four screws holding the 1TB drive in the carrier and remove the drive from the carrier.
5. Attach the 2TB drive to the carrier using the same four screws you removed from the 1TB drive and then reinsert the carrier with the 2TB drive into drive bay A1.
6. Enter the following command to verify the 2TB drive is recognized:
   ```
   > show system raid detail
   ```
Verify that the A1 disk shows the correct model and size (about 2TB). If the model and size are not correct, run the above command again until the correct model and size are shown.

If the wrong model and size are consistently shown, enter the following command:
```
> request system raid remove A1
```
Wait for 30 seconds once you run the above command, then remove the disk and reinsert it, and repeat the `show system raid detail` command to verify the size and model.

### Step 5: Copy the data from the remaining installed 1TB drive in the RAID 1 array to the newly installed 2TB drive in that array.

1. To copy the data from the 1TB drive in drive bay A2 to the newly installed 2TB drive in drive bay A1, enter the following command and enter `y` when prompted:
   ```
   > request system raid copy from A2 to A1
   ```
2. To view the status of the copy process, run the following command:
   ```
   > show system raid detail
   ```
Continue running this command to view the RAID detail output until you see that the array (A1/A2 in this example) shows `Available`.

At this point, drive A2 will show `not in use` because there is a drive size mismatch.
Step 6 Upgrade the second drive in the RAID 1 array to a 2TB drive.

1. Remove the second 1TB drive (from drive bay A2 in the current example) for the RAID 1 array configuration:  
   ```
   > request system raid remove A2
   ```

2. Insert the carrier with the newly installed 2TB drive into drive bay A2 and add it to the RAID 1 array configuration:  
   ```
   > request system raid add A2
   ```
   The system will copy the data from A2 to A1 to mirror the drives.

3. To view the status of the copy process, run the following command:  
   ```
   > show system raid detail
   ```
   Continue to view the RAID detail output until you see that the array (A1/A2 in this example) shows `Available` and both disks show `active sync`.

   ```
   Disk Pair A Available
   Status clean
   Disk id A1 Present
   model : ST2000NX0253
   size : 1907138 MB
   status : active sync
   Disk id A2 Present
   model : ST2000NX0253
   size : 1907138 MB
   status : active sync
   ```

Step 7 Upgrade drives for additional RAID 1 arrays as needed.

To upgrade additional RAID 1 arrays to 2TB drives, repeat this procedure replacing the drive designators as applicable. For example, replace A1 with B1 and A2 with B2 to upgrade the drives in the B1/B2 RAID 1 array.

---

Upgrade Drives on M-Series Appliances Running Panorama 7.0.8 or a Later Release

The logs on the 1TB drives will not be available after upgrading drives on an M-Series appliance that is running Panorama 7.0.7 or an earlier release. Even if this is acceptable, we recommend that you perform this upgrade during a maintenance window.

If it is important to you to retain logs, you must upgrade to Panorama 7.0.8 or a later release and then use the Upgrade Drives on M-Series Appliances Running Panorama 7.0.8 or a Later Release procedure.

---

Upgrade Drives on M-Series Appliances Running Panorama 7.0.7 or an Earlier Release

Step 1 Access the command line interface (CLI) on the M-Series appliance.

Connect to the M-Series appliance in one of two ways:
- Connect a serial cable from your computer to the Console port and connect to the M-Series appliance using terminal emulation software (9600-8-N-1).
- Use terminal emulation software (such as PuTTY) to open a Secure Shell (SSH) session to the IP address of the M-Series appliance.

Step 2 When prompted, log in to the appliance.

Use the default administrator account and the assigned password.
### Upgrade Drives on M-Series Appliances Running Panorama 7.0.7 or an Earlier Release (Continued)

#### Step 3
Verify that the RAID 1 status for the installed drives shows there are at least two functioning RAID 1 arrays. During the upgrade, you will upgrade one RAID 1 array at a time and there must be at least one other RAID 1 array that is available to the appliance. The appliance will show an abort error if you try to remove the only functioning array from the configuration.

<table>
<thead>
<tr>
<th>Disk Pair A</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
<td>clean</td>
</tr>
<tr>
<td><strong>Disk id A1</strong></td>
<td>Present</td>
</tr>
<tr>
<td>model: ST91000640NS</td>
<td></td>
</tr>
<tr>
<td>size: 953869 MB</td>
<td></td>
</tr>
<tr>
<td>status: active sync</td>
<td></td>
</tr>
</tbody>
</table>

| Disk id A2             | Present            |
| model: ST91000640NS    |                    |
| size: 953869 MB        |                    |
| status: active sync    |                    |

<table>
<thead>
<tr>
<th>Disk Pair B</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
<td>clean</td>
</tr>
<tr>
<td><strong>Disk id B1</strong></td>
<td>Present</td>
</tr>
<tr>
<td>model: ST91000640NS</td>
<td></td>
</tr>
<tr>
<td>size: 953869 MB</td>
<td></td>
</tr>
<tr>
<td>status: active sync</td>
<td></td>
</tr>
</tbody>
</table>

| Disk id B2             | Present            |
| model: ST91000640NS    |                    |
| size: 953869 MB        |                    |
| status: active sync    |                    |

#### Step 4
Remove the first two 1TB drives from the first RAID 1 array configuration and then physically remove the drives.

1. To remove the drives from the RAID 1 array configuration (A1 and A2 in this example), enter the following commands and enter y when prompted to confirm each request:
   ```shell
   > request system raid remove A1
   > request system raid remove A2
   ```

2. Physically remove the drives from the drive bays. Press the ejector button on each drive carrier to release the ejector handle. Then pull the handle toward you and slide the drives out of the appliance.

3. Remove two 2TB drives from their packaging and place them on a table next to the drives you just removed. Take note of how the drives are installed in the carrier because you will install the 2TB drives in these same carriers.

4. Remove the four screws holding each drive in its carrier and remove the drives from the carriers.

5. Attach the 2TB drives to the carriers using the same screws you just removed and then insert the carriers with the newly installed 2TB drives into the drive bays (A1 and A2 in this example).
Step 5  Create a new RAID 1 array for the newly installed 2TB drives and ensure that both drives are in the new array.

1. To create a new array that includes the drive in drive bay A1, enter the following command:
   > request system raid add A1

2. To view and confirm the status of the new RAID 1 array configuration, enter the following command:
   > show system raid detail

   The following output shows that the Disk Pair A array is Available.

   At this point, drive A2 will show not in use.

   Disk Pair A       Available
   Status           clean, degraded
   Disk id A1       Present
       model       : ST9100640NS
       size         : 953869 MB
       status       : active sync
   Disk id A2       Present
       model       : ST9100640NS
       size         : 953869 MB
       status       : not in use

3. Add the second disk to the new array. In this example, add A2:
   > request system raid add A2

4. Continue running the show system raid detail command to view the RAID output until the disk pair status shows clean and both disks show active sync.

Step 6  Upgrade drives for additional RAID 1 arrays as needed.

To upgrade additional RAID 1 arrays to 2TB drives, repeat this procedure replacing the drive designators as applicable. For example, replace A1 with B1 and A2 with B2 to upgrade the drives in the B1/B2 RAID 1 array.
Register Panorama and Install Licenses

Before you can begin using Panorama for centralized management, logging, and reporting, you must register, activate, and retrieve the Panorama licenses. Every instance of Panorama requires valid licenses that entitle you to manage firewalls and obtain support. The firewall management license enforces the maximum number of firewalls that Panorama can manage. This license is based on firewall serial numbers, not on the number of virtual systems on each firewall. The support license enables Panorama software updates and dynamic content updates (for the latest Applications and Threats signatures, as an example). To purchase licenses, contact your Palo Alto Networks Systems Engineer or reseller.

If you are running an evaluation license for firewall management on your Panorama virtual appliance and want to apply a Panorama license that you purchased, perform the tasks Register Panorama and Activate/Retrieve a Firewall Management License on the Panorama Virtual Appliance.

- Register Panorama
- Activate a Panorama Support License
- Activate/Retrieve a Firewall Management License on the Panorama Virtual Appliance
- Activate/Retrieve a Firewall Management License on the M-Series Appliance

Register Panorama

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Record the Panorama serial number or auth code and record your Sales Order Number or Customer ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For the auth code, Sales Order Number, or Customer ID, see the order fulfillment email that Palo Alto Networks Customer Service sent when you placed your order for Panorama. For the serial number, the location depends on the appliance type:</td>
</tr>
<tr>
<td></td>
<td>• M-Series appliance—Log in to the Panorama web interface and record the Serial # value in the Dashboard tab, General Information section.</td>
</tr>
<tr>
<td></td>
<td>• Panorama virtual appliance—See the order fulfillment email.</td>
</tr>
</tbody>
</table>
Register Panorama (Continued)

**Step 2** Register Panorama. The steps depend on whether you already have a login for the Support site.

- If this is the first Palo Alto Networks appliance you are registering and you don’t yet have a login:
  1. Go to the Palo Alto Networks Customer Support web site.
  2. Click **Register** at the bottom of the page (Overview > Get Help > Register), enter your **Email Address**, enter the code displayed on the page, and click **Submit**.
  3. Complete the fields in the **Create Contact Details** section.
  4. Enter a **Display Name**, **Confirm Email Address**, and **Password/Confirm Password**.
  5. Enter the Panorama **Device Serial Number** or **Auth Code**.
  6. Enter your **Sales Order Number** or **Customer ID**.
  7. Click **Submit**.
- If you already have a support account:
  1. Log in to the Palo Alto Networks Customer Support web site.
  2. Select **Assets > Devices**, and click **Register New Device**.
  3. Select **Register Device using Serial Number or Authorization Code**.
  4. Enter the device **Serial Number**, **City**, **Postal Code**, and **Country**.
  5. Click **Agree Submit**.

If the support license expires, Panorama can still manage firewalls and collect logs, but software and content updates will be unavailable. The software and content versions on Panorama must be the same as or later than the versions on the managed firewalls, or else errors will occur. For details, see Panorama, Log Collector, and Firewall Version Compatibility.

Activate a Panorama Support License

Before activating a Panorama support license on a Panorama M-Series appliance or Panorama virtual appliance, you must **Register Panorama**.

![Warning](image)

If the support license expires, Panorama can still manage firewalls and collect logs, but software and content updates will be unavailable. The software and content versions on Panorama must be the same as or later than the versions on the managed firewalls, or else errors will occur. For details, see Panorama, Log Collector, and Firewall Version Compatibility.

**Activate a Panorama Support License**

**Step 1** Select **Panorama > Support** and click **Activate feature using authorization code**.

**Step 2** Enter the **Authorization Code** and click **OK**.

**Step 3** Verify that the subscription is activated by checking the details (for example, the **Expiry Date**, support **Level**, and **Description**) in the Support section of the page.
Activate/Retrieve a Firewall Management License on the Panorama Virtual Appliance

Before activating and retrieving a firewall management license on the Panorama virtual appliance, you must [Register Panorama](#). If you are running an evaluation license and want to apply a license that you purchased, you must still register and activate/retrieve the purchased license.

**Activate/Retrieve a Firewall Management License on the Panorama Virtual Appliance**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select Panorama &gt; Setup &gt; Management and edit the General Settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter the Panorama <strong>Serial Number</strong> (included in the order fulfillment email) and click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select Panorama, and click <strong>Commit</strong> again.</td>
</tr>
</tbody>
</table>

To determine how many firewalls a license enables a Panorama virtual appliance to manage, log in to the [Palo Alto Networks Customer Support web site](#). Then select the **Assets** tab, find the Panorama entry, and view the Model Name. For example, a license for the PAN-PRA-25 model can manage 25 firewalls. This page also displays the Expiration Date and other license information.

Activate/Retrieve a Firewall Management License on the M-Series Appliance

Before activating and retrieving a Panorama firewall management license on the M-Series appliance:

- **Register Panorama**.
- Locate the auth codes for the product/subscription you purchased. When you placed your order, Palo Alto Networks Customer Service sent you an email that listed the auth code associated with the purchase. If you cannot locate this email, contact [Palo Alto Networks Customer Support](#) to obtain your codes before proceeding.

After you activate and retrieve the license, the Panorama > Licenses page displays the associated issuance date, expiration date, and the number of firewalls that the license enables Panorama to manage.

To activate and retrieve the license, the options are:

<table>
<thead>
<tr>
<th>Activate/Retrieve a Firewall Management License on the M-Series Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use the web interface to activate and retrieve the license.</strong></td>
</tr>
<tr>
<td>Select this option if Panorama is ready to connect to the Palo Alto Networks update server (you completed the task Perform Initial Configuration of the M-Series Appliance) but you have not activated the license on the <a href="#">Palo Alto Networks Customer Support web site</a>.</td>
</tr>
</tbody>
</table>
Activate/Retrieve a Firewall Management License on the M-Series Appliance (Continued)

- Retrieve the license key from the license server.
  If Panorama is not ready to connect to the update server (for example, you have not completed the initial M-Series appliance setup), you can activate the license on the Support website so that, when Panorama is ready to connect, you can then use the web interface to retrieve the activated license. The process of retrieving an activated license is faster than the process of both retrieving and activating.

1. Activate the license on the Palo Alto Networks Customer Support web site.
   a. On a host with internet access, use a web browser to access the Palo Alto Networks Customer Support web site and log in.
   b. Select Assets > Devices, find your M-Series appliance and, in the Action column, click the edit icon (📝).
   c. Select Activate Auth-Code, enter the Authorization Code and click Agree and Submit to activate the license.

2. Configure Panorama to connect to the update server: see Perform Initial Configuration of the M-Series Appliance.

3. Select Panorama > Licenses and click Retrieve license keys from the license server. Panorama retrieves the activated license.

- Manually upload the license from a host to Panorama. Panorama must have access to that host.
  If Panorama is set up (you completed the task Perform Initial Configuration of the M-Series Appliance) but does not have a connection to the update server, activate the license on the Support website, download it to a host that has a connection to the update server, then upload it to Panorama.

1. Activate and download the license from the Palo Alto Networks Customer Support web site.
   a. On a host with internet access, use a web browser to access the Palo Alto Networks Customer Support web site and log in.
   b. Select Assets > Devices, find your M-Series appliance and, in the Action column, click the edit icon (📝).
   c. Select Activate Auth-Code, enter the Authorization Code and click Agree and Submit to activate the license.
   d. In the Action column, click the download icon and save the license key file to the host.

2. In the Panorama web interface, select Panorama > Licenses, click Manually upload license key and click Browse.

3. Select the key file you downloaded to the host and click Open.

4. Click OK to upload the activated license key.
Install Content and Software Updates for Panorama

A valid support subscription enables access to the Panorama software image and release notes. To take advantage of the latest fixes and security enhancements, it is a good idea to upgrade to the latest software update or to the update version that your reseller or a Palo Alto Networks Systems Engineer recommends. The procedure to install software and content updates depends on whether Panorama has a direct connection to the internet and whether it has a high availability (HA) configuration.

- Panorama, Log Collector, and Firewall Version Compatibility
- Install Updates for Panorama in an HA Configuration
- Install Updates for Panorama with an Internet Connection
- Install Updates for Panorama without an Internet Connection

Panorama, Log Collector, and Firewall Version Compatibility

Palo Alto Networks highly recommends running the same Panorama release on both the Panorama management server and the Dedicated Log Collectors. Panorama can manage firewalls that are running the same or an earlier PAN-OS release with the caveat that Panorama 6.1 and later versions cannot push configurations to firewalls running PAN-OS 6.0.0 through 6.0.3.

Additionally, you should ensure that the content release version on the Panorama management server is the same (or earlier) version than the content release version on any Dedicated Log Collectors or managed firewalls.

Regardless whether your subscriptions include the Applications database or Applications and Threats database, Panorama installs only the Applications database. Panorama and Dedicated Log Collectors do not enforce policy rules so they do not require the threat signatures in the Threats database. The Applications database contains threat metadata (such as threat IDs and names) that you use on Panorama and Dedicated Log Collectors when defining policy rules to push to managed firewalls and when interpreting threat information in logs and reports. However, firewalls do require the full Applications and Threats database to match the identifiers recorded in logs with the corresponding threat, URL, or application names. Refer to the Release Notes for the minimum content release version required for a Panorama release.
Install Updates for Panorama in an HA Configuration

To ensure a seamless failover when you update the Panorama software in a high availability (HA) configuration, the active and passive Panorama peers must be running the same Panorama release with the same Applications database version. The following example describes how to upgrade an HA pair (active peer is Primary_A and passive peer is Secondary_B).

### Install Updates for Panorama in an HA Configuration

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Task Details</th>
</tr>
</thead>
</table>
| **Step 1** | Upgrade the Panorama software on the Secondary_B (passive) peer. | Perform one of the following tasks on the Secondary_B peer:  
• Install Updates for Panorama with an Internet Connection  
• Install Updates for Panorama without an Internet Connection  
After the upgrade, this Panorama peer transitions to a non-functional state because the peers are no longer running the same software release. |
| **Step 2** | Suspend the Primary_A peer to force a failover. | On the Primary_A peer:  
1. In the Operational Commands section (Panorama > High Availability), Suspend local Panorama.  
2. Verify that state is suspended (displayed on bottom-right corner of the web interface).  
The resulting failover should cause the Secondary_B peer to transition to active state. |
| **Step 3** | Upgrade the Panorama software on the Primary_A (currently passive) peer. | Perform one of the following tasks on the Primary_A peer:  
• Install Updates for Panorama with an Internet Connection  
• Install Updates for Panorama without an Internet Connection  
After you reboot, the Primary_A peer first transitions to the passive state. Then, if preemption is enabled (default), the Primary_A peer automatically transitions to the active state and the Secondary_B peer reverts to the passive state.  
If you disabled preemption, manually Restore the Primary Panorama to the Active State. |
| **Step 4** | Verify that both peers are now running any newly installed content release versions and the newly installed Panorama release. | On the Dashboard of each Panorama peer, check the Panorama Software Version and Application Version and confirm that they are the same on both peers and that the running configuration is synchronized. |
Install Updates for Panorama with an Internet Connection

If Panorama has a direct connection to the internet, perform the following steps to install Panorama software updates. If Panorama is deployed in a high availability (HA) configuration, you must upgrade the Panorama software on each peer as described when you Install Updates for Panorama in an HA Configuration.

As a best practice, before you upgrade software on an M-Series appliance, ensure that Panorama has a local Log Collector (<Panorama > Managed Collectors>) that is assigned to a Collector Group (<Panorama > Collector Groups>). For details, see Configure a Managed Collector.

## Install Updates for Panorama with an Internet Connection

### Step 1
Verify that the updates you plan to install are appropriate for your Panorama deployment.

- Refer to the Release Notes for the minimum content release version required for a Panorama software release. If you intend to upgrade Log Collectors and firewalls to a particular release, you must first upgrade Panorama to that (or a later) release.
- For a Panorama virtual appliance that runs on an ESXi server, ensure that the server meets the requirements (see Setup Prerequisites for the Panorama Virtual Appliance).

### Step 2
Save a backup of the current Panorama configuration file that you can use to restore the configuration if you have problems with the upgrade.

Although Panorama automatically creates a backup configuration, best practice is to create and externally store a backup before you upgrade.

1. Save named Panorama configuration snapshot (<Panorama > Setup > Operations), enter a Name for the configuration, and click OK.
2. Export named Panorama configuration snapshot, select the Name of the configuration you just saved, click OK, and save the exported file to a location that is external to Panorama.

### Step 3
(As needed) Install content updates.

If Panorama is not running the minimum content versions required for the Panorama release to which you intend to upgrade, you must update content versions to the minimum (or later) versions before you install the software updates.

Refer to the Release Notes for the minimum content release version you must install for a Panorama release.

Palo Alto Networks highly recommends that Panorama, Log Collectors, and all managed firewalls run the same content release version. Additionally, we recommend that you schedule automatic, recurring updates so that you are always running the latest content versions (Step 7).

1. Check Now (<Panorama > Dynamic Updates) for the latest updates. If the value in the Action column is Download, an update is available.
   - Ensure that Panorama is running the same but not a later content release version than is running on managed firewalls and Log Collectors.
2. (As needed) Before you update the content release version on Panorama, be sure to upgrade managed firewalls and then Log Collectors (see Deploy an Update to Log Collectors when Panorama is Internet-connected) to the same (or a later) content release version.
   - If you do not need to install content updates at this time, then skip ahead to Step 4.
3. Install content updates in the following sequence. When an installation completes, the Currently Installed column displays a check mark.
   a. Download and Install the Applications or Applications and Threats update. Regardless of your subscription, Panorama installs and needs only the Applications content update, not the Threats content. For details, see Panorama, Log Collector, and Firewall Version Compatibility.
   b. Download and Install any other updates (Antivirus, WildFire, or URL Filtering) as needed, one at a time, and in any sequence.
**Step 4** Determine the software upgrade path. You cannot skip installation of any major release versions in the path to your target release. For example, if you intend to upgrade from Panorama 6.0.13 to Panorama 7.1.3, you must:
- Download and install Panorama 6.1.0 and reboot.
- Download and install Panorama 7.0.1 and reboot (7.0.1 is the base image for the 7.0 release; not 7.0.0).
- Download Panorama 7.1.0. Optionally, install this base image and reboot before you install the target maintenance release.
- Download and install Panorama 7.1.3 and reboot.

Check which version has a check mark in the Currently Installed column (Panorama > Software) and proceed as follows:
- If a Panorama 7.0 release is currently installed, skip ahead to Step 6 to upgrade to a Panorama 7.1 release.
- If a release earlier than Panorama 7.0 is installed, proceed to Step 5 and follow the upgrade path to Panorama 7.0.1 before you upgrade to a Panorama 7.1 release.

We highly recommend that you review the known issues and changes to default behavior in the Release Notes and upgrade/downgrade considerations in the New Features Guide for each release through which you pass as part of your upgrade path.

---

**Step 5** Use the upgrade path identified in Step 4 to upgrade to a Panorama 7.0 release.

Repeat the following procedure until the appliance is running a Panorama 7.0 release—do not skip installation of any major release version in the path to your target Panorama 7.1 release.

1. **Check Now (Panorama > Software)** for the latest updates. If an update is available, the Action column displays **Download**.
2. For each release in your upgrade path, **Download** the model-specific file for the release version to which you are upgrading. For example, to upgrade an M-Series appliance to Panorama 7.0.1, download the `Panorama_m-7.0.1` image; to upgrade a Panorama virtual appliance to Panorama 7.0.1, download the `Panorama_pc-7.0.1` image.

After a successful download, the Action column changes from **Download** to **Install** for the downloaded image.

By default, you can download a maximum of two software or content updates of each type on a Panorama appliance and if you download a third update of the same type, Panorama will delete the update for the earliest version of that type. If you need to upload more than two software updates or content updates of a single type, use the `set max-num-images count <number>` CLI command to increase the maximum.

3. **Install** the software update.
   - If prompted to reboot, click **Yes**. If you see a CMS Login prompt, press Enter without typing a username or password. When the Panorama login prompt appears, enter the username and password you specified during initial configuration.
   - If you are not prompted to reboot, **Reboot Panorama** from the Device Operations section (Panorama > Setup > Operations).
4. Repeat these steps for each release in your upgrade path.
### Install Updates for Panorama with an Internet Connection (Continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td><strong>Install Panorama 7.1.</strong></td>
</tr>
</tbody>
</table>

1. **Check Now (Panorama > Software)** for the latest updates. If an update is available, the Action column displays **Download**.
   - If you are upgrading to a Panorama 7.1 maintenance release (a release other than the Panorama 7.1.0 base image), first download the Panorama 7.1.0 release.

2. Locate and **Download** the model-specific file for the release version to which you are upgrading. For example, to upgrade an M-Series appliance to Panorama 7.1.0, download the Panorama_m-7.1.0 image; to upgrade a Panorama virtual appliance to Panorama 7.1.0, download Panorama_pc-7.1.0. After a successful download, the Action column changes from **Download** to **Install** for the downloaded image.

3. **(Required for the target release; optional for the base-image—PAN-OS 7.1.0 release—if upgrading to a maintenance release)** Install the downloaded image and then reboot.
   - **a. Install the image.**
     - As a best practice, when upgrading to a Panorama 7.1 maintenance release (Panorama 7.1.1 or later release), install the Panorama 7.1.0 base image and reboot the appliance before you download and install the maintenance release.
   - **b. After the installation completes successfully, reboot using one of the following methods:**
     - If prompted to reboot, click **Yes**. If you see a CMS Login prompt, press Enter without typing a username or password. When the Panorama login prompt appears, enter the username and password you specified during initial configuration.
     - If you are not prompted to reboot, **Reboot Panorama** from the Device Operations section (Panorama > Setup > Operations).

4. **(Required only if upgrading to a PAN-OS 7.1 maintenance release)** After completing the above steps for the PAN-OS 7.1.0 base image, repeat steps 1 through 3 to upgrade to the target maintenance release.
### Install Updates for Panorama with an Internet Connection (Continued)

<table>
<thead>
<tr>
<th>Step 7</th>
<th>(Best Practice) Schedule recurring, automatic content updates. Panorama does not synchronize content update schedules across HA peers. You must perform this task on both the active and passive Panorama.</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the header row for each update type (<a href="#">Panorama &gt; Dynamic Updates</a>), the Schedule is initially set to None. Perform the remaining steps for each update type.</td>
<td></td>
</tr>
<tr>
<td>1. Click None and select the update frequency (<a href="#">Recurrence</a>). The frequency options depend on the update type.</td>
<td></td>
</tr>
<tr>
<td>2. Select the schedule action:</td>
<td></td>
</tr>
<tr>
<td>• Download And Install (Best Practice)—Panorama automatically installs updates after downloading them.</td>
<td></td>
</tr>
<tr>
<td>• Download Only—You must manually install updates after Panorama downloads them.</td>
<td></td>
</tr>
<tr>
<td>3. Based on the <a href="#">best practices for the security posture</a> of your organization, configure a delay (<a href="#">Threshold</a>) after an update becomes available before Panorama downloads the update.</td>
<td></td>
</tr>
<tr>
<td>4. Click OK to save your changes.</td>
<td></td>
</tr>
<tr>
<td>5. Select Commit &gt; Commit to Panorama and Commit your changes.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>(Only if upgrading from a release earlier than Panorama 5.1 to a Panorama 5.1 or later release running on an ESXi server) Configure the Panorama virtual appliance settings on the VMware ESXi server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>After Panorama reboots, complete the following tasks:</td>
<td></td>
</tr>
<tr>
<td>1. Access the VMware vSphere Client and select go to the Virtual Machines tab.</td>
<td></td>
</tr>
<tr>
<td>2. Right-click the Panorama virtual appliance and select Power &gt; Power Off.</td>
<td></td>
</tr>
<tr>
<td>3. Right-click the Panorama virtual appliance again and Edit Settings as follows:</td>
<td></td>
</tr>
<tr>
<td>a. Select the Hardware tab and allocate Memory based on how many firewalls Panorama manages:</td>
<td></td>
</tr>
<tr>
<td>- 1–10 managed firewalls: 4GB</td>
<td></td>
</tr>
<tr>
<td>- 11–50 managed firewalls: 8GB</td>
<td></td>
</tr>
<tr>
<td>- 51–1,000 managed firewalls: 16GB</td>
<td></td>
</tr>
<tr>
<td>b. Set the <a href="#">SCSI Controller</a> to <a href="#">LSI Logic Parallel</a>.</td>
<td></td>
</tr>
<tr>
<td>c. Go to the Options tab, select <a href="#">General Options</a>, set the <a href="#">Guest Operating System</a> to <a href="#">Linux</a>, and set the <a href="#">Version</a> to Other Linux (64-bit).</td>
<td></td>
</tr>
<tr>
<td>d. Click OK.</td>
<td></td>
</tr>
<tr>
<td>4. Right-click the Panorama virtual appliance and select Power &gt; Power On.</td>
<td></td>
</tr>
</tbody>
</table>
Install Updates for Panorama without an Internet Connection

If Panorama does not have a direct connection to the internet, perform the following steps to install content and software updates. If Panorama is deployed in a high availability (HA) configuration, you must upgrade each peer as described when you Install Updates for Panorama in an HA Configuration.

As a best practice, before you upgrade software on an M-Series appliance, ensure that Panorama has a local Log Collector (Panorama > Managed Collectors) that is assigned to a Collector Group (Panorama > Collector Groups). For details, see Configure a Managed Collector.

### Step 1: Verify that the updates you plan to install are appropriate for your Panorama deployment.

- Refer to the Release Notes for the minimum content release version you must install for a Panorama software release. If you intend to upgrade Log Collectors and firewalls to a particular release, you must first upgrade Panorama to that (or a later) release.
- For a Panorama virtual appliance that runs on an ESXi server, ensure that the server meets the requirements (see Setup Prerequisites for the Panorama Virtual Appliance).

### Step 2: Save a backup of the current Panorama configuration file that you can use to restore the configuration if you have problems with the upgrade.

1. **Save named Panorama configuration snapshot (Panorama > Setup > Operations), enter a Name for the configuration, and click OK.**
2. **Export named Panorama configuration snapshot**, select the Name of the configuration you just saved, click OK, and save the exported file to a location that is external to Panorama.

### Step 3: Determine which content updates you need to install.

1. **For each content update, determine whether you need updates and which content updates you need to download in Step 4.**
   - Ensure that Panorama is running the same but not a later content release version than is running on managed firewalls and Log Collectors.
2. **(As needed) To ensure that you can update Panorama to the latest content updates, first upgrade managed firewalls to the latest updates.**
## Install Updates for Panorama without an Internet Connection (Continued)

### Step 4  
**As needed**
Download content updates to a host that can connect and upload content to Panorama either over SCP or HTTPS.

If you do not need to install content updates at this time, skip ahead to Step 6.

1. Use a host that has internet access to log in to the Palo Alto Networks Customer Support website.
2. Download content updates as needed:
   - If Panorama is not running the minimum content versions required for the Panorama release to which you intend to upgrade, refer to the Release Notes for the minimum content release version you must install before you update the Panorama software.
   - Palo Alto Networks highly recommends that Panorama, Log Collectors, and all managed firewalls run the same content release version.
     - Click Updates > Dynamic Updates in the Resources section.
     - Download the appropriate content updates and save the files to the host. Perform this step for each content type you need to update.

### Step 5  
Install content updates as needed.

You must install content updates before software updates and you must install the content updates on firewalls first and then install the content updates on Log Collectors before you install them on the Panorama management server.

Install the Applications or Applications and Threats update first, and then install any other updates (Antivirus, WildFire, and URL Filtering) as needed, one at a time, and in any sequence.

Regardless whether your subscription includes both Applications and Threats content, Panorama installs and needs only the Applications content. For details, see Panorama, Log Collector, and Firewall Version Compatibility.

In Panorama (Panorama > Dynamic Updates), perform the following steps for each content type:

1. Click Upload, select content Type, Browse to the location on the host to which you downloaded the update, select the update, and click OK.
2. Click Install From File, select the Package Type, and click OK.

### Step 6  
Determine the software upgrade path.

You cannot skip installation of any major release versions in the path to your target release. For example, if you intend to upgrade from Panorama 6.0.13 to Panorama 7.1.3, you must:

- Upload and install Panorama 6.1.0 and reboot.
- Upload and install Panorama 7.0.1 and reboot (7.0.1 is the base image for the 7.0 release; not 7.0.0).
- Upload Panorama 7.1.0.
- Optionally, install this base image and reboot before you install the target maintenance release.
- Upload and install Panorama 7.1.3 and reboot.

Check which version has a check mark in the Currently Installed column (Panorama > Software) and make a list of all versions in your upgrade path that you need to download from the Palo Alto Networks update server so that you can upload each to the appliance as needed when you upgrade.

We highly recommend that you review the known issues and changes to default behavior in the Release Notes and upgrade/downgrade considerations in the New Features Guide for each release through which you pass as part of your upgrade path.
## Install Updates for Panorama without an Internet Connection (Continued)

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Download software updates to a host that can connect and upload content to Panorama either over SCP or HTTPS.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Use a host with internet access to log in to the <a href="https://panDocument">Palo Alto Networks Customer Support website</a></td>
</tr>
<tr>
<td>2.</td>
<td>Download software updates:</td>
</tr>
<tr>
<td>a.</td>
<td>On the main page of Palo Alto Networks Customer Support website, click <strong>Updates &gt; Software Updates</strong> (Resources section).</td>
</tr>
<tr>
<td>b.</td>
<td>For the first (or next) Panorama release in your upgrade path, identify the model-specific file. For example, to upgrade an M-Series appliance to Panorama 7.0.1, download the Panorama_m-7.0.1 image; to upgrade a Panorama virtual appliance to Panorama 7.0.1, download the Panorama_pc-7.0.1 image. You can quickly locate Panorama images by selecting <strong>Panorama M Images</strong> (M-Series appliances) or <strong>Panorama Updates</strong> (virtual appliances) from the Filter By drop-down.</td>
</tr>
<tr>
<td>c.</td>
<td>Click the filename and save the file to the host.</td>
</tr>
<tr>
<td>d.</td>
<td>Repeat steps b and c for any additional release versions in your upgrade path as determined in Step 6.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Install the software updates. For each release in your upgrade path (starting with the earliest), perform the following steps:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Click <strong>Upload (Panorama &gt; Software)</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td><strong>Browse</strong> to the location on the host to which you downloaded the update, select the update, <strong>Sync To Peer</strong> if Panorama is in an HA configuration (to push the software image to the secondary peer), and click <strong>OK</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>(Required for each base image release in the upgrade path except the base-image—PAN-OS 7.1.0 release—if upgrading to a PAN-OS 7.1 maintenance release) Install the software image and reboot. For an HA configuration, <strong>Install Updates for Panorama in an HA Configuration</strong>; otherwise:</td>
</tr>
<tr>
<td>a.</td>
<td>Install the downloaded image.</td>
</tr>
<tr>
<td>b.</td>
<td>As a best practice, when upgrading to a Panorama 7.1 maintenance release (Panorama 7.1.1 or a later Panorama 7.1 release), install the Panorama 7.1.0 base image and reboot the appliance before you upload and install the maintenance release.</td>
</tr>
<tr>
<td>b.</td>
<td>After the installation completes successfully, reboot using one of the following methods:</td>
</tr>
<tr>
<td>-</td>
<td>If prompted to reboot, click <strong>Yes</strong>. If you see a CMS Login prompt, press Enter without typing a username or password. When the Panorama login prompt appears, enter the username and password you specified during initial configuration.</td>
</tr>
<tr>
<td>-</td>
<td>If you are not prompted to reboot, <strong>Reboot Panorama</strong> from the Device Operations section (Panorama &gt; Setup &gt; Operations).</td>
</tr>
<tr>
<td>4.</td>
<td>Repeat steps 1 through 3 for each release in your path.</td>
</tr>
</tbody>
</table>
### Install Updates for Panorama without an Internet Connection (Continued)

**Step 9** (Only if upgrading from a release earlier than Panorama 5.1 to a Panorama 5.1 or later release running on an ESXi server)

Configure the Panorama virtual appliance settings on the VMware ESXi server.

After Panorama reboots, complete the following tasks:

1. Access the VMware vSphere Client and go to the **Virtual Machines** tab.
2. Right-click the Panorama virtual appliance and select **Power > Power Off**.
3. Right-click the Panorama virtual appliance and **Edit Settings**:
   a. Select the **Hardware** tab and allocate **Memory** based on how many firewalls Panorama manages:
      - 1 to 10 managed firewalls: 4GB
      - 11 to 50 managed firewalls: 8GB
      - 51 to 1,000 managed firewalls: 16GB
   b. Set the **SCSI Controller** to **LSI Logic Parallel**.
   c. Go to the **Options** tab, select **General Options**, set the **Guest Operating System** to **Linux**, and set the **Version** to **Other Linux (64-bit)**.
   d. Click **OK**.
4. Right-click the Panorama virtual appliance and select **Power > Power On**.
Transition to a Different Panorama Platform

When your network requirements change (for example, the logging rate increases), you can migrate the Panorama management server and Dedicated Log Collectors to Panorama Platforms that better support those requirements.

- Migrate from a Panorama Virtual Appliance to an M-Series Appliance
- Migrate from an M-Series Appliance to a Panorama Virtual Appliance
- Migrate from an M-100 Appliance to an M-500 Appliance

Migrate from a Panorama Virtual Appliance to an M-Series Appliance

You can migrate the Panorama configuration from a Panorama virtual appliance to an M-Series appliance in Panorama mode. However, you cannot migrate the logs because the log format on the Panorama virtual appliance is incompatible with that on M-Series appliances. Therefore, if you want to maintain access to the old logs stored on the Panorama virtual appliance, you must continue running the Panorama virtual appliance after the migration. The M-Series appliance will collect the new logs that firewalls forward after the migration. After the pre-migration logs expire or become irrelevant due to aging, you can shut down the Panorama virtual appliance.

If you store firewall logs on Dedicated Log Collectors (M-Series appliances in Log Collector mode) instead of on the Panorama virtual appliance, you can maintain access to the logs by migrating the Dedicated Log Collectors to the new M-Series appliance in Panorama mode.

Migrate from a Panorama Virtual Appliance to an M-Series Appliance

**Step 1** Plan the migration.

- Upgrade the software on the Panorama virtual appliance before the migration if the M-Series appliance requires a later release of the current software (the M-500 appliance requires Panorama 7.0 or a later release). For important details about software versions, see [Panorama, Log Collector, and Firewall Version Compatibility](#).
- Schedule a maintenance window for the migration. Although firewalls can buffer logs after the Panorama virtual appliance goes offline and then forward the logs after the M-Series appliance comes online, completing the migration during a maintenance window minimizes the risk that logs will exceed the buffer capacities and be lost during the transition between Panorama appliances.
- Consider whether to maintain access to the Panorama virtual appliance after the migration to access existing logs. The most efficient approach is to assign a new IP address to the Panorama virtual appliance and reuse its old IP address for the M-Series appliance. This ensures that the Panorama virtual appliance remains accessible and that firewalls can point to the M-Series appliance without you reconfiguring the Panorama IP address on each firewall.
Set Up Panorama

Transition to a Different Panorama Platform

| Step 2 | Migrate your subscriptions to the new appliance. | 1. Purchase the new support license and migration license.  
2. Provide your sales representative the serial number of the Panorama virtual appliance you will phase out, the auth code you received when you purchased the new M-Series appliance, and the effective date for the migration. On the effective date, Palo Alto Networks will automatically apply the auth code to the serial number of the M-Series appliance, phase out support for the Panorama virtual appliance, and trigger support for the M-Series appliance. Consult your sales representative regarding how much time is available to complete the migration after the effective date. At the end of that period, Palo Alto Networks terminates the support entitlement on the Panorama virtual appliance, after which it can no longer receive software or content updates. |
|——— | ——— | ——— |
| Step 3 | Export the Panorama configuration from the Panorama virtual appliance. | 1. Log in to the Panorama virtual appliance and select Panorama > Setup > Operations.  
2. Click Save named Panorama configuration snapshot, enter a Name to identify the configuration, and click OK.  
3. Click Export named Panorama configuration snapshot, select the Name of the configuration you just saved, and click OK. Panorama exports the configuration to your client system as an XML file. |
|——— | ——— | ——— |
| Step 4 | Power off the Panorama virtual appliance if you won’t need to access to it after the migration or assign a new IP address to its management (MGT) interface if you will need access to it. | To power off the Panorama virtual appliance, see the documentation for your VMware product.  
To change the IP address on the Panorama virtual appliance:  
1. Select Panorama > Setup > Management, and edit the Management Interface Settings.  
2. Enter the new IP Address and click OK.  
3. Click Commit, for the Commit Type select Panorama, and click Commit again. |
|——— | ——— | ——— |
| Step 5 | Perform the initial setup of the M-Series appliance. | 1. Rack mount the M-Series appliance. Refer to the M-100 or M-500 Appliance Hardware Reference Guide for instructions.  
2. Perform Initial Configuration of the M-Series Appliance to define the network connections required to activate licenses and install updates.  
3. Register Panorama.  
4. Activate a Panorama Support License.  
5. Activate/Retrieve a Firewall Management License on the M-Series Appliance. Use the auth code associated with the migration license.  
6. Install Content and Software Updates for Panorama. Install the same versions as those on the Panorama virtual appliance. |
### Migrate from an M-Series Appliance to a Panorama Virtual Appliance

You can migrate the Panorama configuration from an M-100 or M-500 appliance to a Panorama virtual appliance in Panorama mode. However, you cannot migrate the logs because the log format on the M-Series appliances is incompatible with that on the Panorama virtual appliances. Therefore, if you want to maintain

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Load the Panorama configuration snapshot that you exported from the Panorama virtual appliance into the M-Series appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>On the M-Series appliance, select <strong>Panorama &gt; Setup &gt; Operations</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Import named Panorama configuration snapshot</strong>. Browse to the Panorama configuration file you exported from the Panorama virtual appliance, and click <strong>OK</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>Click <strong>Load named Panorama configuration snapshot</strong>, select the <strong>Name</strong> of the configuration you just imported, select a <strong>Decryption Key</strong> (the master key for Panorama), and click <strong>OK</strong>. Panorama overwrites its current candidate configuration with the loaded configuration. Panorama displays any errors that occur when loading the configuration file.</td>
</tr>
<tr>
<td>4.</td>
<td>If errors occurred, save them to a local file. Resolve each error to ensure the migrated configuration is valid.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Modify the configuration on the M-Series appliance. Required if the M-Series appliance will use different values than the Panorama virtual appliance. If you will maintain access to the Panorama virtual appliance to access its logs, use a different hostname and IP address for the M-Series appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select <strong>Panorama &gt; Setup &gt; Management</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Edit the General Settings, modify the <strong>Hostname</strong>, and click <strong>OK</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>Edit the Management Interface Settings, modify the values as necessary, and click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Add the default managed collector and Collector Group back to the M-Series appliance. Loading the configuration from the Panorama virtual appliance (Step 6) removes the default managed collector and Collector Group that are predefined on each M-Series appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Configure a Managed Collector that is local to the M-Series appliance.</td>
</tr>
<tr>
<td>2.</td>
<td>Configure a Collector Group for the default managed collector.</td>
</tr>
<tr>
<td>3.</td>
<td>Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Panorama</strong>, and click <strong>Commit</strong> again.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Synchronize the M-Series appliance with the firewalls to resume firewall management. Complete this step during a maintenance window to minimize network disruption.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>On the M-Series appliance, select <strong>Panorama &gt; Managed Devices</strong> and verify that the Device State column displays <strong>Connected</strong> for the firewalls. At this point, the Shared Policy (device groups) and Template columns display <strong>Out of sync</strong> for the firewalls.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Device Group</strong>, select every device group, select the <strong>Include Device and Network Templates</strong> check box, and click <strong>Commit</strong> again.</td>
</tr>
<tr>
<td>3.</td>
<td>In the <strong>Panorama &gt; Managed Devices</strong> page, verify that the Shared Policy and Template columns display <strong>In sync</strong> for the firewalls.</td>
</tr>
</tbody>
</table>
access to the old logs stored on the M-Series appliance, you must continue running the M-Series appliance as a Dedicated Log Collector after the migration and add it to the Panorama virtual appliance as a managed collector. The M-Series appliance will continue to collect the new logs that firewalls forward after the migration.

| Migrate from an M-Series Appliance to a Panorama Virtual Appliance |
|---|---|
| **Step 1** Plan the migration. | - Determine the required software version of the Panorama virtual appliance. Upgrade the software on the M-Series appliance before the migration if the Panorama virtual appliance requires a more recent Panorama release (the M-500 appliance requires Panorama 7.0 or a later release). For important details about software versions, see Panorama, Log Collector, and Firewall Version Compatibility.
- Schedule a maintenance window for the migration. Although firewalls can buffer logs after the M-Series appliance goes offline and then forward the logs after the Panorama virtual appliance comes online, completing the migration during a maintenance window minimizes the risk that logs will exceed the buffer capacities and be lost during the transition between Panorama models. |
| **Step 2** Purchase the licenses for the new Panorama virtual appliance. | 1. Get the auth-code for the Panorama virtual appliance and the support license.
2. Provide your sales representative the serial number of the M-Series appliance you will phase out, the auth-code you received when you purchased the new Panorama virtual appliance, and the effective date for the migration. On the effective date, Palo Alto Networks will automatically apply the existing auth-code to the serial number of the Panorama virtual appliance, apply the new management license to the M-Series appliance, and trigger support for the M-Series appliance. Consult your sales representative regarding how much time is available to complete the migration after the effective date. |
| **Step 3** Export the configuration from the M-Series appliance. | 1. Log in to the M-Series appliance and select Panorama > Setup > Operations.
2. Click Save named Panorama configuration snapshot, enter a Name to identify the configuration, and click OK.
3. Click Export named Panorama configuration snapshot, select the Name of the configuration you just saved, and click OK. Panorama exports the configuration to your client system as an XML file. Save the configuration to a location external to the Panorama appliance. |
### Migrate from an M-Series Appliance to a Panorama Virtual Appliance (Continued)

#### Step 4
Power off the M-Series appliance if you won’t need to access to it after the migration or assign a new IP address to its management (MGT) interface if you will need access to it.

- **To power off the M-Series appliance:**
  1. Log in to the Panorama web interface.
  2. Select **Panorama > Setup > Operations** and under Device Operations, **Shutdown Panorama**. Click **Yes** to confirm the shutdown.

- **To change the IP address on the M-Series appliance:**
  1. Log in to the Panorama web interface.
  2. Select **Panorama > Setup > Management**, and edit the Management Interface Settings.
  3. Enter the new **IP Address** and click **OK**.
  4. Select **Commit > Commit to Panorama** and commit your changes.

#### Step 5
Perform the initial setup of the Panorama virtual appliance.

To manage your firewalls and resume log forwarding, you will need to assign the MGT interface of the Panorama virtual appliance the same IP address as the original MGT interface of the M-Series appliance during the initial configuration of the Panorama virtual appliance.

1. **Set Up the Panorama Virtual Appliance.**
2. **Perform Initial Configuration of the Panorama Virtual Appliance** to define the network connections required to activate licenses and install updates.
3. **Register Panorama.**
4. **Activate a Panorama Support License.**
5. **Activate/Retrieve a Firewall Management License on the Panorama Virtual Appliance.**
6. **Install Content and Software Updates for Panorama.** Install the same versions as those on the M-Series appliance.

#### Step 6
Load the Panorama configuration snapshot that you exported from the M-Series appliance into the Panorama virtual appliance.

1. Log in to the Panorama web interface of the Panorama virtual appliance, and select **Panorama > Setup > Operations**.
2. Click **Import named Panorama configuration snapshot**, browse to the Panorama configuration file you exported from the M-Series appliance, and click **OK**.
3. Click **Load named Panorama configuration snapshot**, select the **Name** of the configuration you just imported, select a **Decryption Key** (the master key for Panorama), and click **OK**. Panorama overwrites its current candidate configuration with the loaded configuration. Panorama displays any errors that occur when loading the configuration file.

If errors occurred, save them to a local file. Resolve each error to ensure the migrated configuration is valid. The configuration has been loaded once the commit is successful.

#### Step 7
Modify the configuration on the Panorama virtual appliance.

Required if the Panorama virtual appliance will use different values than the M-Series appliance.

1. Select **Panorama > Setup > Management**.
2. Edit the General Settings, modify the **Hostname**, and click **OK**.
3. Edit the Management Interface Settings, modify the values as necessary, and click **OK**.
Set Up Panorama

Transition to a Different Panorama Platform

Migrate from an M-Series Appliance to a Panorama Virtual Appliance (Continued)

Step 8 Set up the M-Series appliance as a Dedicated Log Collector and add it as a managed collector on the Panorama virtual appliance.

Loading the configuration from the M-Series appliance (Step 6) removes the default managed collector and Collector Group that are predefined on each M-Series appliance.

1. Power on the M-Series appliance.
2. Set up the M-Series Appliance as a Log Collector.
3. Configure a Managed Collector on the Panorama virtual appliance.
5. Select Commit > Commit to Panorama and Commit your changes to the Panorama configuration.

Step 9 Synchronize the Panorama virtual appliance with the firewalls to resume firewall management.

Complete this step during a maintenance window to minimize network disruption.

1. On the Panorama virtual appliance, select Panorama > Managed Devices and verify that the Device State column displays Connected for the firewalls.
   At this point, the Shared Policy (device groups) and Template columns display Out of sync for the firewalls.
2. Push your changes to device groups and templates:
   a. Select Commit > Push to Devices and Edit Selections.
   b. Select Device Groups, select every device group, Include Device and Network Templates, and click OK.
   c. Push your changes.
3. In the Panorama > Managed Devices page, verify that the Shared Policy and Template columns display In sync for the firewalls.

Migrate from an M-100 Appliance to an M-500 Appliance

You can migrate the Panorama configuration and firewall logs from an M-100 appliance to an M-500 appliance in Panorama mode (Panorama management server). You can also migrate the firewall logs from an M-100 appliance to an M-500 appliance in Log Collector mode (Dedicated Log Collector). Because all the Log Collectors in a Collector Group must be the same hardware model, you must migrate all or none of the M-100 appliances in any Collector Group.

In the following procedure, the Panorama management server is deployed in an active/passive high availability (HA) configuration, you will migrate both the configuration and logs, and the M-500 appliances will reuse the IP addresses from the M-100 appliances.

If you will migrate only the logs and not the Panorama configuration, perform the task Migrate Logs to a New M-Series Appliance in Log Collector Mode or Migrate Logs to a New M-Series Appliance in Panorama Mode.

If you will migrate to a new Panorama management server that is not deployed in an HA configuration and the new Panorama must access logs on existing Dedicated Log Collectors, perform the task Migrate Log Collectors after Failure/RMA of Non-HA Panorama.
### Migrate from an M-100 Appliance to an M-500 Appliance

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Plan the migration.</td>
</tr>
<tr>
<td>-</td>
<td><strong>Upgrade the software</strong> on the M-100 appliance if its current release is earlier than 7.0; the M-500 appliance requires Panorama 7.0 or a later release. For important details about software versions, see Panorama, Log Collector, and Firewall Version Compatibility.</td>
</tr>
<tr>
<td>-</td>
<td><strong>Forward the System and Config logs</strong> that Panorama and Log Collectors generate to an external destination before the migration if you want to preserve those logs. The M-Series appliance in Panorama mode stores these log types on its SSD, which you cannot move between models. You can move only the RAID drives, which store firewall logs.</td>
</tr>
<tr>
<td>-</td>
<td><strong>Schedule a maintenance window for the migration.</strong> Although firewalls can buffer logs after the M-100 appliance goes offline and then forward the logs after the M-500 appliance comes online, completing the migration during a maintenance window minimizes the risk that logs will exceed the buffer capacities and be lost during the transition between appliances.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Migrate your subscriptions to the new appliance.</td>
</tr>
<tr>
<td>1.</td>
<td>Purchase the new support license and migration license.</td>
</tr>
<tr>
<td>2.</td>
<td>Provide your sales representative the serial number of the M-100 appliance you will phase out, the auth code you received when you purchased the M-500 appliance, and the effective date for the migration. On the effective date, Palo Alto Networks will automatically apply the auth code to the serial number of the M-500 appliance, phase out support for the M-100 appliance, and trigger support for the M-500 appliance. Consult your sales representative regarding how much time is available to complete the migration after the effective date. At the end of that period, Palo Alto Networks terminates the support entitlement on the M-100 appliance; it can no longer receive software or content updates.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Export the Panorama configuration from each M-100 appliance in Panorama mode.</td>
</tr>
<tr>
<td>Perform this task on each M-100 appliance HA peer:</td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Log in to the M-100 appliance and select <strong>Panorama &gt; Setup &gt; Operations</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Save named Panorama configuration snapshot</strong>, enter a <strong>Name</strong> to identify the configuration, and click <strong>OK</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>Click <strong>Export named Panorama configuration snapshot</strong>, select the <strong>Name</strong> of the configuration you just saved, and click <strong>OK</strong>. Panorama exports the configuration to your client system as an XML file.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Power off each M-100 appliance in Panorama mode.</td>
</tr>
<tr>
<td>1.</td>
<td>Log in to the M-100 appliance HA peer that you will power off.</td>
</tr>
<tr>
<td>2.</td>
<td>Select <strong>Panorama &gt; Setup &gt; Operations</strong>, and click <strong>Shutdown Panorama</strong>.</td>
</tr>
</tbody>
</table>
### Migrate from an M-100 Appliance to an M-500 Appliance (Continued)

**Step 5**  Perform the initial setup of each M-500 appliance.

1. Rack mount the M-500 appliances. Refer to the **M-500 Appliance Hardware Reference Guide** for instructions.
2. Perform Initial Configuration of the M-Series Appliance to define the network connections required to activate licenses and install updates.
3. Register Panorama.
4. Activate a Panorama Support License.
5. Activate a firewall management license. Use the auth code associated with the migration license.
6. Install Content and Software Updates for Panorama. Install the same versions as those on the M-100 appliance.
7. (Dedicated Log Collector only) Set up the M-Series Appliance as a Log Collector.

**Step 6**  Load the Panorama configuration snapshot that you exported from each M-100 appliance into each M-500 appliance in Panorama mode (both HA peers).

Perform this task on each M-500 appliance HA peer:

1. Log in to the M-500 appliance and select **Panorama > Setup > Operations**.
2. Click **Import named Panorama configuration snapshot**, **Browse** to the configuration file you exported from the M-100 appliance that has the same HA priority (primary or secondary) as the M-500 appliance will have, and click **OK**.
3. Click **Load named Panorama configuration snapshot**, select the **Name** of the configuration you just imported, select a **Decryption Key** (the master key for Panorama), and click **OK**. Panorama overwrites its current candidate configuration with the loaded configuration. Panorama displays any errors that occur when loading the configuration file. If errors occurred, save them to a local file. Resolve each error to ensure the migrated configuration is valid.
4. Click **Commit** and **Validate Changes**. Resolve any errors before proceeding.
5. Click **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.

**Step 7**  Synchronize the configuration between the M-500 appliance HA peers in Panorama mode.

1. On the active M-500 appliance, select the **Dashboard** tab and, in the High Availability widget, click **Sync to peer**.
2. In the High Availability widget, verify that the **Local** (primary M-500 appliance) is **active**, the **Peer** is passive, and the **Running Config** is **synchronized**.

**Step 8**  Move the RAID drives from each M-100 appliance to its replacement M-500 appliance to migrate the logs collected from firewalls.

In the following tasks, skip any steps that you already completed on the M-500 appliance.

- **Migrate Logs to a New M-Series Appliance in Panorama Mode.** Migrate logs from the M-100 appliance only if it uses a **default managed collector** for log collection.
- **Migrate Logs to a New M-Series Appliance in Log Collector Mode.**
**Migrate from an M-100 Appliance to an M-500 Appliance (Continued)**

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Synchronize the active M-500 appliance in Panorama mode with the firewalls to resume firewall management.</th>
<th>1. In the active M-500 appliance, select Panorama &gt; Managed Devices, and verify that the Device State column displays <strong>Connected</strong> for the firewalls. At this point, the Shared Policy (device groups) and Template columns display <strong>Out of sync</strong> for the firewalls.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Complete this step during a maintenance window to minimize network disruption.</td>
<td>2. Click Commit, for the Commit Type select Device Group, select every device group, select the Include Device and Network Templates check box, and click Commit again.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. In the Panorama &gt; Managed Devices page, verify that the Shared Policy and Template columns display <strong>In sync</strong> for the firewalls.</td>
</tr>
</tbody>
</table>
Access and Navigate Panorama Management Interfaces

Panorama provides three management interfaces:

- **Web interface**—The Panorama web interface has a look and feel similar to the firewall web interface. If you are familiar with the latter, you can easily navigate, complete administrative tasks, and generate reports from the Panorama web interface. This graphical interface enables you to access Panorama using HTTPS and it is the best way to perform administrative tasks. See Log in to the Panorama Web Interface and Navigate the Panorama Web Interface. If you need to enable HTTP access to Panorama, edit the Management Interface Settings on the Panorama > Setup > Management tab.

- **Command line interface (CLI)**—The CLI is a no-frills interface that allows you to type commands in rapid succession to complete a series of tasks. The CLI supports two command modes—operational and configuration—and each has its own hierarchy of commands and statements. When you become familiar with the nesting structure and the syntax for the commands, the CLI enables quick response times and administrative efficiency. See Log in to the Panorama CLI.

- **XML API**—The XML-based API is provided as a web service that is implemented using HTTP/HTTPS requests and responses. It enables you to streamline your operations and integrate with existing, internally developed applications and repositories. For details on using the Panorama API, refer to the PAN-OS and Panorama XML API Usage Guide.

Log in to the Panorama Web Interface

<table>
<thead>
<tr>
<th>Log in to the Panorama Web Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
</tr>
<tr>
<td><strong>Note</strong></td>
</tr>
</tbody>
</table>

Navigate the Panorama Web Interface

Use the Panorama web interface to configure Panorama, manage and monitor firewalls and Log Collectors, and access the web interface of each firewall through the **Context** drop-down. Refer to the Panorama online help for details on the options and fields in each web interface tab. The following is an overview of the tabs:
### Access and Navigate Panorama Management Interfaces

### Set Up Panorama

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>View general information about Panorama and network access settings. This tab includes widgets that display information about applications, logs, system resources, and system settings.</td>
</tr>
<tr>
<td>ACC</td>
<td>View the overall risk and threat level on the network, based on information that Panorama gathered from the managed firewalls.</td>
</tr>
<tr>
<td>Monitor</td>
<td>View and manage logs and reports.</td>
</tr>
<tr>
<td>Device Groups &gt; Policies</td>
<td>Create centralized policy rules and apply them to multiple firewalls/device groups. You must Add a Device Group for this tab to display.</td>
</tr>
<tr>
<td>Device Groups &gt; Objects</td>
<td>Define policy objects that policy rules can reference and that managed firewalls/device groups can share. You must Add a Device Group for this tab to display.</td>
</tr>
<tr>
<td>Templates &gt; Network</td>
<td>Configure network setting, such as network profiles, and apply them to multiple firewalls. You must Add a Template for this tab to display.</td>
</tr>
<tr>
<td>Templates &gt; Device</td>
<td>Configure device settings, such as server profiles and admin roles, and apply them to multiple firewalls. You must Add a Template for this tab to display.</td>
</tr>
<tr>
<td>Panorama</td>
<td>Configure Panorama, manage licenses, set up high availability, access software updates and security alerts, manage administrative access, and manage the deployed firewalls and Log Collectors.</td>
</tr>
</tbody>
</table>

### Log in to the Panorama CLI

You can log in to the Panorama CLI using a serial port connection or remotely using a Secure Shell (SSH) client.
<table>
<thead>
<tr>
<th>Log in to the Panorama CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Use SSH to log in to the Panorama CLI. The same instructions apply to an M-Series appliance in Log Collector mode. Optionally, you can <strong>Configure an Administrator with SSH Key-Based Authentication for the CLI.</strong></td>
</tr>
</tbody>
</table>
| 1. Ensure the following prerequisites are met:  
  • You have a computer with network access to Panorama.  
  • You know the Panorama IP address.  
  • The Management interface supports SSH, which is the default setting. If an administrator disabled SSH and you want to re-enable it, select **Panorama > Setup > Management**, edit the Management Interface Settings, select **SSH**, and click **OK** and **Commit.** |
| 2. To access the CLI using SSH:  
  a. Enter the Panorama IP address in the SSH client and use port 22.  
  b. Enter your administrative access credentials when prompted. After you log in, the *message of the day* displays, followed by the CLI prompt in Operational mode. For example:  
    
    ```
    admin@ABC_Sydney>
    ``` |
| • Use a serial port connection to log in to the Panorama CLI. |
| 1. Make sure that you have the following:  
  • A null-modem serial cable that connects Panorama to a computer with a DB-9 serial port  
  • A terminal emulation program running on the computer |
| 2. Use the following settings in the terminal emulation software to connect: 9600 baud; 8 data bits; 1 stop bit; No parity; No hardware flow control. |
| 3. Enter your administrative access credentials when prompted. After you log in, the message of the day displays, followed by the CLI prompt in Operational mode. |
| • Change to Configuration mode. |
| 1. To switch to Configuration mode, enter the following command at the prompt:  
  ```
  admin@ABC_Sydney> configure
  ``` |
| The prompt changes to **admin@ABC_Sydney#** |
Set Up Administrative Access to Panorama

Panorama implements Role-Based Access Control (RBAC) to enable you to specify the privileges and responsibilities of administrators. The following topics describe how to create administrator roles, access domains, and accounts for accessing the Panorama web interface and command line interface (CLI):

▲ Configure an Admin Role Profile
▲ Configure an Access Domain
▲ Configure Administrative Accounts and Authentication

Configure an Admin Role Profile

Admin Role profiles are custom Administrative Roles that enable you to define granular administrative access privileges to ensure protection for sensitive company information and privacy for end users. As a best practice, create Admin Role profiles that allow administrators to access only the areas of the management interfaces required to perform their jobs.

Configure an Admin Role Profile

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select Panorama &gt; Admin Roles and click Add.</td>
</tr>
<tr>
<td>2</td>
<td>Enter a Name for the profile and select the Role type: Panorama or Device Group and Template.</td>
</tr>
<tr>
<td>3</td>
<td>Configure access privileges to each functional area of Panorama (Web UI) and firewalls (Context Switch UI) by toggling the icons to the desired setting: Enable (read-write), Read Only, or Disable. If administrators with custom roles will commit device group or template changes to managed firewalls, you must give those roles read-write access to Panorama &gt; Device Groups and Panorama &gt; Templates. If you upgrade from an earlier Panorama version, the upgrade process provides read-only access to those nodes. You cannot manage access to the firewall CLI or XML API through context-switching privileges in Panorama roles.</td>
</tr>
<tr>
<td>4</td>
<td>If the Role type is Panorama, configure access to the XML API by toggling the Enabled/Disabled icon for each functional area.</td>
</tr>
<tr>
<td>5</td>
<td>If the Role type is Panorama, select an access level for the Command Line interface: None (default), superuser, superreader, or panorama-admin.</td>
</tr>
<tr>
<td>6</td>
<td>Click OK to save the profile.</td>
</tr>
</tbody>
</table>

Configure an Access Domain

Use Access Domains to define access for Device Group and Template administrators for specific device groups and templates, and also to control the ability of those administrators to switch context to the web interface of managed firewalls. Panorama supports up to 4,000 access domains.
Configure an Access Domain

Step 1  Select Panorama > Access Domain and click Add.

Step 2  Enter a Name to identify the access domain.

Step 3  Select an access privilege for Shared Objects:
- write—Administrators can perform all operations on Shared objects. This is the default value.
- read—Administrators can display and clone but cannot perform other operations on Shared objects. When adding non-Shared objects or cloning Shared objects, the destination must be a device group within the access domain, not the Shared location.
- shared-only—Administrators can add objects only to the Shared location. Administrators can display, edit, and delete Shared objects but cannot move or clone them.

A consequence of this option is that administrators can’t perform any operations on non-Shared objects other than to display them. An example of why you might select this option is for an organization that requires all objects to be in a single, global repository.

Step 4  Toggle the icons in the Device Groups tab to enable read-write or read-only access for device groups in the access domain.

If you set the Shared Objects access to shared-only, Panorama applies read-only access to the objects in any device groups for which you specify read-write access.

Step 5  Select the Templates tab and Add each template you want to assign to the access domain.

Step 6  Select the Device Context tab, select firewalls to assign to the access domain, and click OK. Administrators can access the web interface of these firewalls by using the Context drop-down in Panorama.

Configure Administrative Accounts and Authentication

If you have already configured Administrative Roles, external authentication services (if applicable), and Access Domains (for Device Group and Template administrators), you can Configure an Administrative Account. Otherwise, perform one of the other procedures listed below to configure administrative accounts for specific types of authentication.

- Configure an Administrative Account
- Configure an Administrator with Kerberos SSO, External, or Local Authentication
- Configure an Administrator with Certificate-Based Authentication for the Web Interface
- Configure an Administrator with SSH Key-Based Authentication for the CLI
- Configure RADIUS Vendor-Specific Attributes for Administrator Authentication
Configure an Administrative Account

Administrative accounts specify Administrative Roles, Administrative Authentication methods, and Access Domains for Panorama administrators.

You can’t add an administrator account to a Dedicated Log Collector (M-Series appliance in Log Collector mode). Only the predefined administrator account with the default username (admin) is available on Dedicated Log Collectors.

Configure an Administrative Account

Step 1 Select Panorama > Administrators and click Add.

Step 2 Enter a user Name for the administrator.

Step 3 Select an Authentication Profile if Panorama will use Kerberos SSO or an external service for authentication. If Panorama will use local authentication, set the Authentication Profile to None and enter a Password and then Confirm Password.

Step 4 For the Administrator Type, select the role type:
- Dynamic—Select a predefined administrator role.
- Custom Panorama Admin—Select the Admin Role Profile you created for this administrator.
- Device Group and Template Admin—In the Access Domain to Administrator Role section, add access domains and map each one to an Admin Role profile:
  1. Click Add.
  2. Select an Access Domain from the drop-down.
  3. Click the adjacent Admin Role cell.
  4. Select an Admin Role profile.

Step 5 (Optional) Select a Password Profile if you will use local authentication. For details, see Configure Panorama Password Profiles and Complexity.

Step 6 Click OK and Commit, select Panorama for the Commit Type, and click Commit again.

Configure an Administrator with Kerberos SSO, External, or Local Authentication

When you configure Administrative Authentication for an administrator account, you can combine Kerberos single sign-on (SSO) authentication with an external authentication service or with local authentication. You can also configure the administrator to use only one of those authentication methods.

Configure an Administrator with Kerberos SSO, External, or Local Authentication

Step 1 Create a Kerberos keytab. Required for Kerberos SSO authentication.

Step 2 Configure access domains. Required for Device Group and Template administrators.

Create a Kerberos keytab. A keytab is a file that contains Kerberos account information (principal name and hashed password) for Panorama.

Configure an Access Domain.
Configure an Administrator with Certificate-Based Authentication for the Web Interface

As a more secure alternative to password-based authentication to the Panorama web interface, you can configure certificate-based authentication for administrator accounts that are local to Panorama. Certificate-based authentication involves the exchange and verification of a digital signature instead of a password.

Configure an Administrator with Certificate-Based Authentication for the Web Interface (Continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Configure Admin Role profiles. Required if you are assigning a custom role to the administrator.</th>
<th>Configure an Admin Role Profile.</th>
</tr>
</thead>
</table>
| Step 4 | Configure access to an external authentication service if you will use one. | Select Panorama > Server Profiles, select the authentication service type (RADIUS, TACACS+, LDAP, or Kerberos), and configure the server profile:  
- Configure a RADIUS Server Profile.  
- Configure a TACACS+ Server Profile.  
- Configure an LDAP Server Profile.  
- Configure a Kerberos Server Profile. |
| Step 5 | Configure an authentication profile. Required for Kerberos SSO or external authentication.  
If your administrators are in multiple Kerberos realms, you can create an authentication profile for each realm and assign all the profiles to an authentication sequence. You can then assign the same authentication sequence to all administrators.  
For details, see Authentication Profiles and Sequences. | Configure an authentication profile or sequence. |
| Step 6 | Configure an administrator. | Configure an Administrative Account. |

Configure an Administrator with Kerberos SSO, External, or Local Authentication (Continued)

Step 1 Generate a certificate authority (CA) certificate on Panorama. You will use this CA certificate to sign the client certificate of each administrator. Create a self-signed root CA certificate. Alternatively, you can import a certificate from your enterprise CA.
Set Up Administrative Access to Panorama

Configure an Administrator with Certificate-Based Authentication for the Web Interface (Continued)

2. Enter a Name for the certificate profile and set the Username Field to Subject.  
3. Select Add in the CA Certificates section and select the CA Certificate you just created.  
4. Click OK to save the profile. |
| Step 3 | Configure Panorama to use the certificate profile for authenticating administrators. | 1. Select the Panorama > Setup > Management and edit the Authentication Settings.  
2. Select the Certificate Profile you just created and click OK. |
| Step 4 | Configure the administrator accounts to use client certificate authentication. | Configure an Administrative Account for each administrator who will access the Panorama web interface. Select the Use only client certificate authentication (Web) check box.  
If you have already deployed client certificates that your enterprise CA generated, skip to Step 8. Otherwise, continue with Step 5. |
| Step 5 | Generate a client certificate for each administrator. | Generate a certificate on Panorama. In the Signed By drop-down, select the CA certificate you created. |
| Step 6 | Export the client certificates. | 1. Export the certificates.  
2. Commit your changes. Panorama restarts and terminates your login session. Thereafter, administrators can access the web interface only from client systems that have the client certificate you generated. |
| Step 7 | Import the client certificate into the client system of each administrator who will access the web interface. | Refer to your web browser documentation as needed to complete this step. |
| Step 8 | Verify that administrators can access the web interface. | 1. Open the Panorama IP address in a browser on the computer that has the client certificate.  
2. When prompted, select the certificate you imported and click OK. The browser displays a certificate warning.  
3. Add the certificate to the browser exception list.  
4. Click Login. The web interface should appear without prompting you for a username or password. |

Configure an Administrator with SSH Key-Based Authentication for the CLI

For administrators who use Secure Shell (SSH) to access the Panorama CLI, SSH keys provide a more secure authentication method than passwords. SSH keys almost eliminate the risk of brute-force attacks, provide the option for two-factor authentication (private key and passphrase), and don’t send passwords over the network. SSH keys also enable automated scripts to access the CLI.
Configure an Administrator with SSH Key-Based Authentication for the CLI

**Step 1** Use an SSH key generation tool to create an asymmetric key pair on the client system of the administrator. The supported key formats are IETF SECSH and Open SSH. The supported algorithms are DSA (1024 bits) and RSA (768-4096 bits).

For the commands to generate the key pair, refer to your SSH client documentation.
The public key and private key are separate files. Save both to a location that Panorama can access. For added security, enter a passphrase to encrypt the private key. Panorama prompts the administrator for this passphrase during login.

**Step 2** Configure the administrator account to use public key authentication.

1. **Configure an Administrative Account.**
   - Configure one of two authentication methods to use as a fallback if SSH key authentication fails:
     - Select an Authentication Profile if you configured one for the administrator.
     - Select None and enter a Password and Confirm Password.
   - Select the Use Public Key Authentication (SSH) check box, click Import Key, Browse to the public key you just generated, and click OK.

2. Click OK and Commit, select Panorama for the Commit Type, and click Commit again.

**Step 3** Configure the SSH client to use the private key to authenticate to Panorama.

Perform this task on the client system of the administrator. Refer to your SSH client documentation as needed to complete this step.

**Step 4** Verify that the administrator can access the Panorama CLI using SSH key authentication.

1. Use a browser on the client system of the administrator to go to the Panorama IP address.

2. Log in to the Panorama CLI as the administrator. After entering a username, you will see the following output (the key value is an example):
   ```
   Authenticating with public key “dsa-key-20130415”
   ```

3. If prompted, enter the passphrase you defined when creating the keys.

Configure RADIUS Vendor-Specific Attributes for Administrator Authentication

The following procedure provides an overview of the tasks required to configure RADIUS Vendor-Specific Attributes (VSAs) for administrator authentication to Panorama. For detailed instructions, refer to the following Knowledge Base (KB) articles:

- For Windows 2003 Server, Windows 2008 (and later), and Cisco ACS 4.0—**RADIUS Vendor-Specific Attributes (VSAs).**
- For Cisco ACS 5.2—**Configuring Cisco ACS 5.2 for use with Palo Alto Networks VSAs.**

Be sure to complete the following three tasks before you start this procedure:

- Create the administrative accounts in the directory service that your network uses (for example, Active Directory).
- Set up a RADIUS server that can communicate with that directory service.
Import the Palo Alto Networks RADIUS dictionary into your RADIUS server.

### Use RADIUS Vendor-Specific Attributes for Account Authentication

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Configure Panorama.</th>
<th>Step 2</th>
<th>Configure the RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Configure an Admin Role Profile if the administrator will use a custom role.</td>
<td>1.</td>
<td>Add the Panorama IP address or hostname as the RADIUS client.</td>
</tr>
<tr>
<td>2.</td>
<td>Configure an Access Domain if the administrator will use a Device Group and Template role.</td>
<td>2.</td>
<td>Define the VSAs for administrator authentication. You must specify the vendor code (25461 for Panorama) and the VSA name, number, and value.</td>
</tr>
<tr>
<td>3.</td>
<td>Configure a RADIUS server profile.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Configure an authentication profile. Set the authentication Type to RADIUS and assign the RADIUS Server Profile.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Configure Panorama to use the authentication profile for administrator access: select Panorama &gt; Setup &gt; Management, edit the Authentication Settings, and select the Authentication Profile.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Click OK and Commit, select Panorama for the Commit Type, and click Commit again.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Manage Firewalls

To use Panorama for managing Palo Alto Networks firewalls, you must add the firewalls as managed devices and then assign them to device groups and to templates or template stacks. The following tasks best suit a first-time firewall deployment. Before proceeding, review Plan Your Deployment to understand the deployment options.

▲ Add a Firewall as a Managed Device
▲ Manage Device Groups
▲ Manage Templates and Template Stacks
▲ Transition a Firewall to Panorama Management
▲ Use Case: Configure Firewalls Using Panorama

To view the Objects and Policies tabs on the Panorama web interface, you must first create at least one device group. To view the Network and Device tabs, you must create at least one template. These tabs contain the options by which you configure and manage the firewalls on your network.
Add a Firewall as a Managed Device

To use Panorama for central management of firewalls, the first step is to add them as managed devices. Before starting, collect the firewall serial numbers and prepare each firewall as follows:

- **Perform initial configuration** on the firewall so that it is accessible and can communicate with Panorama over the network.
- Add the Panorama IP address(es) (one server or two, if Panorama is configured in a high availability pair) in the Panorama Settings section of the **Device > Setup > Management** tab and commit the changes.
- **Set up the data interfaces.** For each interface you plan to use, select the interface type and attach it to a security zone so that you can push configuration and policy from Panorama.

You can then add the firewalls as managed devices on Panorama.

When you add a firewall as a managed device, it uses an SSL connection with AES-256 encryption to register with Panorama. Panorama and the firewall authenticate each other using 2,048-bit certificates and use the SSL connection for configuration management and log collection.

### Add a Firewall as a Managed Device

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Add the firewall to Panorama.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select <strong>Panorama &gt; Managed Devices</strong> and click <strong>Add</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Enter the serial number for each firewall (one entry per line) that you want to manage centrally using Panorama, and then click <strong>OK</strong>. The Managed Devices page displays the new firewall.</td>
</tr>
<tr>
<td>3.</td>
<td><strong>(Optional)</strong> Add a <strong>Tag</strong>. Tags make it easier for you to find a firewall from a large list; they help you to dynamically filter and refine the list of firewalls that display. For example, if you add a tag called branch office, you can filter for all branch office firewalls across your network.</td>
</tr>
<tr>
<td>a.</td>
<td>Select the check box beside the firewall and click <strong>Tag</strong>.</td>
</tr>
<tr>
<td>b.</td>
<td>Click <strong>Add</strong>, enter a string of up to 31 characters (no empty spaces), and click <strong>OK</strong>.</td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Panorama</strong>, and click <strong>Commit</strong> again.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Verify that the firewall is connected to Panorama.</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the <strong>Panorama &gt; Managed Devices</strong> page, the Device State column displays whether the firewall is connected or disconnected to Panorama.</td>
<td></td>
</tr>
</tbody>
</table>
Manage Device Groups

▲ Add a Device Group
▲ Create a Device Group Hierarchy
▲ Create Objects for Use in Shared or Device Group Policy
▲ Revert to Inherited Object Values
▲ Manage Unused Shared Objects
▲ Manage Precedence of Inherited Objects
▲ Move or Clone a Policy Rule or Object to a Different Device Group
▲ Select a URL Filtering Vendor on Panorama
▲ Push a Policy Rule to a Subset of Firewalls
▲ Manage the Rule Hierarchy

Add a Device Group

After adding firewalls (see Add a Firewall as a Managed Device), you can group them into Device Groups (up to 256), as follows. Be sure to assign both firewalls in an active-passive high availability (HA) configuration to the same device group so that Panorama will push the same policy rules and objects to those firewalls. PAN-OS doesn't synchronize pushed rules across HA peers. To manage rules and objects at different administrative levels in your organization, Create a Device Group Hierarchy.

<table>
<thead>
<tr>
<th>Add a Device Group</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Select <strong>Panorama &gt; Device Groups</strong>, and click <strong>Add</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Enter a unique <strong>Name</strong> and a <strong>Description</strong> to identify the device group.</td>
</tr>
<tr>
<td><strong>Step 3</strong> In the Devices section, select check boxes to assign firewalls to the group. To search a long list of firewalls, use the Filters. You can assign any firewall to only one device group. You can assign each virtual system on a firewall to a different device group.</td>
</tr>
<tr>
<td><strong>Step 4</strong> (Optional) Select <strong>Group HA Peers</strong> for firewalls that are HA peers. The firewall name of the passive or active-secondary peer is in parentheses.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Select the <strong>Parent Device Group</strong> (default is <strong>Shared</strong>) that will be just above the device group you are creating in the device group hierarchy.</td>
</tr>
<tr>
<td><strong>Step 6</strong> If your policy rules will reference users and groups, assign a <strong>Master</strong> firewall. This will be the only firewall in the device group from which Panorama gathers username and user group information.</td>
</tr>
<tr>
<td><strong>Step 7</strong> Click <strong>OK</strong> and <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Panorama</strong>, and click <strong>Commit</strong> again.</td>
</tr>
<tr>
<td><strong>Step 8</strong> Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Device Group</strong>, select the device group you just created, and click <strong>Commit</strong> again.</td>
</tr>
</tbody>
</table>
# Create a Device Group Hierarchy

| Create a Device Group Hierarchy |  
|-------------------------------|---|
| **Step 1** Plan the Device Group Hierarchy. |  
| 1. Decide the device group levels, and which firewalls and virtual systems you will assign to each device group and the Shared location. You can assign any one firewall or virtual system (vsys) to only one device group. If a device group will be just an organizational container for lower level device groups, you don’t need to assign firewalls to it. |  
| 2. Remove firewall or vsys assignments from existing device groups if those assignments don’t fit your planned hierarchy. |  
| a. Select **Panorama > Device Groups** and select the device group. |  
| b. In the Devices section, clear the check boxes of firewalls and virtual systems you want to remove, and click **OK**. |  
| 3. If necessary, add more firewalls that you will assign to device groups: see Add a Firewall as a Managed Device. |  
| **Step 2** For each top-level device group, Add a Device Group. |  
| 1. In the **Panorama > Device Groups** page, click **Add** and enter a **Name** to identify the device group. |  
| 2. In the Devices section, select check boxes to assign firewalls and virtual systems to the device group. |  
| 3. Leave the **Parent Device Group** option at **Shared** (the default) and click **OK**. |  
| **Step 3** For each lower-level device group, Add a Device Group. |  
|  
| • For new device groups at each lower level, repeat **Step 2** but set the **Parent Device Group** to a device group at the next level above. |  
| • For each existing device group, in the **Device Groups** page, select the device group to edit it, select a **Parent Device Group**, and click **OK**. |  
| If you move a device group to a different parent, all its descendant device groups move with it, along with all firewalls, policy rules, and objects associated with the device group and its descendants. If the new parent is in another access domain, the moved device group will no longer have membership in the original access domain. If the new access domain has read-write access for the parent device group, it will also have read-write access for the moved device group. If the new access domain has read-only access for the parent, it will have no access for the moved device group. To reconfigure access for device groups, see Configure an Access Domain. |
### Create a Device Group Hierarchy (Continued)

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Configure, move, and clone objects and policy rules as needed to account for inheritance in the device group hierarchy.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Create Objects for Use in Shared or Device Group Policy, or edit existing objects. You can edit objects only at their location: the device group to which they are assigned. Descendant device groups inherit read-only instances of the objects from that location. However, you can optionally Override inherited object values.</td>
</tr>
<tr>
<td></td>
<td>• Create or edit policies.</td>
</tr>
<tr>
<td></td>
<td>• Move or Clone a Policy Rule or Object to a Different Device Group.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Override inherited object values. Applicable only if object values in a particular device group must differ from the values inherited from an ancestor device group. After overriding an object, you can override it again in descendant device groups. However, you can never override shared or predefined (default) objects. In the Objects tab, inherited objects have a green icon in the Name column, and the Location column displays the ancestor device group.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. In the Objects tab, select the object type (for example, Objects &gt; Addresses).</td>
</tr>
<tr>
<td></td>
<td>2. Select the Device Group that will have the override instance.</td>
</tr>
<tr>
<td></td>
<td>3. Select the object and click Override.</td>
</tr>
<tr>
<td></td>
<td>4. Edit the values. You can’t edit the Name or Shared settings.</td>
</tr>
<tr>
<td></td>
<td>5. Click OK. The Name column displays a yellow-overlapping-green icon for the object to indicate it is overridden.</td>
</tr>
<tr>
<td></td>
<td>If necessary, you can later Revert to Inherited Object Values.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Save and commit your changes. Perform a Panorama and device group commit after any change to the hierarchy. You must also perform a template commit if a template references objects in a device group (for example, interfaces referencing addresses), and a firewall assigned to the template is no longer assigned to that device group because of a hierarchy change.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Click Commit, for the Commit Type select Panorama, and click Commit again.</td>
</tr>
<tr>
<td></td>
<td>2. Click Commit, for the Commit Type select Device Group, select all the device groups you added or changed, and click Commit again.</td>
</tr>
</tbody>
</table>

### Create Objects for Use in Shared or Device Group Policy

You can use an object in any policy rule that is in the Shared location, or in the same device group as the object, or in descendants of that device group (for details, see **Device Group Objects**).
Create Objects for Use in Shared or Device Group Policy

1. Select the **Objects > Security Profiles > URL Filtering** tab and click **Add**.
   The **Objects** tab appears only after you **Add a Device Group** (at least one).
2. Enter a **Name** and a **Description**.
3. Select the **Shared** check box.
4. The **Disable Override** check box is cleared by default, which means you can override inherited instances of the object in all device groups. To disable overrides for the object, select the check box.
5. In the **Categories** tab, select the check box of every Category for which you want notification.
6. In the **Action** column, select **Alert**.
7. Click **OK** and **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.

1. Select the **Objects > Addresses** and select the **Device Group** in which you will use the object.
2. Click **Add** and enter a **Name** to identify the object.
3. Be sure to leave the **Shared** check box cleared.
4. The **Disable Override** check box is cleared by default, which means you can override inherited instances of the object in device groups that are descendants of the selected **Device Group**. To disable overrides for the object, select the check box.
5. Select the **Type** of address object and the associated value. For example, select **IP Range** and enter the IP address range for the web servers.
6. Click **OK** and **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.
7. Click **Commit**, for the **Commit Type** select **Device Group**, select the device group to which you added the object, and click **Commit** again.

1. In the pages of the **Objects** tab, the Location column indicates whether an object is shared or is specific to a device group.
   1. In the **Objects** tab, select the object type (**Objects > Addresses**, in this example).
   2. Select the **Device Group** to which you added the object.
      The **Objects** tab only displays objects that are in the selected **Device Group** or are inherited from an ancestor device group or the Shared location.
   3. Verify that the device group object appears. Note that the device group name in the Location column matches the selection in the **Device Group** drop-down.
Revert to Inherited Object Values

After overriding the values that a device group object inherits from an ancestor device group, you can revert the object to its ancestor values at any time. In the Objects tab, overridden objects have a yellow-overlapping-green icon (çon) in the Name column.

If you want to push ancestor values to all overridden objects instead of reverting a specific object, see Manage Precedence of Inherited Objects.
For the steps to override values, see Override inherited object values.
For details on object inheritance and overrides, see Device Group Objects.

Revert an Overridden Object

Step 1 In the Objects tab, select the object type (for example, Objects > Addresses) and select the Device Group that has an override instance of the object.

Step 2 Select the object, click Revert, and click Yes. The Name column displays a green icon for the object, indicating that it now inherits all values from an ancestor device group.

Step 3 Click Commit, for the Commit Type select Panorama, and click Commit again.

Step 4 Click Commit, for the Commit Type select Device Group, select the device group in which you reverted the object, and click Commit again.

Manage Unused Shared Objects

When you commit Device Groups, by default Panorama pushes all shared objects to firewalls whether or not any shared or device group policy rules reference the objects. However, you can configure Panorama to push only the shared objects that rules reference in the device groups you commit. The Share Unused Address and Service Objects with Devices check box enables you to limit the objects that Panorama pushes to the managed firewalls.

When Share Unused Address and Service Objects with Devices is disabled, Panorama ignores the Target firewalls when you Push a Policy Rule to a Subset of Firewalls. This means that all objects referenced by any rules are pushed to all firewalls in the device group.
To limit the number of objects pushed to a set of managed firewalls, add the policy rules to a child device group and reference shared objects as needed. See Create a Device Group Hierarchy for more information on creating a child device group.

On smaller firewalls, such as the PA-200, consider pushing only the relevant shared objects to the managed firewalls. This is because the number of objects that can be stored on a smaller firewall is considerably lower than that of the mid-size and larger models. Also, if you have many address and service objects that are unused, clearing the Share Unused Address and Service Objects with Devices check box reduces the commit times significantly on the firewalls because the configuration pushed to each firewall is smaller. Disabling this option may, however, increase the commit time on Panorama. This is because Panorama has to dynamically check whether policy rules reference a particular object.

Manage Unused Shared Objects

Step 1 Select Panorama > Setup > Management, and edit the Panorama Settings.
Manage Precedence of Inherited Objects

By default, when device groups at different levels in the Device Group Hierarchy have an object with the same name but different values (because of overrides, as an example), policy rules in a descendant device group use the object values in that descendant instead of using object values inherited from ancestor device groups. Optionally, you can reverse this order of precedence to push values from the highest ancestor containing the object to all descendant device groups. After you enable this option, the next device group commit replaces any overridden objects in the descendant device groups with the inherited objects.

If a firewall has locally defined objects with the same name as shared or device group objects that Panorama pushes, a commit failure occurs. If you want to revert a specific overridden object to its ancestor values instead of pushing ancestor values to all overridden objects, see Revert to Inherited Object Values.

Manage Precedence of Inherited Objects

Step 1 Select Panorama > Setup > Management and edit the Panorama Settings.

Step 2 If you want to reverse the default order of precedence, select the Objects defined in ancestors will take higher precedence check box. The dialog then displays the Find Overridden Objects link, which provides the option to see how many overridden (shadowed) objects will have ancestor values after you commit this change. You can hover over the quantity message to display the object names.

Find Overridden Objects only detects a Shared device group object that shares a name with another object in the device group.

Step 3 Click OK and Commit, for the Commit Type select Panorama, and click Commit again.

Step 4 (Optional) If you selected the Objects defined in ancestors will take higher precedence check box, Panorama won’t push the ancestor objects until you perform a device group commit: click Commit, for the Commit Type select Device Group, select the desired device groups, and click Commit again.

Move or Clone a Policy Rule or Object to a Different Device Group

On Panorama, if a policy rule or object that you will move or clone from a device group has references to objects that are not available in the target device group (Destination), you must move or clone the referenced objects and the referencing rule or object in the same operation. In a Device Group Hierarchy, remember that referenced objects might be available through inheritance. For example, shared objects are available in all device groups. You can perform a global find to check for references. If you move or clone an overridden object, be sure that overrides are enabled for that object in the parent device group of the Destination (see Create Objects for Use in Shared or Device Group Policy).
Manage Firewalls  Manage Device Groups

Move or Clone a Policy Rule or Object to a Device Group

Step 1 Log in to Panorama and select the rulebase (for example, Policy > Security > Pre Rules) or object type (for example, Objects > Addresses).

Step 2 Select the Device Group and select one or more rules or objects.

Step 3 Perform one of the following steps:
- (Rules only) Move > Move to other device group
- (Objects only) Move
- (Rules or objects) Clone

Step 4 In the Destination drop-down, select the new device group or Shared. The default is the Device Group selected in Step 2.

Step 5 (Rules only) Select the Rule order:
- Move top (default)—The rule will come before all other rules.
- Move bottom—The rule will come after all other rules.
- Before rule—In the adjacent drop-down, select the rule that comes after the Selected Rules.
- After rule—In the adjacent drop-down, select the rule that comes before the Selected Rules.

Step 6 The Error out on first detected error in validation check box is selected by default, which means Panorama will display the first error it finds and stop checking for more errors. For example, an error occurs if the Destination device group doesn't have an object that is referenced in the rule you are moving. When you move or clone many items at once, selecting this check box can simplify troubleshooting. If you clear the check box, Panorama will find all the errors before displaying them. Regardless of this setting, Panorama won't move or clone anything until you fix all the errors for all the selected items.

Step 7 Click OK to start the error validation. If Panorama finds errors, fix them and retry the move or clone operation. If Panorama doesn't find errors, it performs the operation.

Step 8 Click Commit, for the Commit Type select Panorama, and click Commit again.

Step 9 Click Commit, for the Commit Type select Device Group, select the original and destination device groups, and click Commit again.

Select a URL Filtering Vendor on Panorama

URL filtering enables firewalls to monitor and control web access for your users. The policy rules that you configure to control web access (Security, QoS, Captive Portal, and Decryption rules) reference URL categories. The URL filtering vendor you select on Panorama determines which URL categories are available for referencing in the rules that you add to device groups and push to firewalls.

By default, Panorama uses PAN-DB, a URL filtering database that is tightly integrated into PAN-OS and the Palo Alto Networks threat intelligence cloud. PAN-DB provides high-performance local caching to maximize in-line performance for URL lookups. The other vendor option is BrightCloud, a third-party URL database.

Unlike firewalls, Panorama does not download the URL database and does not require a URL filtering license.

The following topics describe how to change the URL filtering vendor on Panorama or on both Panorama and managed firewalls. You can also change the URL filtering vendor on just the firewalls.
Must Panorama and Firewalls Have Matching URL Filtering Vendors?

On any single Panorama management server or firewall, only one URL filtering vendor can be active: PAN-DB or BrightCloud. When selecting a vendor for Panorama, you must consider the vendor and PAN-OS version of the managed firewalls:

- PAN-OS 5.0.x and earlier versions—Panorama and the firewalls require matching URL filtering vendors.
- PAN-OS 6.0 or later versions—Panorama and the firewalls do not require matching URL filtering vendors. If a vendor mismatch is detected, the firewall maps the URL categories in the URL Filtering profiles and rules that it received from Panorama to URL categories that align with those of the vendor enabled on the firewall.

Therefore, for a deployment in which some firewalls run PAN-OS 6.0 or later and some firewalls run earlier PAN-OS versions, Panorama must use the same URL filtering vendor as the firewalls that run earlier PAN-OS versions. For example, if firewalls that run PAN-OS 5.0 use PAN-DB, and firewalls that run PAN-OS 7.0 use BrightCloud, Panorama must use PAN-DB.

Change the URL Filtering Vendor on HA Panorama

In a high availability (HA) deployment, each Panorama peer must be in a non-functional state when you change the URL filtering vendor. Therefore, to avoid disrupting Panorama operations, change the URL filtering vendor on the passive Panorama (Panorama2 in this example) and then trigger failover before changing the vendor on the active Panorama (Panorama1 in this example).

<table>
<thead>
<tr>
<th>Change URL Filtering Vendor on HA Panorama</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Change the URL filtering vendor on each Panorama HA peer.</td>
</tr>
<tr>
<td>Complete this task on Panorama2 (passive peer) before Panorama1 (active peer).</td>
</tr>
<tr>
<td>1. Log in to the Panorama web interface.</td>
</tr>
<tr>
<td>2. Select <strong>Panorama &gt; High Availability</strong> and <strong>Suspend local Panorama</strong>. When you perform this step on Panorama1, failover occurs and Panorama2 becomes active.</td>
</tr>
<tr>
<td>3. Select <strong>Panorama &gt; Setup &gt; Management</strong> and edit the General Settings.</td>
</tr>
<tr>
<td>4. Select the <strong>URL Filtering Database</strong> vendor: <strong>paloaltonetworks</strong> (PAN-DB) or <strong>brightcloud</strong>.</td>
</tr>
<tr>
<td>5. Select <strong>Panorama &gt; High Availability</strong> and <strong>Make local Panorama functional</strong>. When you perform this step on Panorama1 with <strong>preemption</strong> enabled on both HA peers, Panorama1 automatically reverts to active status and Panorama2 reverts to passive status.</td>
</tr>
</tbody>
</table>
### Change URL Filtering Vendor on HA Panorama (Continued)

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Verify that the URL categories are available for referencing in policies.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Select <strong>Objects &gt; Security Profiles &gt; URL Filtering.</strong></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add</strong> and verify that the <strong>Categories</strong> tab of the URL</td>
</tr>
<tr>
<td></td>
<td>Filtering profile dialog displays the URL categories associated with the</td>
</tr>
<tr>
<td></td>
<td>selected vendor.</td>
</tr>
</tbody>
</table>

### Change the URL Filtering Vendor on non-HA Panorama

Perform this procedure to change the URL filtering vendor on a Panorama management server that is not deployed in a high availability (HA) configuration.

<table>
<thead>
<tr>
<th>Change URL Filtering Vendor on non-HA Panorama</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td>1.</td>
</tr>
<tr>
<td>2.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td>1.</td>
</tr>
<tr>
<td>2.</td>
</tr>
</tbody>
</table>
### Migrate Panorama and HA Firewalls from BrightCloud to PAN-DB

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Details</th>
</tr>
</thead>
</table>
| Step 1 | Determine which firewalls require new PAN-DB URL filtering licenses   | 1. Log in to Panorama and select **Panorama > Device Deployment > Licenses**.  
2. Check the URL column to determine which firewalls have PAN-DB licenses and whether the licenses are valid or expired.  
A firewall can have valid licenses for both BrightCloud and PAN-DB, but only one license can be active.  
If you're not sure whether a PAN-DB URL filtering license is active, access the firewall web interface, select **Device > Licenses**, and verify that the **Active** field displays **Yes** in the PAN-DB URL Filtering section.  
3. Purchase a new license for each firewall that does not have a valid PAN-DB license.  
In HA deployments, each firewall peer needs a distinct PAN-DB license and authorization code. Palo Alto Networks sends an email containing activation codes for the licenses you purchase. If you can't find this email, contact **Customer Support** before proceeding. |
| Step 2 | Change the URL filtering vendor to PAN-DB on Panorama                  | Access the Panorama web interface and perform one of the following tasks:  
- Change the URL Filtering Vendor on HA Panorama  
- Change the URL Filtering Vendor on non-HA Panorama |
| Step 3 | Configure the TCP session settings on both firewall HA peers to ensure sessions that are not yet synchronized will fail over when you suspend a peer. | Log in to the CLI of each firewall and run the following command:  
> set session tcp-reject-non-syn no |
Migrate Panorama and HA Firewalls from BrightCloud to PAN-DB (Continued)

**Step 4**  Migrate the URL filtering vendor to PAN-DB on each firewall HA peer.

- Complete this task on fw2 (passive or active-secondary peer) before fw1 (active or active-primary peer).

1. Access the firewall web interface, select **Device > High Availability > Operational Commands**, and **Suspend local device**.
   - Performing this step on fw1 triggers failover to fw2.
2. Select **Device > Licenses**.
3. In the License Management section, select **Activate feature using authorization code**, enter the **Authorization Code** and click **OK**.
   - Activating the PAN-DB license automatically deactivates the BrightCloud license.
4. In the PAN-DB URL Filtering section, **Download** the seed file, select your region, and click **OK**.
5. Access the Panorama web interface, click **Commit**, set the **Commit Type to Device Group**, select the firewall, and click **Commit** again.
6. Access the firewall web interface, select **Device > High Availability > Operational Commands**, and **Make local device functional**.
   - When you perform this step on fw1 with **preemption** enabled on both firewalls, fw1 automatically reverts to active (or active-primary) status and fw2 reverts to passive (or active-secondary) status.

**Step 5**  Revert both firewall HA peers to the original TCP session settings.

- Run the following command at the CLI of each firewall:
  
  ```
  set session tcp-reject-non-syn yes
  ```

Migrate Panorama and non-HA Firewalls from BrightCloud to PAN-DB

Perform this procedure to migrate the URL filtering vendor from BrightCloud to PAN-DB on Panorama and firewalls when the firewalls are not deployed in a high availability (HA) configuration. The migration automatically maps BrightCloud URL categories to PAN-DB URL categories.
Manage Device Groups

Push a Policy Rule to a Subset of Firewalls

A policy target allows you to specify the firewalls in a device group to which to push policy rules. It allows you to exclude one or more firewalls or virtual systems, or to apply a rule only to specific firewalls or virtual systems in a device group.

The ability to target a rule enables you to keep policies centralized on Panorama; it offers visibility and efficiency in managing the rules. Instead of creating local rules on a only or virtual system, targeted rules allow you to define the rules (as shared or device group pre- or post-rules) on Panorama (for details, see Device Group Policies).

Migrate Panorama and non-HA Firewalls from BrightCloud to PAN-DB

Step 1 Determine which firewalls require new PAN-DB URL filtering licenses.

1. Log in to Panorama and select Panorama > Device Deployment > Licenses.
2. Check the URL column to determine which firewalls have PAN-DB licenses and whether the licenses are valid or expired.
   
   A firewall can have valid licenses for both BrightCloud and PAN-DB, but only one license can be active.
   
   If you're not sure whether a PAN-DB URL filtering license is active, access the firewall web interface, select Device > Licenses, and verify that the Active field displays Yes in the PAN-DB URL Filtering section.
3. Purchase new licenses for the firewalls that don’t have valid PAN-DB licenses.
   
   Palo Alto Networks sends an email containing activation codes for the licenses you purchase. If you can’t find this email, contact Customer Support before proceeding.

Step 2 Change the URL filtering vendor to PAN-DB on Panorama.

Access the Panorama web interface and perform one of the following tasks:

- Change the URL Filtering Vendor on HA Panorama
- Change the URL Filtering Vendor on non-HA Panorama

Step 3 Migrate the URL filtering vendor to PAN-DB on each firewall.

1. Access the firewall web interface and select Device > Licenses.
2. In the License Management section, select Activate feature using authorization code, enter the Authorization Code, and click OK.
   
   Activating the PAN-DB license automatically deactivates the BrightCloud license.
3. In the PAN-DB URL Filtering section, Download the seed file, select your region, and click OK.
4. In the Panorama web interface, click Commit, set the Commit Type to Device Group, select the firewall, and click Commit again.
## Manage the Rule Hierarchy

The order of policy rules is critical for the security of your network. Within any policy layer (shared, device group, or locally defined rules) and rulebase (for example, shared Security pre-rules), the firewall evaluates rules from top to bottom in the order they appear in the pages of the Policies tab. The firewall matches a packet against the first rule that meets the defined criteria and ignores subsequent rules. Therefore, to enforce the most specific match, move the more specific rules above more generic rules.

### Push a Policy Rule to a Subset of Firewalls

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Create a rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>In this example, we define a pre-rule in the Security rulebase that permits users on the internal network to access the servers in the DMZ.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Target the rule to include or exclude a subset of firewalls.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To apply the rule to a selected set of firewalls:</td>
</tr>
<tr>
<td></td>
<td>2. Select the firewalls on which you want the rule to apply.</td>
</tr>
<tr>
<td></td>
<td>If you do not select firewalls to target, the rule is added to all of the (unchecked) firewalls in the device group.</td>
</tr>
<tr>
<td></td>
<td>By default, although the check box for the virtual systems in the device group is unchecked, all the virtual systems will inherit the rule on commit. Select the check box for one or more virtual systems to which you want the rule to apply.</td>
</tr>
<tr>
<td></td>
<td>3. <em>(Optional)</em> To exclude a subset of firewalls from inheriting the rule, select the check box <em>Install on all but specified devices</em>.</td>
</tr>
<tr>
<td></td>
<td>If you select <em>Install on all but specified devices</em> and do not select any firewall, the rule is added to none of the firewalls in the device group.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong> to add the rule.</td>
</tr>
<tr>
<td></td>
<td>5. Save the configuration changes.</td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Commit</strong>, for the Commit Type select <strong>Panorama</strong>, and click <strong>Commit</strong> again.</td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>Commit</strong>, for the Commit Type select <strong>Device Group</strong>, select the device group to which you just added the rule, and click <strong>Commit</strong> again.</td>
</tr>
</tbody>
</table>
To understand the order in which the firewall evaluates rules by layer and by type (pre-rules, post-rules, and default rules) across the Device Group Hierarchy, see Device Group Policies.

Manage the Rule Hierarchy

Step 1  View the rule hierarchy for each rulebase.
1. Select the Policies tab and click Preview Rules.
2. Filter the preview by Rulebase (for example, Security or QoS).
3. Filter the preview to display the rules of a specific Device Group and the rules it inherits from the Shared location and ancestor device groups. You must select a device group that has firewalls assigned to it.
4. Filter the preview by Device to display its locally defined rules.
5. Click the green arrow icon to apply your filter selections to the preview (see Figure: Rule Hierarchy).

Step 2  Delete or disable rules, if necessary.
To determine which rules a firewall doesn’t currently use, select that firewall in the Context drop-down on Panorama, select the rulebase (for example, Policies > Security), and select the Highlight Unused Rules check box. A dotted orange background indicates the rules that the firewall doesn’t use.
1. Select the rulebase (for example, Policies > Security > Pre Rules) that contains the rule you will delete or disable.
2. Select the Device Group that contains the rule.
3. Select the rule, and click Delete or Disable as desired. Disabled rules appear in italicized font.

Step 3  Reposition rules within a rulebase, if necessary.
To reposition local rules on a firewall, access its web interface by selecting that firewall in the Context drop-down before performing this step.
1. Select the rulebase (for example, Policies > Security > Pre Rules) that contains the rule you will move.
2. Select the Device Group that contains the rule.
3. Select the rule, select Move, and select:
   • Move Top—Moves the rule above all other rules in the device group (but not above rules inherited from Shared or ancestor device groups).
   • Move Up—Moves the rule above the one that precedes it (but not above rules inherited from Shared or ancestor device groups).
   • Move Down—Moves the rule below the one that follows it.
   • Move Bottom—Moves the rule below all other rules.
   • Move to other device group—See Move or Clone a Policy Rule or Object to a Different Device Group.

Step 4  If you modified the rules, save the changes.
1. Click Commit, for the Commit Type select Panorama, and click Commit again.
2. Click Commit, for the Commit Type select Device Group, select the device group that contains the rules you changed or deleted, and click Commit again.
Manage Templates and Template Stacks

Use templates and template stacks to define the common base configurations that enable firewalls to operate in your network. See Templates and Template Stacks for an overview of the issues you should consider when deciding which firewalls to add to which templates, ordering templates in a stack to manage layers of common and firewall group-specific settings, and overriding template settings with firewall-specific values.

To delete a template, you must first locally Disable/Remove Template Settings on the firewall. Only administrators with the superuser role can disable a template.

▲ Template Capabilities and Exceptions
▲ Add a Template
▲ Configure a Template Stack
▲ Override a Template Setting
▲ Disable/Remove Template Settings

Template Capabilities and Exceptions

You can use Templates and Template Stacks to define a wide array of settings, but you can perform the following tasks only locally on each managed firewall:

- Configure a device block list.
- Clear logs.
- Enable operational modes such as multi-vsys mode, Federal Information Processing Standards (FIPS) mode, or Common Criteria (CC) mode.
- Configure the IP addresses of a firewall HA pair.
- Configure a master key and diagnostics.
- Compare configuration files (Config Audit).

To Manage Licenses and Updates (software or content) for firewalls, use Panorama tab options, not templates.

Add a Template

You must add at least one template before Panorama will display the Device and Network tabs required to define the network set up and device configuration elements for firewalls. Panorama supports up to 512 templates.

You can avoid duplicating many configurations among templates by combining them into a template stack: see Templates and Template Stacks and Configure a Template Stack.
### Add a Template

**Step 1** Add a template.

1. Select Panorama > Templates.
2. Click Add and enter a unique Name to identify the template.
3. If the template has a virtual system (vsys) with configurations (for example, interfaces) that you want Panorama to push to firewalls that don’t have virtual systems, select it in the Default VSYS drop-down.
4. In the Devices section, select check boxes to assign firewalls to the template.
   
   Whenever you add a new managed firewall to Panorama, you must assign it to the appropriate template; Panorama does not automatically assign new firewalls. When you perform a template commit, Panorama pushes the configuration to every firewall assigned to the template.

5. (Optional) Select Group HA Peers to display a single check box for firewalls that are in a high availability (HA) configuration. Icons indicate the HA state: green for active and yellow for passive. The firewall name of the secondary peer is in parentheses.

   For active/passive HA, add both peers to the same template so that both will receive the configurations. For active/active HA, whether you add both peers to the same template depends on whether each peer requires the same configurations. For a list of the configurations that PAN-OS synchronizes between HA peers, see High Availability Synchronization.

6. Click OK and Commit, for the Commit Type select Panorama, and click Commit again.

7. Click Commit, for the Commit Type select Template, select the firewalls assigned to the template you just added, and click Commit again.

**Step 2** Verify that the template is available.

After you add the first template, Panorama displays the Device and Network tabs. These tabs display a Template drop-down. Check that the drop-down displays the template you just added.

**Step 3** Use the template to push a configuration change to firewalls.

Renaming a vsys is allowed only on the local firewall. If you rename a vsys on Panorama, you will create an entirely new vsys, or the new vsys name may get mapped to the wrong vsys on the firewall.

Let’s define a primary Domain Name System (DNS) server for the firewalls in the template.

1. In the Device tab, select the Template from the drop-down.
2. Select Device > Setup > Services > Global, and edit the Services section.
3. Enter an IP address for the Primary DNS Server.
4. Click OK and Commit, for the Commit Type select Panorama, and click Commit again.
5. Click Commit, for the Commit Type select Template, select the firewalls assigned to the template, and click Commit again.
Configure a Template Stack

A template stack is a combination of templates: Panorama pushes the settings from every template in the stack to the firewalls you assign to that stack. Panorama supports up to 128 template stacks and each stack can have up to 16 templates. For details and planning, see Templates and Template Stacks.

Configure a Template Stack

**Step 1** Plan the templates and their order in the stack.

For each template you will assign to the stack, Add a Template. When planning the priority order of templates within the stack (for overlapping settings), remember that Panorama doesn’t check the order for invalid relationships. For example, consider a stack in which the ethernet1/1 interface is of type Layer 3 in Template_A but of type Layer 2 with a VLAN in Template_B. If Template_A has a higher priority, Panorama will push ethernet1/1 as type Layer 3 but assigned to a VLAN.

Also note that a template configuration can’t reference a configuration in another template, even if both templates are in the same stack. For example, a zone configuration in Template_A can’t reference a zone protection profile in Template_B.

**Step 2** Create a template stack.

1. Select Panorama > Templates and click Add Stack.
2. Enter a unique Name to identify the stack.
3. For each of the Templates the stack will combine (up to 16), click Add and select the template. The dialog lists the added templates in order of priority with respect to duplicate settings, where values in the higher templates override those that are lower in the list. To change the order, select a template and click Move Up or Move Down.
4. In the Devices section, select check boxes to assign firewalls. You can’t assign individual virtual systems, only an entire firewall. You can assign any firewall to only one template or stack. After you finish selecting, click OK.
### Configure a Template Stack (Continued)

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Edit the <strong>Network</strong> and <strong>Device</strong> settings, if necessary.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>While Panorama pushes mode-specific settings only to firewalls that support those modes, this selective push doesn't adjust mode-specific values. For example, if a template has firewalls in Federal Information Processing Standards (FIPS) mode and an IKE Crypto profile that uses non-FIPS algorithms, the template commit will fail. To avoid such errors, use the <strong>Mode</strong> drop-down in the <strong>Network</strong> and <strong>Device</strong> tabs to filter mode-specific features and value options. In an individual firewall context, you can override settings that Panorama pushes from a stack in the same way you override settings pushed from a template: see Override a Template Setting.</td>
</tr>
<tr>
<td></td>
<td>Renaming a vsys is allowed only on the local firewall. If you rename a vsys on Panorama, you will create an entirely new vsys, or the new vsys name may get mapped to the wrong vsys on the firewall.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Verify that the template stack works as expected.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Perform the same verification steps as when you Add a Template but select the template stack from the <strong>Template</strong> drop-down:</td>
</tr>
<tr>
<td></td>
<td>1. Use the template to push a configuration change to firewalls.</td>
</tr>
<tr>
<td></td>
<td>2. Verify that the firewall is configured with the template settings that you pushed from Panorama.</td>
</tr>
</tbody>
</table>

### Override a Template Setting

While **Templates and Template Stacks** enable you to apply a base configuration to multiple firewalls, you might want to configure firewall-specific settings that don’t apply to all the firewalls in a template or template stack. Overrides allow for exceptions or modifications to meet your deployment needs. For example, if you
use a template to create a base configuration but a few firewalls in a test lab environment need different settings for the Domain Name System (DNS) server IP address or the Network Time Protocol (NTP) server, you can override the template settings.

If you want to disable or remove all the template or stack settings on a firewall instead of overriding a single setting, see Disable/Remove Template Settings.

**Override a Template Setting**

| Step 1 | Access the web interface of the firewall. | 1. Select Device > Setup > Services > Global and edit the Services section.  
2. Click the template icon (green cog) for the Primary DNS Server to enable overrides for that field.  
3. Enter a new IP address for the Primary DNS Server. Note that the dialog now displays a template override icon (orange-overlapping-green cogs) to indicate that the value is overridden.  
4. Click OK and Commit. |
| Step 2 | Navigate to the setting you will override. In this example, you will override the DNS server IP address that you assigned using a template in Add a Template. |  |

If you want to override a single setting instead of disabling or removing every template or stack setting, see Override a Template Setting. See Templates and Template Stacks for details on how to use these for managing firewalls.

**Disable/Remove Template Settings**

If you want to stop using a template or template stack for managing the configuration on a managed firewall, you can disable the template or stack. When disabling, you can copy the template/stack values to the local configuration of the firewall or delete the values.

If you want to override a single setting instead of disabling or removing every template or stack setting, see Override a Template Setting. See Templates and Template Stacks for details on how to use these for managing firewalls.

| Step 1 | Access the web interface of the managed firewall as an administrator with the Superuser role. You can directly access the firewall by entering its IP address in the browser URL field or, in Panorama, select the firewall in the Context drop-down. |
| Step 2 | Select Device > Setup > Management and edit the Panorama Settings. |
| Step 3 | Click Disable Device and Network Template. |
| Step 4 | (Optional) Select Import Device and Network Template before disabling, to save the configuration settings locally on the firewall. If you do not select this option, PAN-OS will delete all Panorama-pushed settings from the firewall. |
| Step 5 | Click OK twice and then click Commit to save the changes. |
Transition a Firewall to Panorama Management

If you have already deployed Palo Alto Networks firewalls and configured them locally, but now want to use Panorama for centrally managing them, you must perform pre-migration planning. The migration involves importing firewall configurations into Panorama and verifying that the firewalls function as expected after the transition. If some settings are unique to individual firewalls, you can continue accessing the firewalls to manage the unique settings. You can manage any given firewall setting by pushing its value from Panorama or by configuring it locally on the firewall, but you cannot manage the setting through both Panorama and the firewall. If you want to exclude certain firewall settings from Panorama management, you can either:

- Migrate the entire firewall configuration and then, on Panorama, delete the settings that you will manage locally on firewalls. You can also Override a Template Setting that Panorama pushes to a firewall instead of deleting the setting on Panorama.
- Load a partial firewall configuration, including only the settings that you will use Panorama to manage.

Firewalls do not lose logs during the transition to Panorama management.

Plan the Transition to Panorama Management

- Migrate a Firewall to Panorama Management
- Migrate a Firewall HA Pair to Panorama Management
- Load a Partial Firewall Configuration into Panorama

Plan the Transition to Panorama Management

The following tasks are a high-level overview of the planning required to migrate firewalls to Panorama management:

- Decide which firewalls to migrate.
- Determine the Panorama and firewall software and content versions, and how you will Manage Licenses and Updates. For important details, see Panorama, Log Collector, and Firewall Version Compatibility.
- Plan Your Deployment for Panorama with respect to the URL filtering database (BrightCloud or PAN-DB), log collection, and administrator roles.
- Plan how to manage shared settings.

Plan the Device Group Hierarchy, Templates and Template Stacks in a way that will reduce redundancy and streamline the management of settings that are shared among all firewalls or within firewall sets. During the migration, you can select whether to import objects from the Shared location on the firewall into Shared on Panorama, with the following exceptions:

- If a shared firewall object has the same name and value as an existing shared Panorama object, the import excludes that firewall object.
- If the name or value of the shared firewall object differs from an existing shared Panorama object, Panorama imports the firewall object into each new device group that is created for the import.
- If a configuration imported into a template references a shared firewall object, or if a shared firewall object references a configuration imported into a template, Panorama imports the object as a shared
object regardless of whether you select the **Import devices’ shared objects into Panorama’s shared context** check box.

- Determine if the firewall has configuration elements (policies, objects, and other settings) that you don’t want to import, either because Panorama already contains similar elements or because those elements are firewall-specific (for example, timezone settings) and you won’t use Panorama to manage them. You can perform a **global find** to determine if similar elements exist on Panorama.

- Decide the common zones for each device group. This includes a zone-naming strategy for the firewalls and virtual systems in each device group. For example, if you have zones called Branch LAN and WAN, Panorama can push policy rules that reference those zones without being aware of the variations in port or media type, model, or logical addressing schema.

- Create a post-migration test plan.

  You will use the test plan to verify that the firewalls work as efficiently after the migration as they did before. The plan might include tasks such as:
  - Monitor the firewalls for at least 24 hours after the migration.
  - Monitor Panorama and firewall logs for anomalies.
  - Check administrator logins on Panorama.
  - Test various types of traffic from multiple sources. For example, check bandwidth graphs, session counts, and deny-rule traffic log entries (see **Use Panorama for Visibility**). The testing should cover a representative sample of policy configurations.
  - Check with your network operations center (NOC) and security operations center (SOC) for any user-reported issues.
  - Include any other test criteria that will help verify firewall functionality.

### Migrate a Firewall to Panorama Management

When you import a firewall configuration, Panorama automatically creates a template to contain the imported network and device settings. To contain the imported policies and objects, Panorama automatically creates one device group for each firewall or one device group for each virtual system (vsys) in a multi-vsys firewall.

When you perform the following steps, Panorama imports the entire firewall configuration. Alternatively, you can **Load a Partial Firewall Configuration into Panorama**.

<table>
<thead>
<tr>
<th>Migrate a Firewall to Panorama Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Plan the migration.</td>
</tr>
</tbody>
</table>

Panorama can import configurations from firewalls that run PAN-OS 5.0 or later releases and can push configurations to those firewalls. The exception is that Panorama 6.1 and later releases cannot push configurations to firewalls running PAN-OS 6.0.0 through 6.0.3.

Panorama can import configurations from firewalls that are already managed devices but only if they are not already assigned to device groups or templates.
## Migrate a Firewall to Panorama Management (Continued)

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Add the firewall as a managed device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a Firewall as a Managed Device:</td>
<td></td>
</tr>
<tr>
<td>1. Log in to Panorama, select Panorama &gt; Managed Devices and click Add.</td>
<td></td>
</tr>
<tr>
<td>2. Enter the serial number of the firewall and click OK.</td>
<td></td>
</tr>
<tr>
<td>If you will import multiple firewall configurations, enter the serial number of each one on a separate line. Optionally, you can copy and paste the serial numbers from a Microsoft Excel worksheet.</td>
<td></td>
</tr>
<tr>
<td>3. Click Commit, for the Commit Type select Panorama, and click Commit again.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Set up a connection from the firewall to Panorama.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Log in to the firewall, select Device &gt; Setup, and edit the Panorama Settings.</td>
<td></td>
</tr>
<tr>
<td>2. In the Panorama Servers fields, enter the IP addresses of the Panorama management server.</td>
<td></td>
</tr>
<tr>
<td>3. Click OK and Commit.</td>
<td></td>
</tr>
</tbody>
</table>
Step 4  Import the firewall configuration into Panorama.

If you later decide to re-import a firewall configuration, first remove the firewall device groups and template to which it is a member. If the device group and template names are the same as the firewall hostname, then you can delete the device group and template before re-importing the firewall configuration or use the Device Group Name Prefix fields to define device group names that differ from the ones Panorama created in the original import. Additionally, firewalls don’t lose logs when you remove them from device groups or templates.

1. From Panorama, select Panorama > Setup > Operations, click Import device configuration to Panorama, and select the Device.

   Panorama can’t import a configuration from a firewall that is assigned to an existing device group or template.

2. (Optional) Enter a Template Name. The default value is the firewall name. You can’t use the name of an existing template.

3. For a multi-vsys firewall, optionally add a character string as a Device Group Name Prefix for all the device groups.

4. (Optional) Edit the Device Group names. If this is a multi-vsys firewall, each device group has a vsys name by default. Otherwise, the default value is the firewall name. You can’t use the names of existing device groups.

The Import devices’ shared objects into Panorama’s shared context check box is selected by default, which means Panorama compares imports objects that belong to the Shared location in the firewall to Shared in Panorama. If an imported object is not in the Shared context of the firewall, it is applied to each device group being imported. If you clear the check box, Panorama copies will not compare imported objects, and apply all shared firewall objects into device groups being imported instead of Shared. This could create duplicate objects, so selecting the check box is a best practice in most cases. To understand the consequences of importing shared or duplicate objects into Panorama, see Plan how to manage shared settings.

5. Select a Rule Import Location for the imported policy rules: Pre Rulebase or Post Rulebase. Regardless of your selection, Panorama imports default security rules (intrazone-default and interzone-default) into the post-rulebase.

   If Panorama has a rule with the same name as a firewall rule that you import, Panorama displays both rules. Delete one of the rules before performing a Panorama commit to prevent a commit error.

6. Click OK. Panorama displays the import status, result, details about your selections, details about what was imported, and any warnings. Click Close.

Step 5  Push the firewall configuration bundle to the firewall to remove all policy rules and objects from its local configuration. This step is necessary to prevent duplicate rule or object names, which would cause commit errors when you push the device group configuration from Panorama to the firewall in the next step.

1. Click Commit, for the Commit Type select Panorama, and click Commit again. Panorama creates a firewall configuration bundle named <firewall_name>_import.tgz, in which all policies and objects are removed.

2. In Panorama, select Panorama > Setup > Operations and click Export or push device config bundle.

3. Select the Device from which you imported the configuration, click OK, and click Push & Commit. Panorama pushes the bundle and initiates a commit on the firewall.

4. Click Close after the push has committed successfully.
### Migrate a Firewall to Panorama Management (Continued)

#### Step 6  Fine-tune the imported configuration.

1. In Panorama, select Panorama > Config Audit, select the Running config and Candidate config for the comparison, click Go, and review the output.
2. Update the device group and template configurations as needed based on the configuration audit and any warnings that Panorama displayed after the import. For example:
   - Delete redundant objects and policy rules.
   - Move or Clone a Policy Rule or Object to a Different Device Group.
   - Move firewalls to different device groups or templates.
   - Move a device group that Panorama created during the import to a different parent device group: Select Panorama > Device Groups, select the device group you want to move, select a new Parent Device Group, and click OK.

#### Step 7  Push the device group and template configurations to the firewall to complete the transition to centralized management.

If you are migrating multiple firewalls, perform all the preceding steps—including this one—for each firewall before continuing.

1. In Panorama, click Commit and for the Commit Type select Device Group.
2. Select the Merge with Device Candidate Config, Include Device and Network Templates and Force Template Values check boxes.
3. Select the device groups that contain the imported firewall configurations and click Commit.

#### Step 8  Consolidate all the imported firewall configurations.

Required if you are migrating multiple firewalls. Settings might be duplicated among the firewalls. For example, if you imported an object with the same name from two firewalls, you must delete one object in Panorama before performing a commit on Panorama.

1. After importing all the firewall configurations, update the device groups and templates as needed to eliminate redundancy and streamline configuration management: see Fine-tune the imported configuration. (You don’t need to push firewall configuration bundles again.)
2. Configure any firewall-specific settings.
   - If the firewalls will have local zones, you must create them before performing a device group or template commit; Panorama can’t poll the firewalls for zone name or zone configuration. If you will use local firewall rules, ensure their names are unique (not duplicated in Panorama). If necessary, you can Override a Template Setting with a firewall-specific value.
3. In Panorama, click Commit, for the Commit Type select Device Group, select the device groups, select the Include Device and Network Templates check box, and click Commit.

#### Step 9  Perform your post-migration test plan.

Perform the verification tasks that you devised during the migration planning to confirm that the firewalls work as efficiently with the Panorama-pushed configuration as they did with their original local configuration: see Create a post-migration test plan.
Migrate a Firewall HA Pair to Panorama Management

If you have a pair of firewalls in an HA configuration that you want to manage using Panorama, you have the option to import the configuration local to your firewall HA pair to Panorama without needing to recreate any configurations or policies. You first import the firewall configurations to Panorama, which are used to create a new device group and template. You will perform a special configuration push of the device group and template to the firewalls to overwrite the local firewall configurations and synchronize the firewalls with Panorama.

### Migrate a Firewall HA Pair to Panorama Management

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Plan the migration.</th>
<th>See the checklist in Plan the Transition to Panorama Management.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Disable configuration synchronization between the HA peers.</td>
<td>Repeat these steps for both firewalls in the HA pair. 1. Log in to the web interface on each firewall, select Device &gt; High Availability &gt; General and edit the Setup section. 2. Clear Enable Config Sync and click OK. 3. Commit the configuration changes on each firewall.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Connect each firewall to Panorama. If Panorama is already receiving logs from these firewalls, you do not need to perform this step. Continue to Step 5.</td>
<td>Repeat these steps for both firewalls in the HA pair. 1. Log in to the web interface on each firewall, select Device &gt; Setup &gt; Management and edit the Panorama Settings. 2. In the Panorama Servers fields, enter the IP addresses of the Panorama management servers, confirm Panorama Policy and Objects and Device and Network Template are enabled and select OK. 3. Commit the configuration changes on each firewall.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Add each firewall as a managed device. If Panorama is already receiving logs from these firewalls, you do not need to perform this step. Continue to Step 5.</td>
<td>Add a Firewall as a Managed Device: 1. Log in to Panorama, select Panorama &gt; Managed Devices and click Add. 2. Enter the serial number of each firewall and click OK. 3. Select Commit &gt; Commit to Panorama and Commit your changes. 4. Verify that the Device State for each firewall is Connected.</td>
</tr>
</tbody>
</table>
Transition a Firewall to Panorama Management

Manage Firewalls

Step 5  Import each firewall configuration into Panorama.

If you later decide to re-import a firewall configuration, first remove the firewall device groups and template to which it is a member. If the device group and template names are the same as the firewall hostname, then you can delete the device group and template before re-importing the firewall configuration or use the Device Group Name Prefix fields to define device group names that differ from the ones Panorama created in the original import. Additionally, firewalls don’t lose logs when you remove them from device groups or templates.

1. From Panorama, select Panorama > Setup > Operations, click Import device configuration to Panorama, and select the Device.

   Panorama can’t import a configuration from a firewall that is assigned to an existing device group or template.

2. (Optional) Edit the Template Name. The default value is the firewall name. You can’t use the name of an existing template.

3. (Optional) Edit the Device Group names. For a multi-vsys firewall, each device group has a vsys name by default, so add a character string as a Device Group Name Prefix for each. Otherwise, the default value is the firewall name. You can’t use the names of existing device groups.

   The Import devices’ shared objects into Panorama’s shared context check box is selected by default, which means Panorama compares imports objects that belong to the Shared location in the firewall to Shared in Panorama. If an imported object is not in the shared context of the firewall, it is applied to each device group being imported. If you clear the check box, Panorama copies will not compare imported objects, and apply all shared firewall objects into device groups being imported instead of Shared. This could create duplicate objects, so selecting the check box is a best practice in most cases. To understand the consequences of importing shared or duplicate objects into Panorama, see Plan how to manage shared settings.

4. Commit to Panorama.

5. Select Panorama > Setup > Operations and select Export or push device config bundle. Select the Device, select OK and Push & Commit the configuration.

   HA Config Sync in Step 2 must be disabled on both firewalls before you push the device group and template.

6. Launch the Web Interface of the firewall and ensure that the configuration has been successfully committed. If not, Commit the changes locally on the firewall.

7. On Panorama, select Panorama > Managed Devices, and verify that the device group and template are in sync for the passive firewall. Verify policy rules, objects and network settings on the passive firewall match the active firewall.

8. Commit to Panorama.

9. Repeat Step 1-8 above on the second firewall. The process will create a device group and template for the firewall.

10. Commit to Panorama.

   The import process does not import the HA IP addresses and management IP address of the firewalls. These IP addresses will continue to be defined locally on the device.
Manage Firewalls

Transition a Firewall to Panorama Management

Migrate a Firewall HA Pair to Panorama Management (Continued)

**Step 6** Add the HA firewall pair into the same device group and template. Skip this step if the HA firewall pair are in an active/active configuration. Do not combine the HA firewall pair in to a single template if a unique Hostname, management IP address, or HA configuration is configured for each HA peer. You may also configure a unique Hostname, management IP address, or HA configuration locally the firewalls.

1. Select Panorama > Device Group, select the device group of the second firewall and Delete it.
2. Select the device group for the first firewall, select the second firewall, click OK and Commit to Panorama to add it to the same device group as the HA peer.
3. Select Panorama > Templates, select the template for the second firewall and Delete it.
4. Select the template for the first firewall, select OK and Commit to Panorama to add it to the same template as the HA peer.
5. Select Commit > Push to Devices and Push your configuration changes to the firewalls.

**Step 7** Enable configuration synchronization between the HA peers.

Repeat these steps for both firewalls in the HA pair if you plan on maintaining a local configuration that needs to be synchronized

1. Log in to the web interface on each firewall, select Device > High Availability > General and edit the Setup section.
2. Select Enable Config Sync and click OK.
3. Commit the configuration changes on each firewall.

Load a Partial Firewall Configuration into Panorama

If some configuration settings on a firewall are common to other firewalls, you can load those specific settings into Panorama and then push them to all the other firewalls or to the firewalls in particular device groups and templates.

**Load a Partial Firewall Configuration into Panorama**

**Step 1** Plan the transition to Panorama.

See the checklist in Plan the Transition to Panorama Management.
### Transition a Firewall to Panorama Management

#### Manage Firewalls

<table>
<thead>
<tr>
<th>Load a Partial Firewall Configuration into Panorama (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> Resolve how to manage duplicate settings, which are those that have the same names in Panorama as in a firewall. Before you load a partial firewall configuration, Panorama and that firewall might already have duplicate settings. Loading a firewall configuration might also add settings to Panorama that are duplicates of settings in other managed firewalls.</td>
</tr>
</tbody>
</table>
| **1.** On Panorama, perform a **global find** to determine if duplicate settings exist.  
**2.** Delete or rename the duplicate settings on the firewall if you will use Panorama to manage them, or delete or rename the duplicate settings on Panorama if you will use the firewall to manage them. If you will use the firewall to manage device or network settings, instead of deleting or renaming the duplicates on Panorama, you can also push the settings from Panorama (**Step 6**) and then **Override a Template Setting** on the firewall with firewall-specific values. |
| **Step 3** Export the entire firewall configuration to your local computer. |
| **1.** On the firewall, select **Device > Setup > Operations**.  
**2.** Click **Save named configuration snapshot**, enter a **Name** to identify the configuration, and click **OK**.  
**3.** Click **Export named configuration snapshot**, select the **Name** of the configuration you just saved, and click **OK**. The firewall exports the configuration as an XML file. |
| **Step 4** Import the firewall configuration snapshot into Panorama. |
| **1.** On Panorama, select **Panorama > Setup > Operations**.  
**2.** Click **Import named Panorama configuration snapshot**, **Browse** to the firewall configuration file you exported to your computer, and click **OK**.  
**A** After using this option to import a firewall configuration file, you can't use the Panorama web interface to load it. You must use the XML API or CLI, as described in the next step. |
Load the desired part of the firewall configuration into Panorama.

To specify a part of the configuration (for example, all application objects), you must identify the:

- **Source xpath**—The XML node in the firewall configuration file from which you are loading.
- **Destination xpath**—The node in the Panorama configuration to which you are loading.

### Use the XML API or CLI to identify and load the partial configuration:

1. Use the firewall XML API or CLI to identify the source xpath. For example, the xpath for application objects in vsys1 of the firewall is:
   `/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/application`

2. Use the Panorama XML API or CLI to identify the destination xpath. For example, to load application objects into a device group named US-West, the xpath is:
   `/config/devices/entry[@name='localhost.localdomain']/device-group/entry[@name='US-West']/application`

3. Use the Panorama CLI to load the configuration and commit the change:

   ```
   # load config partial from <filename> from-xpath <source-xpath> to-xpath <destination-xpath> mode [append|merge|replace]
   # commit
   ```

   For example, enter the following to load the application objects from vsys1 on an imported firewall configuration named fw1-config.xml into a device group named US-West on Panorama:

   ```
   # load config partial from fw1-config.xml from-xpath devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/application to-xpath /config/devices/entry[@name='localhost.localdomain']/device-group/entry[@name='US-West']/application mode merge
   # commit
   ```

### Push the partial configuration from Panorama to the firewall to complete the transition to centralized management.

1. On the firewall, delete any rules or objects that have the same names as those in Panorama. If the device group for that firewall has other firewalls with rules or objects that are duplicated in Panorama, perform this step on those firewalls also. For details, see Step 2.

2. On Panorama, click **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.

3. On Panorama, click **Commit** and for the **Commit Type** select **Device Group**.

4. Select the **Merge with Device Candidate Config**. Include **Device and Network Templates** and **Force Template Values** check boxes.

5. Select the device groups that contain the imported firewall configurations and click **Commit**.

6. If the firewall has a device or network setting that you won’t use Panorama to manage, **Override a Template Setting** on the firewall.
| Step 7 | Perform your post-migration test plan. | Perform the verification tasks that you devised during the migration planning to confirm that the firewall works as efficiently with the Panorama-pushed configuration as it did with its original local configuration: see Create a post-migration test plan. |
Use Case: Configure Firewalls Using Panorama

Let's say that you want to use Panorama in a high availability configuration to manage a dozen firewalls on your network: you have six firewalls deployed across six branch offices, a pair of firewalls in a high availability configuration at each of two data centers, and a firewall in each of the two regional head offices.

The first step in creating your central management strategy is to determine how to group the firewalls into device groups and templates to efficiently push configurations from Panorama. You can base the grouping on the business functions, geographic locations, or administrative domains of the firewalls. In this example, you create two device groups and three templates to administer the firewalls using Panorama:

- **Device Groups in this Use Case**
- **Templates in this Use Case**
- **Set Up Your Centralized Configuration and Policies**
Device Groups in this Use Case

In Use Case: Configure Firewalls Using Panorama, we need to define two device groups based on the functions the firewalls will perform:

- **DG_BranchAndRegional** for grouping firewalls that serve as the security gateways at the branch offices and at the regional head offices. We placed the branch office firewalls and the regional office firewalls in the same device group because firewalls with similar functions will require similar policy rulebases.
- **DG_DataCenter** for grouping the firewalls that secure the servers at the data centers.

We can then administer shared policy rules across both device groups as well as administer distinct device group rules for the regional office and branch office groups. Then for added flexibility, the local administrator at a regional or branch office can create local rules that match specific source, destination, and service flows for accessing applications and services that are required for that office. In this example, we create the following hierarchy for security rules. You can use a similar approach for any of the other rulebases.

<table>
<thead>
<tr>
<th>Device Groups</th>
<th>DG_BranchAndRegional</th>
<th>DG_DataCenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules</td>
<td>Regional</td>
<td>Datacenter</td>
</tr>
<tr>
<td>Shared pre-rule</td>
<td>Allow DNS and SNMP services.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Acceptable use policy that denies access to specified URL categories and peer-to-peer traffic that is of risk level 3, 4, and 5.</td>
<td></td>
</tr>
<tr>
<td>Device Group pre-rule</td>
<td>Allow Facebook to all users in the marketing group in the regional offices only.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Allow access to the Amazon cloud application for the specified hosts/servers in the datacenter.</td>
<td></td>
</tr>
<tr>
<td>Local rules on a device</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Device Group post-rule</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Shared post-rule</td>
<td>To enable logging for all Internet-bound traffic on your network, create a rule that allows or denies all traffic from the trust zone to the untrust zone.</td>
<td></td>
</tr>
</tbody>
</table>

Templates in this Use Case

When grouping firewalls for templates, we must take into account the differences in the networking configuration. For example, if the interface configuration is not the same—the interfaces are unlike in type, or the interfaces used are not alike in the numbering scheme and link capacity, or the zone to interface mappings are different—the firewalls must be in separate templates. Further, the way the firewalls are configured to access network resources might be different because the firewalls are spread geographically; for example, the DNS server, syslog servers and gateways that they access might be different. So, to allow for an optimal base configuration, in Use Case: Configure Firewalls Using Panorama we must place the firewalls in separate templates as follows:

- **T_Branch** for the branch office firewalls
• T_Regional for the regional office firewalls
• T_DataCenter for the data center firewalls

Set Up Your Centralized Configuration and Policies

In Use Case: Configure Firewalls Using Panorama, we would need to perform the following tasks to centrally deploy and administer firewalls:
▲ Add the Managed Firewalls and Deploy Updates
▲ Use Templates to Administer a Base Configuration
▲ Use Device Groups to Push Policy Rules
▲ Preview the Rules and Commit Changes

Add the Managed Firewalls and Deploy Updates

The first task in Use Case: Configure Firewalls Using Panorama is to add the firewalls as managed devices and deploy content updates and PAN-OS software updates to those firewalls.

Add the Managed Firewalls and Deploy Updates

<table>
<thead>
<tr>
<th>Step 1</th>
<th>For each firewall that Panorama will manage, Add a Firewall as a Managed Device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>In this example, add 12 firewalls.</td>
<td></td>
</tr>
</tbody>
</table>
### Use Case: Configure Firewalls Using Panorama

**Manage Firewalls**

#### Add the Managed Firewalls and Deploy Updates (Continued)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Deploy the content updates to the firewalls. If you purchased a Threat Prevention subscription, the content and antivirus databases are available to you. First install the Applications or Applications and Threats database, then the Antivirus. To review the status or progress for all tasks performed on Panorama, see Use the Panorama Task Manager.</td>
</tr>
<tr>
<td>1.</td>
<td>Select Panorama &gt; Device Deployment &gt; Dynamic Updates.</td>
</tr>
<tr>
<td>2.</td>
<td>Click Check Now to check for the latest updates. If the value in the Action column is Download, this indicates an update is available.</td>
</tr>
<tr>
<td>3.</td>
<td>Click Download. When the download completes, the value in the Action column changes to Install.</td>
</tr>
<tr>
<td>4.</td>
<td>In the Action column, click Install. Use the filters or user-defined tags to select the managed firewalls on which you would like to install this update.</td>
</tr>
<tr>
<td>5.</td>
<td>Click OK, then monitor the status, progress, and result of the content update for each firewall. The Result column displays the success or failure of the installation.</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Deploy the software updates to the firewalls.</td>
</tr>
<tr>
<td>1.</td>
<td>Select Panorama &gt; Device Deployment &gt; Software.</td>
</tr>
<tr>
<td>2.</td>
<td>Click Check Now to check for the latest updates. If the value in the Action column is Download, this indicates an update is available.</td>
</tr>
<tr>
<td>3.</td>
<td>Locate the version that you need for each hardware model and click Download. When the download completes, the value in the Action column changes to Install.</td>
</tr>
<tr>
<td>4.</td>
<td>In the Action column, click the Install link. Use the filters or user-defined tags to select the managed firewalls on which to install this version.</td>
</tr>
<tr>
<td>5.</td>
<td>Enable the check box for Reboot device after install or Upload only to device (do not install) and click OK. The Results column displays the success or failure of the installation.</td>
</tr>
</tbody>
</table>

#### Use Templates to Administer a Base Configuration

The second task in Use Case: Configure Firewalls Using Panorama is to create the templates you will need to push the base configuration to the firewalls.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>For each template you will use, Add a Template and assign the appropriate firewalls to each. In this example, create templates named T_Branch, T_Regional, and T_DataCenter.</td>
</tr>
</tbody>
</table>
Use Templates to Administer a Base configuration (Continued)

Step 2 Define a DNS server, NTP server, syslog server, and login banner. Repeat this step for each template.

1. In the **Device** tab, select the **Template** from the drop-down.
2. Define the DNS and NTP servers:
   a. Select **Device > Setup > Services > Global** and edit the Services.
   b. In the **Services** tab, enter an IP address for the **Primary DNS Server**.
      
      For any firewall that has more than one virtual system (vsys), for each vsys, add a DNS server profile to the template (**Device > Server Profiles > DNS**).
   c. In the **NTP** tab, enter an IP address for the **Primary NTP Server**.
   d. Click **OK** to save your changes.
3. Add a login banner: select **Device > Setup > Management**, edit the General Settings, enter text for the **Login Banner** and click **OK**.
4. Configure a Syslog server profile (**Device > Server Profiles > Syslog**).

Step 3 Enable HTTPS, SSH, and SNMP access to the management interface of the managed firewalls. Repeat this step for each template.

1. In the **Device** tab, select the **Template** from the drop-down.
2. Select **Setup > Management**, and edit the Management Interface Settings.
3. Under Services, select the **HTTPS**, **SSH**, and **SNMP** check boxes, and click **OK**.

Step 4 Create a Zone Protection profile for the firewalls in the data center template (**T_DataCenter**).

1. Select the **Network** tab and, in the **Template** drop-down, select **T_DataCenter**.
2. Select **Network Profiles > Zone Protection** and click **Add**.
3. For this example, enable protection against a SYN flood—In the **Flood Protection** tab, select the **SYN** check box, set the **Action** to **SYN Cookies**, set the **Alert** packets/second to 100, set the **Activate** packets/second to 1000, and set the **Maximum** packets/second to 10000.
4. For this example, enable alerts—In the **Reconnaissance Protection** tab, select the **Enable** check boxes for **TCP Port Scan**, **Host Sweep**, and **UDP Port Scan**. Ensure the Action values are set to **alert** (the default value).
5. Click **OK** to save the Zone Protection profile.
Use Case: Configure Firewalls Using Panorama

Manage Firewalls

Use Templates to Administer a Base configuration (Continued)

Step 5 Configure the interface and zone settings in the data center template (T_DataCenter), and then attach the Zone Protection profile you just created. Before performing this step, you must have configured the interfaces locally on the firewalls. As a minimum, for each interface, you must have defined the interface type, assigned it to a virtual router (if needed), and attached a security zone.

1. Select the Network tab and, in the Template drop-down, select T_DataCenter.
2. Select Network > Interface and, in the Interface column, click the interface name.
3. Select the Interface Type from the drop-down.
4. In the Virtual Router drop-down, click New Virtual Router. When defining the router, ensure the Name matches what is defined on the firewall.
5. In the Security Zone drop-down, click New Zone. When defining the zone, ensure that the Name matches what is defined on the firewall.
6. Click OK to save your changes to the interface.
7. Select Network > Zones, and select the zone you just created. Verify that the correct interface is attached to the zone.
8. In the Zone Protection Profile drop-down, select the profile you created, and click OK.

Step 6 Commit your template changes.

1. Click Commit, for the Commit Type select Panorama, and click Commit again.
2. Click Commit, for the Commit Type select Template, select the firewalls assigned to the templates in which you made changes, and click Commit again.

Use Device Groups to Push Policy Rules

The third task in Use Case: Configure Firewalls Using Panorama is to create the device groups to manage policy rules on the firewalls.

Use Device Groups to Push Policy Rules

Step 1 Create device groups and assign the appropriate firewalls to each device group: see Add a Device Group.

In this example, create device groups named DG_BranchAndRegional and DG_DataCenter. When configuring the DG_BranchAndRegional device group, you must assign a Master firewall. This is the only firewall in the device group that gathers user and group mapping information for policy evaluation.
Step 2  
Create a shared pre-rule to allow DNS and SNMP services.

1. Create a shared application group for the DNS and SNMP services.
   a. Select **Objects > Application Group** and click **Add**.
   b. Enter a **Name** and select the **Shared** check box to create a shared application group object.
   c. Click **Add**, type **DNS**, and select **dns** from the list. Repeat for **SNMP** and select **snmp, snmp-trap**.
   d. Click **OK** to create the application group.

2. Create the shared rule.
   a. Select the **Policies** tab and, in the **Device Group** drop-down, select **Shared**.
   b. Select the **Security > Pre-Rules** rulebase.
   c. Click **Add** and enter a **Name** for the security rule.
   d. In the **Source** and **Destination** tabs for the rule, click **Add** and enter a **Source Zone** and a **Destination Zone** for the traffic.
   e. In the **Applications** tab, click **Add**, type the name of the applications group object you just created, and select it from the drop-down.
   f. In the **Actions** tab, set the **Action to Allow**, and click **OK**.

Step 3  
Define the corporate acceptable use policy for all offices. In this example, create a shared rule that restricts access to some URL categories and denies access to peer-to-peer traffic that is of risk level 3, 4, or 5.

1. Select the **Policies** tab and, in the **Device Group** drop-down, select **Shared**.
2. Select **Security > Pre-Rules** and click **Add**.
3. In the **General** tab, enter a **Name** for the security rule.
4. In the **Source** and **Destination** tabs, click **Add** and select any for the traffic **Source Zone** and **Destination Zone**.
5. In the **Application** tab, define the application filter:
   a. Click **Add** and click **New Application Filter** in the footer of the drop-down.
   b. Enter a **Name**, and select the **Shared** check box.
   c. In the Risk column, select levels **3**, **4**, and **5**.
   d. In the Technology column, select **peer-to-peer**.
   e. Click **OK** to save the new filter.
6. In the **Service/URL Category** tab, **URL Category** section, click **Add** and select the categories you want to block (for example, **streaming-media**, **dating**, and **online-personal-storage**).
7. You can also attach the default URL Filtering profile—In the **Actions** tab, **Profile Setting** section, select the **Profile Type** option **Profiles**, and select the **URL Filtering** option **default**.
8. Click **OK** to save the security pre-rule.
## Use Device Groups to Push Policy Rules (Continued)

### Step 4
Allow Facebook for all users in the Marketing group in the regional offices only. Enabling a security rule based on user and group has the following prerequisite tasks:
- **Set up User-ID** on the firewalls.
- **Enable User-ID for each zone** that contains the users you want to identify.
- Define a master firewall for the DG_BranchAndRegional device group (Step 1).

1. Select the **Policies** tab and, in the **Device Group** drop-down, select DG_BranchAndRegional.
2. Select the **Security > Pre-Rules** rulebase.
3. Click **Add** and enter a **Name** for the security rule.
4. In the **Source** tab, **Add** the Source Zone that contains the Marketing group users.
5. In the **Destination** tab, **Add** the Destination Zone.
6. In the **User** tab, **Add** the Marketing user group to the Source User list.
7. In the **Application** tab, click **Add**, type **Facebook**, and then select it from the drop-down.
8. In the **Action** tab, set the **Action** to **Allow**.
9. In the **Target** tab, select the regional office firewalls and click **OK**.

### Step 5
Allow access to the Amazon cloud application for the specified hosts/servers in the data center.

1. Create an address object for the servers/hosts in the data center that need access to the Amazon cloud application.
   a. Select **Objects > Addresses** and, in the **Device Group** drop-down, select DG_DataCenter.
   b. Click **Add** and enter a **Name** for the address object.
   c. Select the **Type**, and specify an IP address and netmask (IP Netmask), range of IP addresses (IP Range), or FQDN.
   d. Click **OK** to save the object.
2. Create a security rule that allows access to the Amazon cloud application.
   a. Select **Policies > Security > Pre-Rules** and, in the **Device Group** drop-down, select DG_DataCenter.
   b. Click **Add** and enter a **Name** for the security rule.
   c. Select the **Source** tab, **Add** the Source Zone for the data center, and **Add** the address object (Source Address) you just defined.
   d. Select the **Destination** tab and **Add** the Destination Zone.
   e. Select the **Application** tab, click **Add**, type **amazon**, and select the Amazon applications from the list.
   f. Select the **Action** tab and set the **Action** to **Allow**.
   g. Click **OK** to save the rule.

### Step 6
To enable logging for all internet-bound traffic on your network, create a rule that matches trust zone to untrust zone.

1. Select the **Policies** tab and, in the **Device Group** drop-down, select **Shared**.
2. Select the **Security > Pre-Rules** rulebase.
3. Click **Add** and enter a **Name** for the security rule.
4. In the **Source** and **Destination** tabs for the rule, **Add** `trust_zone` as the Source Zone and `untrust_zone` as the Destination Zone.
5. In the **Action** tab, set the **Action** to **Deny**, set the **Log Setting** to **Log at Session end**, and click **OK**.
Preview the Rules and Commit Changes

The final task in Use Case: Configure Firewalls Using Panorama is to review the rules and commit the changes you have made to Panorama, device groups, and templates.

<table>
<thead>
<tr>
<th>Preview the Rules and Commit Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> In the Policies tab, click Preview Rules, and select a Rulebase, Device Group, and Device. This preview enables you to visually evaluate how rules are layered for a particular rulebase. Close the preview dialog when you are done.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Click Commit, for the Commit Type select Panorama, and click Commit again.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Click Commit, for the Commit Type select Device Group, select the device groups you added, select the Include Device and Network Templates check box, and click Commit again.</td>
</tr>
<tr>
<td><strong>Step 4</strong> In the Context drop-down, select the firewall to access its web interface and confirm that Panorama applied the template and policy configurations.</td>
</tr>
</tbody>
</table>
Manage Log Collection

All Palo Alto Networks next-generation firewalls can generate logs that provide an audit trail of firewall activities. For Centralized Logging and Reporting, you must forward the logs generated on the firewalls to Panorama. You can then configure Panorama to aggregate the logs and forward them to remote logging destinations. If you forward logs to a Panorama virtual appliance, you don’t need to perform any additional tasks to enable logging. If you will forward logs to an M-Series appliance in Panorama mode or Log Collector mode, you must add the Log Collectors as managed collectors and assign them to Collector Groups to access, manage, and update the Log Collectors using Panorama. To determine which deployment best suits your needs, see Plan a Log Collection Deployment.

To manage the System and Config logs that Panorama generates locally, see Monitor Panorama.

- Configure a Managed Collector
- Manage Collector Groups
- Configure Log Forwarding to Panorama
- Verify Log Forwarding to Panorama
- Modify Log Forwarding and Buffering Defaults.
- Configure Log Forwarding from Panorama to External Destinations
- Log Collection Deployments
Configure a Managed Collector

To enable the Panorama management server (Panorama virtual appliance or M-Series appliance in Panorama mode) to manage a Log Collector, you must add it as a managed collector. The M-Series appliance in Panorama mode has a predefined (default) local Log Collector. However, switching from Panorama Mode to Log Collector Mode would remove the local Log Collector and would require you to re-configure the appliance as a Dedicated Log Collector (M-Series appliance in Log Collector mode). When the Panorama management server has a high availability (HA) configuration, each HA peer can have a local Log Collector. Dedicated Log Collectors don’t support HA.

As a best practice, install the same Applications update on Panorama as on managed Collectors and firewalls. For details, see Panorama, Log Collector, and Firewall Version Compatibility. Palo Alto Networks recommends retaining a local Log Collector and local Collector Group on the M-Series appliance in Panorama mode, regardless of whether it manages Dedicated Log Collectors.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Rack mount the M-Series appliance. Refer to the M-100 or M-500 Hardware Reference Guide for instructions.</td>
</tr>
<tr>
<td>2.</td>
<td>Perform Initial Configuration of the M-Series Appliance. When configuring interfaces, configure only the Management (MGT) interface. When you switch to Log Collector mode later in this procedure, the mode change removes any Eth1 and Eth2 interface configurations. If the Log Collector will use Eth1 and Eth2, add them when configuring the Log Collector later in this procedure.</td>
</tr>
<tr>
<td>3.</td>
<td>Register Panorama and Install Licenses.</td>
</tr>
<tr>
<td>4.</td>
<td>Install Content and Software Updates for Panorama.</td>
</tr>
<tr>
<td>5.</td>
<td>Configure each array. This task is required to make the RAID disks available for logging. Optionally, you can add disks to Increase Storage on the M-Series Appliance.</td>
</tr>
</tbody>
</table>
## Configure a Managed Collector (Continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| **Step 2** | Switch from Panorama mode to Log Collector mode. | 1. Access the CLI of the M-Series appliance.<br>2. Enter the following command to switch to Log Collector mode:<br>`> request system system-mode Logger`<br>3. Enter Y to confirm the mode change. The M-Series appliance reboots. If the reboot process terminates your terminal emulation software session, reconnect to the M-Series appliance to display the Panorama login prompt.<br>   - If you see a CMS Login prompt, press Enter without typing a username or password.<br>4. Log back in to the CLI.<br>5. Enter the following command to verify that the switch to Log Collector mode succeeded:<br>`> show system info | match system-mode`<br>   - If the mode change succeeded, the output displays: `system-mode: logger`<br>

| **Step 3** | Enable connectivity among the M-Series appliances. | These steps vary by Log Collector type. For HA deployments, `<IPaddress1>` and `<IPaddress2>` are for the management interface of the primary and secondary Panorama management server respectively. For non-HA deployments, specify only `<IPaddress1>`.  
   - **Dedicated Log Collectors**—Run the following commands at the CLI of each Log Collector:<br>`> Configure`<br>`# set deviceconfig system panorama-server <IPaddress1> panorama-server-2 <IPaddress2>`<br>`# commit`  
   - **Local Log Collectors**—These steps are required only for an HA deployment:<br>a. Log into the CLI of the primary Panorama and enter:<br>`> Configure`<br>`# set deviceconfig system panorama-server <IPaddress2>`<br>`# commit`  
b. Log into the CLI of the secondary Panorama and enter:<br>`> Configure`<br>`# set deviceconfig system panorama-server <IPaddress1>`<br>`# commit` |
| **Step 4** | Record the serial number of the Log Collector. You will need this when you add the Log Collector as a managed collector. | The steps to display the serial number vary by Log Collector type:  
   - **Local**—Access the Panorama web interface and record the value on the Dashboard tab, General Information section, **Serial #** field. In an HA deployment, record the **Serial #** of each Panorama peer on which you will configure a Log Collector.  
   - **Dedicated**—Access the Log Collector CLI, run the `show system info` command, and record the serial number. |
## Configure a Managed Collector (Continued)

### Step 5 Configure the general settings of the Log Collector.

Use the web interface of the primary Panorama management server to perform these steps:

1. Select **Panorama > Managed Collectors** and **Add** a new Log Collector or edit the predefined local Log Collector (named **default**).

   Although the secondary Panorama HA peer has a predefined local Log Collector, you must manually add it on the primary Panorama.

2. In the **General** tab, **Collector S/N** field, enter the serial number you recorded for the Log Collector.

### Step 6 Configure network access for the Log Collector.

**Perform this step only for a Dedicated Log Collector or a local Log Collector on the secondary Panorama HA peer.**

Although you defined similar parameters during initial configuration of the Panorama management server, you must re-define the parameters for the Log Collector.

1. In the **Panorama Server IP** field, enter the IP address or FQDN of the solitary (non-HA) or primary (HA) Panorama. For an HA deployment, enter the IP address or FQDN of the secondary Panorama peer in the **Panorama Server IP 2** field. These fields are required.

2. Configure the IP addresses of the **Primary DNS Server** and **Secondary DNS Server**.

3. (Optional) Set the **Timezone** that Panorama will use to record log entries.

### Step 7 Configure administrative access to the Log Collector CLI.

**Only Dedicated Log Collectors require this step. The default CLI administrator is **admin**. You cannot modify this username nor add CLI administrators.**

1. Select the **Authentication** tab, select the password **Mode**, and enter the **Password** (the default is **admin**).

2. Enter the number of **Failed Attempts** to log in that Panorama allows before locking out the administrator. Enter the **Lockout Time** in minutes. These settings can help protect the Log Collector from a brute force attack.

### Step 8 Configure the Log Collector interfaces.

**Perform this step only for a Dedicated Log Collector or a local Log Collector on the secondary Panorama HA peer.**

The **Eth1** or **Eth2** interfaces are available only if you defined them during initial configuration of the Panorama management server.

1. Configure each interface that the Log Collector will use. Only the **Management** interface is required.

   For each interface, select the corresponding tab and configure one or both of the following field sets based on the IP protocols of your network.

   - **IPv4**—**IP Address**, **Netmask**, and **Default Gateway**
   - **IPv6**—**IPv6 Address/Prefix Length** and **Default IPv6 Gateway**

2. (Optional) In the **Management** tab, select the **SNMP** service if you will use SNMP to monitor the Log Collector. Using SNMP requires additional steps besides configuring the Log Collector. For details, see **Monitor Panorama and Log Collector Statistics Using SNMP**.

3. Click **OK** and **Commit**, set the **Commit Type** to **Panorama**, and click **Commit** again.

   This step is required before you can enable logging disks or assign the Eth1 and Eth2 interfaces to logging functions.

4. (Optional) Edit the Log Collector and select the interfaces (**mgmt**, **eth1**, or **eth2**) that it will use for **Device Log Collection** and **Collector Group Communication** (default is **mgmt**).
**Configure a Managed Collector (Continued)**

<table>
<thead>
<tr>
<th>Step 9</th>
<th>(Optional) Configure the Log Collector admin authentication.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select <strong>Panorama &gt; Managed Collectors</strong> and edit the Log Collector by clicking its name.</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the Log Collector admin password:</td>
</tr>
<tr>
<td></td>
<td>a. Select the password <strong>Mode</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. If you select <strong>Password</strong> mode, enter a plaintext <strong>Password</strong> and <strong>Confirm Password</strong>. If you selected <strong>Password Hash</strong> mode, enter a hashed password string of up to 63 characters.</td>
</tr>
<tr>
<td></td>
<td>c. (Password Hash only) Enter a hashed password string of up to 63 characters.</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the admin login security requirements:</td>
</tr>
<tr>
<td></td>
<td>a. Enter the number of login <strong>Failed Attempts</strong> value. The range is between the default 0 to the maximum of 10 where the value 0 specifies unlimited login attempts.</td>
</tr>
<tr>
<td></td>
<td>b. Enter the <strong>Lockout Time</strong> value between the default value 0 and the maximum of 60 minutes.</td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>OK</strong> to save your changes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Enable the logging disks.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select <strong>Disks</strong> and <strong>Add</strong> each disk pair.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>OK</strong> and <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Panorama</strong>, and click <strong>Commit</strong> again.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 11</th>
<th>Verify your changes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Verify that the <strong>Panorama &gt; Managed Collectors</strong> page lists the Log Collector you added. The Connected column displays a check mark to indicate that the Log Collector is connected to Panorama. You might have to wait a few minutes before the page displays the updated connection status.</td>
</tr>
<tr>
<td></td>
<td>Until you <strong>Configure a Collector Group</strong> and perform a Collector Group commit, the Configuration Status column displays Out of Sync, the Run Time Status column displays disconnected, and the CLI command <code>show interface all</code> displays the interfaces as down.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Statistics</strong> in the last column to verify that the logging disks are enabled.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 12</th>
<th>Next steps...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Before a Log Collector can receive firewall logs, you must:</td>
</tr>
<tr>
<td>1.</td>
<td><strong>Configure Log Forwarding to Panorama</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td><strong>Configure a Collector Group</strong>. The predefined local Log Collector is preassigned to a predefined Collector Group.</td>
</tr>
</tbody>
</table>
Manage Collector Groups

A Collector Group is 1 to 16 Log Collectors that operate as a single logical unit for collecting firewall logs. You can configure a Collector Group with multiple Log Collectors to ensure log redundancy or to accommodate logging rates that exceed the capacity of a single Log Collector (see Panorama Platforms). To understand the risks and recommended mitigations, see Caveats for a Collector Group with Multiple Log Collectors.

The M-Series appliance in Panorama mode (Panorama management server) has a predefined (default) local Collector Group that contains a predefined local Log Collector. However, switching to Log Collector mode would remove the local Log Collector and Collector Group; you would have to Set up the M-Series Appliance as a Log Collector, add it as a managed collector to the Panorama management server, and configure a Collector Group to contain the managed collector.

If you delete a Collector Group, you will lose logs. Palo Alto Networks recommends retaining a local Log Collector and local Collector Group on the M-Series appliance in Panorama mode, regardless of whether it manages Dedicated Log Collectors.

▲ Configure a Collector Group
▲ Move a Log Collector to a Different Collector Group
▲ Remove a Firewall from a Collector Group

Configure a Collector Group

After you configure Log Collectors and firewalls, you must assign them to a Collector Group so that the firewalls can send logs to the Log Collectors. A Collector Group with multiple Log Collectors (the maximum is 16) has the following requirements:

- All the Log Collectors in any particular Collector Group must be the same model, such as all M-100 appliances or all M-500 appliances.
- Log redundancy is available only if each Log Collector has the same number of logging disks. To add disks to a Log Collector, see Increase Storage on the M-Series Appliance.
### Configure a Collector Group

**Step 1** Perform the following tasks before configuring the Collector Group.

In these tasks, skip any steps that involve configuring or committing changes to the Collector Group; you will perform those steps later in the current procedure.

1. **Add a Firewall as a Managed Device** for each firewall that you will assign to the Collector Group.

2. **(Optional) Configure Log Forwarding from Panorama to External Destinations.**

3. **Configure a Managed Collector** for each Log Collector (1 to 16) that you will assign to the Collector Group.

   You must manually add each Dedicated Log Collector (M-Series appliance in Log Collector mode). The M-Series appliance in Panorama mode has a predefined local Log Collector that you don't need to add.

   If you will use SNMP for monitoring, select the SNMP service when you configure the Management interface of a Log Collector. Using SNMP requires additional steps besides configuring the Collector Group. For details, see Monitor Panorama and Log Collector Statistics Using SNMP.

**Step 2** Add the Collector Group.

1. Access the Panorama web interface, select **Panorama > Collector Groups**, and **Add** a Collector Group or edit an existing one.

   The M-Series appliance in Panorama mode has a predefined Collector Group named **default**.

2. In the **General** tab, enter a **Name** for the Collector Group if you are adding one. You cannot rename an existing Collector Group.

3. Enter the **Minimum Retention Period** in days (1-2,000) for which the Collector Group will retain firewall logs.

4. **(Optional) Enable log redundancy across collectors** to ensure that no logs are lost if any one Log Collector in the Collector Group becomes unavailable. Each log will have two copies and each copy will reside on a different Log Collector. Redundancy is available only if each Log Collector has the same number of logging disks.

   Enabling redundancy creates more logs and therefore requires more storage capacity. When a Collector Group runs out of space, it deletes older logs. Redundancy also doubles the log processing traffic in a Collector Group, which reduces its maximum logging rate by half, as each Log Collector must distribute a copy of each log it receives.

   If you add multiple Log Collectors to a single Collector group, enabling redundancy is a best practice.
Configure a Collector Group (Continued)

Step 3  (Optional) Configure SNMP monitoring.

Select the **Monitoring** tab, select the SNMP **Version** and enter the corresponding details:

- **V2c**—Enter the **SNMP Community String**, which identifies a community of SNMP managers and monitored devices (Log Collectors, in this case), and serves as a password to authenticate the community members to each other.

  Don’t use the default community string `public`; it is well known and therefore not secure.

- **V3**—Create at least one SNMP view group and one user. User accounts and views provide authentication, privacy, and access control when Log Collectors forward traps and SNMP managers get Log Collector statistics.

  - **Views**—Each view is a paired OID and bitwise mask: the OID specifies a MIB and the mask (in hexadecimal format) specifies which objects are accessible within (include matching) or outside (exclude matching) that MIB. Click **Add** in the first list and enter a **Name** for the group of views. For each view in the group, click **Add** and configure the view **Name**, **OID**, matching **Option** (include or exclude), and **Mask**.

  - **Users**—Click **Add** in the second list, enter a username in the Users column, select the **View** group from the drop-down, enter the authentication password (**Auth Password**) used to authenticate to the SNMP manager, and enter the privacy password (**Priv Password**) used to encrypt SNMP messages to the SNMP manager.

Step 4  Assign Log Collectors and firewalls to the Collector Group.

1. Select the **Device Log Forwarding** tab.

2. In the Collector Group Members section, **Add** the Log Collectors.

   All the Log Collectors in any particular Collector Group must be the same model: all M-100 appliances or all M-500 appliances.

3. In the Log Forwarding Preferences section, click **Add**.

4. In the Devices section, click **Modify**, select the firewalls, and click **OK**.

   You cannot assign PA-7000 Series firewalls to a Collector Group. However, when you monitor logs or generate reports for a device group that includes a PA-7000 Series firewall, Panorama queries the firewall in real-time to display its log data.

5. In the Collectors section, **Add** the Log Collectors to which the firewalls will forward logs. If you assign multiple Log Collectors, the first one will be the primary; if the primary becomes unavailable, the firewalls send logs to the next Log Collector in the list. To change the priority of a Log Collector, select it and **Move Up** (higher priority) or **Move Down** (lower priority).

6. Click **OK**.
Manage Log Collection

Step 5 Define the storage capacity (log quotas) and expiration period for each log type.

1. Return to the General tab and click the Log Storage value. If the field displays 0MB, verify that you enabled the disk pairs for logging and committed the changes (see Configure a Managed Collector, Disks tab).
2. Enter the log storage Quota(%) for each log type.
3. Enter the Max Days (expiration period) for each log type (range is 1-2,000). By default, the fields are blank for all log types, which means the logs never expire.

Step 6 (Optional) Configure log forwarding from the Collector Group to external services.

1. Select the Collector Log Forwarding tab.
2. For each log Severity level in the System, Threat, and Correlation tabs, click a cell in the SNMP Trap, Email Profile, or Syslog Profile column, and select the server profile.
3. In the Config, HIP Match, and Traffic tabs, select the SNMP Trap, Email, or Syslog server profile.
4. For each Verdict in the WildFire tab, click a cell in the SNMP Trap, Email Profile, or Syslog Profile column, and select the server profile.
5. Click OK to save the Collector Group.

Step 7 Commit the changes and verify that the Log Collectors you assigned to the Collector Group are connected to, and synchronized with, Panorama.

1. Click Commit, for the Commit Type select Panorama, and click Commit again.
2. Click Commit, for the Commit Type select Collector Group, select the Collector Group you added, and click Commit again.
3. Select Panorama > Managed Collectors. The Connected column displays a check mark icon to indicate that a Log Collector is connected to Panorama. The Configuration Status column indicates whether the configurations you committed to Panorama and the Log Collectors are synchronized (green icon) or are not synchronized (red icon) with each other.

The Collector Group won’t receive firewall logs until you Configure Log Forwarding to Panorama.

Move a Log Collector to a Different Collector Group

When you Plan a Log Collection Deployment, you assign Log Collectors to a Collector Group based on the logging rate and log storage requirements of that Collector Group. If the rates and required storage increase in a Collector Group, the best practice is to Increase Storage on the M-Series Appliance or Configure a Collector Group with additional Log Collectors. However, in some deployments, it might be more economical to move Log Collectors between Collector Groups.
The log data on a Log Collector becomes inaccessible after you remove it from a Collector Group. Also, you must perform a factory reset on the Log Collector before adding it to another Collector Group; a factory reset removes all configuration settings and logs.

When a Log Collector is local to an M-Series appliance in Panorama mode, move it only if the M-Series appliance is the passive peer in a high availability (HA) configuration. HA synchronization will restore the configurations that the factory reset removes. Never move a Log Collector when it’s local to an M-Series appliance that is the active HA peer.

All the Log Collectors in any particular Collector Group must be the same model, such as all M-100 appliances or all M-500 appliances.

Log redundancy is available only if each Log Collector has the same number of logging disks. To add disks to a Log Collector, see Increase Storage on the M-Series Appliance.

### Move a Log Collector to Different Collector Group

**Step 1** Remove the Log Collector from Panorama management.

1. Select **Panorama > Collector Groups** and select the Collector Group that contains the Log Collector you will move.
2. Select the **Device Log Forwarding** tab and, in the Log Forwarding Preferences list, perform the following steps for each set of firewalls assigned to the Log Collector you will move:
   a. In the Devices column, click the link for the firewalls assigned to the Log Collector.
   b. In the Collectors column, select the Log Collector and click **Delete**.
   c. Click **OK** twice to save your changes.
3. Select **Panorama > Managed Collectors**, select the Log Collector you will move, and click **Delete**.
4. Click **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.
5. Click **Commit**, for the **Commit Type** select **Collector Group**, select the Collector Group from which you deleted the Log Collector, and click **Commit** again.

**Step 2** Reset the Log Collector to its factory default settings.

1. Log in to the CLI of the Log Collector.
2. Enter the following CLI operational command:
   
   ```
   > debug system maintenance-mode
   ```
   
   The Log Collector takes approximately six minutes to reboot in maintenance mode.
3. After the Log Collector reboots, press Enter to access the maintenance mode menu.
4. Select **Factory Reset** and press Enter.
5. Select **Factory Reset** and press Enter again.

The factory reset and subsequent reboot take approximately eight minutes in total, after which the Log Collector won’t have any configuration settings or log data. The default username and password to log in to the Log Collector is admin/admin.
Manage Log Collection

In a distributed log collection deployment, where you have Dedicated Log Collectors, if you need a firewall to send logs to Panorama instead of sending logs to the Collector Group, you must remove the firewall from the Collector Group.

When you remove the firewall from the Collector Group and commit the change, the firewall will automatically send logs to Panorama instead of sending them to a Log Collector.

To temporarily remove the log forwarding preference list on the firewall, you can delete it using the CLI on the firewall. You must however, remove the assigned firewalls in the Collector Group configuration on Panorama. Otherwise, the next time you commit changes to the Collector Group, the firewall will be reconfigured to send logs to the assigned Log Collector.

Remove a Firewall from a Collector Group

In a distributed log collection deployment, where you have Dedicated Log Collectors, if you need a firewall to send logs to Panorama instead of sending logs to the Collector Group, you must remove the firewall from the Collector Group.

When you remove the firewall from the Collector Group and commit the change, the firewall will automatically send logs to Panorama instead of sending them to a Log Collector.

To temporarily remove the log forwarding preference list on the firewall, you can delete it using the CLI on the firewall. You must however, remove the assigned firewalls in the Collector Group configuration on Panorama. Otherwise, the next time you commit changes to the Collector Group, the firewall will be reconfigured to send logs to the assigned Log Collector.

Remove a Firewall from a Collector Group

Step 1 Select Panorama > Collector Groups and select the Collector Group.

Step 2 Select Log Forwarding and, in the Log Forwarding Preferences section, select the firewall to remove from the group, click Delete, and click OK.

Step 3 Click Commit, for the Commit Type select Panorama, and click Commit again.

Step 4 Click Commit, for the Commit Type select Collector Group, select the Collector Group from which you removed the firewall, and click Commit again.
Configure Log Forwarding to Panorama

By default, firewalls store all log files locally. To aggregate logs on Panorama, you must configure the firewalls to forward logs to Panorama.

To forward firewall logs directly to external services (such as a syslog server) and also to Panorama, see Configure Log Forwarding.

For details about all the log collection deployments that Panorama supports, see Log Forwarding Options.

The PA-7000 Series firewall can’t forward logs to Panorama, only to external services. However, when you monitor logs or generate reports for a device group that includes a PA-7000 Series firewall, Panorama queries the firewall in real-time to display its log data.

If Panorama will manage firewalls running software versions earlier than PAN-OS 7.0, specify a WildFire server from which Panorama can gather analysis information for WildFire samples that those firewalls submit. Panorama uses the information to complete WildFire Submissions logs that are missing field values introduced in PAN-OS 7.0. Firewalls running earlier releases won’t populate those fields. To specify the server, select Panorama > Setup > WildFire, edit the General Settings, and enter the WildFire Private Cloud name. The default is wildfire-public-cloud, which is the WildFire cloud hosted in the United States.

### Configure Log Forwarding to Panorama

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Add a Device Group</strong> for the firewalls that will forward logs. Panorama requires a device group to push a Log Forwarding profile to firewalls. Create a new device group or assign the firewalls to an existing device group.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Add a Template</strong> for the firewalls that will forward logs. Panorama requires a template to push log settings to firewalls. Create a new template or assign the firewalls to an existing template.</td>
</tr>
</tbody>
</table>
| **Step 3** | Create a Log Forwarding profile. The profile defines the destination of Traffic, Threat, and WildFire logs. (Threat logs include URL Filtering and Data Filtering logs.)  
1. Select Objects > Log Forwarding, select the Device Group of the firewalls that will forward logs, and Add a profile.  
2. Enter a Name to identify the profile.  
3. For each log type and each severity level or WildFire verdict, select Panorama.  
4. Click OK to save the profile. |
## Configure Log Forwarding to Panorama (Continued)

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Assign the Log Forwarding profile to Security rules.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Perform the following steps for each rule that will trigger log forwarding:</td>
</tr>
<tr>
<td></td>
<td>1. Select the rulebase (for example, <strong>Policies &gt; Security &gt; Pre Rules</strong>), select the <strong>Device Group</strong> of the firewalls that will forward logs, and select the rule.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Actions</strong> tab and select the <strong>Log Forwarding</strong> profile.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Profile Type</strong> drop-down, select <strong>Profiles</strong> or <strong>Group</strong>, and then select the <strong>security profiles</strong> or <strong>Group Profile</strong> required to trigger log generation and forwarding for:</td>
</tr>
<tr>
<td></td>
<td>• Threat logs—Traffic must match any security profile assigned to the rule.</td>
</tr>
<tr>
<td></td>
<td>• WildFire logs—Traffic must match a <strong>WildFire Analysis profile</strong> assigned to the rule.</td>
</tr>
<tr>
<td></td>
<td>4. For Traffic logs, select <strong>Log At Session Start</strong> and/or <strong>Log At Session End</strong>.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>OK</strong> to save the rule.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Configure the destination of System, Config, and HIP Match logs.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>You cannot forward Correlation logs (correlated events) from the firewalls to Panorama. On the logs that are forwarded from your managed firewalls, Panorama matches for the conditions specified in the correlation objects and automatically generates correlated event(s) when a match is observed. If you want, you can then forward these correlated events (Correlation logs) from Panorama to an external syslog server.</strong></td>
</tr>
<tr>
<td></td>
<td>1. Select <strong>Device &gt; Log Settings</strong> and select the <strong>Template</strong> of the firewalls that will forward logs.</td>
</tr>
<tr>
<td></td>
<td>2. For System logs, click each Severity level, select <strong>Panorama</strong>, and click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Edit the Config and HIP Match sections, select <strong>Panorama</strong>, and click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>(M-Series appliances only) Configure Panorama to receive the logs.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. For each Log Collector that will receive logs, <strong>Configure a Managed Collector</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. <strong>Configure a Collector Group</strong>, in which you assign firewalls to specific Log Collectors for log forwarding.</td>
</tr>
</tbody>
</table>
### Configure Log Forwarding to Panorama (Continued)

**Step 7** Commit your configuration changes.

1. Click **Commit**, set the **Commit Type** to **Panorama**, and click **Commit** again.
2. Click **Commit**, set the **Commit Type** to **Device Group**, select the device group of the firewalls that will forward logs, select **Merge with Device Candidate Config** and **Include Device and Network Templates**, and click **Commit** again.
3. Click **Commit**, set the **Commit Type** to **Collector Group**, select the Collector Group you configured to receive the logs, and click **Commit** again.
4. **Verify Log Forwarding to Panorama** to confirm that your configuration is successful.

To change the log forwarding mode that the firewalls use to send logs to Panorama and to specify which Panorama HA peer can receive logs, you can **Modify Log Forwarding and Buffering Defaults**. You can also **Manage Storage Quotas and Expiration Periods for Logs and Reports**.
Verify Log Forwarding to Panorama

After you Configure Log Forwarding to Panorama, test that your configuration succeeded.

After you configure log forwarding to Log Collectors, managed firewalls open a TCP connection to all configured Log Collectors. These connections timeout every sixty (60) seconds and do not indicate that the firewall has lost connection to the Log Collectors. When you configure log forwarding to a local or Dedicated Log Collectors over an ethernet interface, the firewall traffic logs show incomplete sessions despite the firewall being able to successfully connect to the Log Collectors. If you configure log forwarding over the management port, no traffic logs showing incomplete sessions are generated. Traffic logs showing incomplete sessions are generated by all firewalls except for the PA-5200 and PA-7000 series firewalls.

### Verify Log Forwarding to Panorama

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Access the firewall CLI.</td>
</tr>
</tbody>
</table>
| 2      | If you configured Log Collectors, verify that each firewall has a log forwarding preference list.  
> `show log-collector preference-list`  
If the Collector Group has only one Log Collector, the output will look something like this:  
Log collector Preference List  
Serial Number: 003001000024  
IP Address: 10.2.133.48 |
| 3      | Verify that each firewall is forwarding logs.  
> `show logging-status device <firewall-serial-number>`  
For successful forwarding, the output indicates that the log forwarding agent is active. For a Panorama virtual appliance, the agent is Panorama. For an M-Series appliance, the agent is a Log Collector. |
| 4      | View the average logging rate. The displayed rate will be the average logs/second for the last five minutes.  
- If Log Collectors receive the logs, access the Panorama web interface, select Panorama > Managed Collectors and click the Statistics link in the far-right column.  
- If a Panorama virtual appliance receives the logs, access the Panorama CLI and run the following command:  
`debug log-collector log-collection-stats show incoming-logs`  
This command also works on an M-Series appliance. |
Modify Log Forwarding and Buffering Defaults

You can define the log forwarding mode that the firewalls use to send logs to Panorama and, when configured in a high availability (HA) configuration, specify which Panorama peer can receive logs. To access these options, select Panorama > Setup > Management, edit the Logging and Reporting Settings, and select the Log Export and Reporting tab.

- Define the log forwarding mode on the firewall: The firewalls can forward logs to Panorama (pertains to both the M-Series appliance and the Panorama virtual appliance) in either Buffered Log Forwarding mode or in the Live Mode Log Forwarding mode.

<table>
<thead>
<tr>
<th>Logging Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffered Log Forwarding from Device</td>
<td>Default: Enabled</td>
</tr>
<tr>
<td></td>
<td>It is a best practice to select the Buffered Log Forwarding from Device option.</td>
</tr>
<tr>
<td></td>
<td>Allows each managed firewall to buffer logs and send the logs at 30-second intervals to Panorama (not user configurable). Buffered log forwarding is very valuable when the firewall loses connectivity to Panorama. The firewall buffers log entries to its local hard disk and keeps a pointer to record the last log entry that was sent to Panorama. When connectivity is restored the firewall resumes forwarding logs from where it left off. The disk space available for buffering depends on the log storage quota for the firewall model and the volume of logs that are pending rollover. If the firewall was disconnected for a long time and the last log forwarded was rolled over, all the logs from its local hard disk will be forwarded to Panorama on reconnection. If the available space on the local hard disk of the firewall is consumed, the oldest entries are deleted to allow logging of new events.</td>
</tr>
</tbody>
</table>

| Live Mode Log Forwarding from Device | In live mode, the managed firewall sends every log transaction to Panorama at the same time as it records it on the firewall. |

- Define log forwarding preference on a Panorama virtual appliance that is in a high availability (HA) configuration:
  - When logging to a virtual disk, enable logging to the local disk on the active-primary Panorama peer only. By default, both Panorama peers in the HA configuration receive logs.
  - When logging to an NFS, enable the firewalls to send only newly generated logs to a secondary Panorama peer, which is promoted to primary, after a failover.

<table>
<thead>
<tr>
<th>Logging Options</th>
<th>Pertains to</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only Active Primary Logs to Local Disk</td>
<td>Panorama virtual appliance that is logging to a virtual disk and is set up in a high availability (HA) configuration.</td>
<td>Allows you to configure only the active-primary Panorama peer to save logs to the local disk.</td>
</tr>
<tr>
<td>Default: Disabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Get Only New Logs on Convert to Primary
Default: Disabled

<table>
<thead>
<tr>
<th>Logging Options</th>
<th>Pertains to</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get Only New Logs on Convert to Primary</td>
<td>Panorama virtual appliance that is mounted to a Network File System (NFS) datastore and is set up in a high availability (HA) configuration</td>
<td>With NFS logging, when you have a pair of Panorama servers configured in a high availability configuration, only the primary Panorama peer mounts the NFS datastore. Therefore, the firewalls can only send logs to the primary Panorama peer, which can write to the NFS datastore. When an HA failover occurs, the <strong>Get Only New Logs on Convert to Primary</strong> option allows an administrator to configure the managed firewalls to send only newly generated logs to Panorama. This event is triggered when the priority of the active-secondary Panorama is promoted to primary and it can begin logging to the NFS. This behavior is typically enabled to prevent the firewalls from sending a large volume of buffered logs when connectivity to Panorama is restored after a significant period of time.</td>
</tr>
</tbody>
</table>
Configure Log Forwarding from Panorama to External Destinations

Panorama enables you to forward logs to external servers, including syslog, email, and SNMP trap servers. Forwarding firewall logs from Panorama reduces the load on the firewalls and provides a reliable and streamlined approach to forwarding logs to remote destinations. You can also forward logs that Panorama and its managed collectors generate.

To forward firewall logs directly to external services and also to Panorama, see Configure Log Forwarding. For details about all the log collection deployments that Panorama supports, see Log Forwarding Options.

On a Panorama virtual appliance running Panorama 5.1 or earlier releases, you can use Secure Copy (SCP) commands from the CLI to export the entire log database to an SCP server and import it to another Panorama virtual appliance. A Panorama virtual appliance running Panorama 6.0 or later releases, and M-Series appliances running any release, do not support these options because the log database on those appliances is too large for an export or import to be practical.

### Configure Log Forwarding from Panorama to External Destinations

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Configure the firewalls to forward logs to Panorama.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Configure a server profile for each external service that will receive log data.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure destinations for:</td>
</tr>
<tr>
<td></td>
<td>• Firewall logs that a Panorama virtual appliance collects.</td>
</tr>
<tr>
<td></td>
<td>• Logs that Panorama (a virtual appliance or M-Series appliance) and managed collectors generate.</td>
</tr>
</tbody>
</table>

1. Select **Panorama > Server Profiles** and select the type of server that will receive the log data: **SNMP Trap**, **Syslog**, or **Email**.
2. Configure the server profile. Optionally, you can configure separate profiles for different log types and severity levels or WildFire verdicts.
   - **Configure an SNMP Trap server profile.** For details on how Simple Network Management Protocol (SNMP) works for Panorama and Log Collectors, refer to SNMP Support.
   - **Configure a Syslog server profile.** If the syslog server requires client authentication, use the **Panorama > Certificate Management > Certificates** page to create a certificate for securing syslog communication over SSL.
   - **Configure an Email server profile.**

1. Select **Panorama > Log Settings**.
2. For System, Correlation, and Threat logs, click each Severity level, select the **SNMP Trap**, **Email**, or **Syslog** server profile you just created, and click **OK**.
3. For WildFire logs, click each Verdict, select the **SNMP Trap**, **Email**, or **Syslog** server profile you just created, and click **OK**.
4. For Config, HIP Match, and Traffic logs, edit the corresponding section, select the **SNMP Trap**, **Email**, or **Syslog** server profile you just created, and click **OK**.
### Configure Log Forwarding from Panorama to External Destinations (Continued)

#### Step 4  
**(M-Series appliance only)** Configure destinations for firewall logs that an M-Series appliance in Panorama or Log Collector mode collects. Each Collector Group can forward logs to different destinations. If the Log Collectors are local to a high availability (HA) pair of M-Series appliances in Panorama mode, you must log into each HA peer to configure log forwarding for its Collector Group.

1. Select **Panorama > Collector Groups** and select the Collector Group that receives the firewall logs.
2. **(SNMP trap forwarding only)** Select the Monitoring tab and configure the settings.
3. Select the **Collector Log Forwarding** tab.
4. For each log Severity level in the System, Threat, and Correlation tabs, click a cell in the SNMP Trap, Email Profile, or Syslog Profile column, and select the server profile you just created.
5. In the Config, HIP Match, and Traffic tabs, select the SNMP Trap, Email, or Syslog server profile you just created.
6. For each Verdict in the WildFire tab, click a cell in the SNMP Trap, Email Profile, or Syslog Profile column, and select the server profile you just created.
7. Click **OK** to save your changes to the Collector Group.

#### Step 5  
**(Syslog forwarding only)** If the syslog server requires client authentication and the firewalls forward logs to Dedicated Log Collectors, assign a certificate that secures syslog communication over SSL.

Perform the following steps for each Dedicated Log Collector:

1. Select **Panorama > Managed Collectors** and select the Log Collector.
2. In the **General** tab, select the Certificate for Secure Syslog and click **OK**.

#### Step 6  
**(SNMP trap forwarding only)** Enable your SNMP manager to interpret traps.

Load the Supported MIBs and, if necessary, compile them. For the specific steps, refer to the documentation of your SNMP manager.

#### Step 7  
Commit your configuration changes.

1. Click **Commit**, set the Commit Type to Panorama, and click **Commit** again.
2. Click **Commit**, set the Commit Type to Device Group, select all the device groups of the firewalls from which Panorama collects logs, Include Device and Network Templates, and click **Commit** again.
3. **(M-Series appliance only)** Click **Commit**, set the Commit Type to Collector Group, select the Collector Group you just configured to forward logs, and click **Commit** again.

#### Step 8  
Verify the external services are receiving logs from Panorama.

- Email server—Verify that the specified recipients are receiving logs as email notifications.
- Syslog server—Refer to the documentation for your syslog server to verify it is receiving logs as syslog messages.
- SNMP manager—Use an SNMP Manager to Explore MIBs and Objects to verify it is receiving logs as SNMP traps.
Log Collection Deployments

The following topics describe how to configure log collection in the most typical deployments.

- Plan a Log Collection Deployment
- Deploy Panorama with Dedicated Log Collectors
- Deploy Panorama with Default Log Collectors
- Deploy Panorama Virtual Appliances with Local Log Collection

Plan a Log Collection Deployment

- Panorama and Log Collectors
- Collector Groups with Single or Multiple Log Collectors
- Log Forwarding Options

Panorama and Log Collectors

Decide which Panorama Platforms to use for the Panorama management server and Log Collectors based on the geographic distribution of managed firewalls, logging rate, and log retention requirements.

If you initially implement log collection using the default Log Collectors but later require more storage or higher logging rates than these support, you can switch to a deployment with Dedicated Log Collectors (M-Series appliances in Log Collector mode). You can also implement a hybrid deployment that includes both default and Dedicated Log Collectors. However, if you initially implement log collection using Dedicated Log Collectors, you will lose logs if you later switch to a deployment that involves only the default Log Collectors because of the reduced storage capacity.

If you deploy firewalls remotely, consider the bandwidth requirement for the connection between the firewalls and Panorama, in addition to whether Panorama supports the required logging rate. Deploying Dedicated Log Collectors close to the firewalls can increase the bandwidth for log forwarding.

The following table summarizes your choice of Log Collector when considering the rate at which it receives firewall logs.
Manage Log Collection

Collector Groups with Single or Multiple Log Collectors

You can configure a Collector Group with multiple Log Collectors to ensure log redundancy, increase the log retention period, or accommodate logging rates that exceed the capacity of a single Log Collector (see Panorama Platforms for capacity information). To understand the requirements, risks and recommended mitigations, see Caveats for a Collector Group with Multiple Log Collectors.

All the Log Collectors in any particular Collector Group must be the same models, such as all M-500 appliances or all M-100 appliances. Log redundancy is available only if each Log Collector has the same number of logging disks.

Log Forwarding Options

By default, each firewall stores its log files locally. To use Panorama for centralized log monitoring and report generation, you must Configure Log Forwarding to Panorama. You can also Configure Log Forwarding from Panorama to External Destinations for archiving, notification, or analysis. When forwarding from Panorama, you can include the System and Config logs that Panorama and its Log Collectors generate. External services include syslog servers, email servers, or SNMP trap servers. The firewall, Panorama virtual appliance, or M-Series appliance that forwards the logs to external services converts the logs to the appropriate format (syslog message, email notification, or SNMP trap).

Palo Alto Networks firewalls and Panorama support the following log forwarding options:

- Forward logs from firewalls to Panorama and from Panorama to external services—This configuration is best for deployments in which the connections between firewalls and external services have insufficient bandwidth to sustain the logging rate, which is often the case when the connections are remote. This configuration improves firewall performance by offloading some processing to Panorama.

You can configure each Collector Group to forward logs to different destinations.
Log Collection Deployments

Manage Log Collection

Figure: Log Forwarding to Panorama and then to External Services

- Forward logs from firewalls to Panorama and to external services in parallel—In this configuration, both Panorama and the external services are endpoints of separate log forwarding flows; the firewalls don’t rely on Panorama to forward logs to external services. This configuration is best for deployments in which the connections between firewalls and external services have sufficient bandwidth to sustain the logging rate, which is often the case when the connections are local.

Figure: Log Forwarding to External Services and Panorama in Parallel

- Forward logs from firewalls directly to external services and also from Panorama to external services—This configuration is a hybrid of the previous two and is best for deployments that require sending syslog messages to multiple Security Information and Event Management (SIEM) solutions, each with its own message format (for example, Splunk and ArcSight). This duplicate forwarding doesn’t apply to SNMP traps or email notifications.

Deploy Panorama with Dedicated Log Collectors

The following figures illustrate Panorama in a Distributed Log Collection Deployment. In these examples, the Panorama management server comprises two M-Series appliances in Panorama mode that are deployed in an active/passive high availability (HA) configuration. Alternatively, you can use an HA pair of Panorama
virtual appliances. The firewalls send logs to Dedicated Log Collectors (M-Series appliances in Log Collector mode). This is the recommended configuration if the firewalls generate over 10,000 logs/second. (For details on deployment options, see Plan a Log Collection Deployment.)

If you will assign more than one Log Collector to a Collector Group, see Caveats for a Collector Group with Multiple Log Collectors to understand the requirements, risks, and recommended mitigations.

Figure: Single Dedicated Log Collector Per Collector Group

Figure: Multiple Dedicated Log Collectors Per Collector Group
Perform the following steps to deploy Panorama with Dedicated Log Collectors. Skip any steps you have already performed (such as the initial setup).

<table>
<thead>
<tr>
<th>Deploy Panorama with Dedicated Log Collectors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Perform the initial setup of the Panorama management server (virtual appliances or M-Series appliances) and the Dedicated Log Collectors.</td>
</tr>
<tr>
<td><strong>For each M-Series appliance:</strong></td>
</tr>
<tr>
<td>1. Rack mount the M-Series appliance. Refer to the M-100 or M-500 Hardware Reference Guide for instructions.</td>
</tr>
<tr>
<td>2. Perform Initial Configuration of the M-Series Appliance. To reduce the traffic load on the management (MGT) interface and to improve security for management traffic, Palo Alto Networks recommends configuring Panorama to use the Eth1 and Eth2 interfaces for log collection and Collector Group communication. You define these interfaces during initial configuration of the Panorama management server.</td>
</tr>
<tr>
<td>3. Configure each array. This task is required to make the RAID disks available for logging. Optionally, you can add disks to Increase Storage on the M-Series Appliance.</td>
</tr>
<tr>
<td>4. Register Panorama and Install Licenses.</td>
</tr>
<tr>
<td>5. Install Content and Software Updates for Panorama.</td>
</tr>
</tbody>
</table>
### Deploy Panorama with Dedicated Log Collectors (Continued)

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Switch from Panorama mode to Log Collector mode on each M-Series appliance that will be a Dedicated Log Collector.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Switching the mode of an M-Series appliance deletes any existing log data and deletes all configurations except the management access settings. After the switch, the M-Series appliance retains CLI access but loses web interface access.</td>
</tr>
<tr>
<td>1.</td>
<td>Connect to the M-Series appliance in one of the following ways:</td>
</tr>
<tr>
<td></td>
<td>• Attach a serial cable from your computer to the Console port on the M-Series appliance. Then use terminal emulation software (9600-8-N-1) to connect.</td>
</tr>
<tr>
<td></td>
<td>• Use terminal emulation software such as PuTTY to open an SSH session to the IP address that you specified for the MGT interface of the M-Series appliance during initial configuration.</td>
</tr>
<tr>
<td>2.</td>
<td>Log in to the CLI when prompted. Use the default admin account and the password that you specified during initial configuration.</td>
</tr>
<tr>
<td>3.</td>
<td>Switch to Log Collector mode by entering the following command:</td>
</tr>
<tr>
<td></td>
<td>&gt; request system system-mode logger</td>
</tr>
<tr>
<td>4.</td>
<td>Enter <code>Y</code> to confirm the mode change. The M-Series appliance reboots. If the reboot process terminates your terminal emulation software session, reconnect to the M-Series appliance to see the Panorama login prompt.</td>
</tr>
<tr>
<td></td>
<td>If you see a CMS Login prompt, this means the Log Collector has not finished rebooting. Press Enter at the prompt without typing a username or password.</td>
</tr>
<tr>
<td>5.</td>
<td>Log back in to the CLI.</td>
</tr>
<tr>
<td>6.</td>
<td>Verify that the switch to Log Collector mode succeeded:</td>
</tr>
<tr>
<td></td>
<td>&gt; show system info</td>
</tr>
<tr>
<td></td>
<td>If the mode change succeeded, the output displays:</td>
</tr>
<tr>
<td></td>
<td>system-mode: logger</td>
</tr>
</tbody>
</table>

| Step 3 | Record the serial number of each Log Collector. |
|        | You need the serial numbers to add the Log Collectors as managed collectors on the Panorama management server. |
| 1.    | At the CLI of each Log Collector, enter the following command to display its serial number. |
|       |   > show system info | match serial |
| 2.    | Record the serial number. |
### Log Collection Deployments

#### Manage Log Collection

**Deploy Panorama with Dedicated Log Collectors (Continued)**

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Add each Log Collector as a managed collector.</th>
<th>Use the web interface of the primary Panorama management server peer to <strong>Configure a Managed Collector:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1. Select Panorama &gt; Managed Collectors and Add the managed collector.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. In the General tab, enter the serial number (Collector S/N) you recorded for the Log Collector.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the IP address or FQDN of the active and passive Panorama HA peers in the Panorama Server IP field and Panorama Server IP 2 field respectively. These fields are required.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Select Management and configure one or both of the following field sets for the MGT interface based on the IP protocols of your network.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- IPv4—IP Address, Netmask, and Default Gateway</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- IPv6—IPv6 Address/Prefix Length and Default IPv6 Gateway</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. (Optional) In the Management Interface Services section, select SNMP if you will use an SNMP manager to monitor Log Collector statistics.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Using SNMP requires additional steps besides configuring the Log Collector (see Monitor Panorama and Log Collector Statistics Using SNMP).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. Click OK and Commit, set the Commit Type to Panorama, and click Commit again. This step is required before you can enable logging disks on the Log Collectors.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. Verify that the Panorama &gt; Managed Collectors page lists the Log Collector you added. The Connected column displays a check mark to indicate that the Log Collector is connected to Panorama. You might have to wait a few minutes before the page displays the updated connection status.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>At this point, the Configuration Status column displays Out of Sync and the Run Time Status column displays disconnected. The status will change to In Sync and connected after you configure a Collector Group later in this procedure.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Enable connectivity between each Log Collector and the Panorama management server. This step is required before you can enable logging disks on the Log Collectors.</th>
<th>Enter the following commands at the CLI of each Log Collector.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This step is required before you can enable logging disks on the Log Collectors.</td>
<td>&lt;IPaddress1&gt; is for the MGT interface of the active Panorama and &lt;IPaddress2&gt; is for the MGT interface of the passive Panorama.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&gt; configure</td>
</tr>
<tr>
<td></td>
<td></td>
<td># set deviceconfig system panorama-server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;IPaddress1&gt; panorama-server-2 &lt;IPaddress2&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td># commit</td>
</tr>
<tr>
<td></td>
<td></td>
<td># exit</td>
</tr>
</tbody>
</table>

© Palo Alto Networks, Inc.
### Deploy Panorama with Dedicated Log Collectors (Continued)

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Enable the logging disks on each Log Collector.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Use the web interface of the primary Panorama management server peer to perform these steps:</td>
</tr>
<tr>
<td></td>
<td>1. Select <strong>Panorama &gt; Managed Collectors</strong> and edit the Log Collector.</td>
</tr>
<tr>
<td></td>
<td>2. Select <strong>Disks</strong> and <strong>Add</strong> each disk pair.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>OK</strong> and <strong>Commit</strong>, set the <strong>Commit Type</strong> to <strong>Panorama</strong>, and click <strong>Commit</strong> again.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>(Optional) Configure the Eth1 and/or Eth2 interfaces if the Log Collectors will use them for log collection and Collector Group communication. These interfaces are available only if you configured them for the Panorama management server during initial configuration. Palo Alto Networks recommends using Eth1 and/or Eth2 to reduce the traffic load on the MGT interface and to improve security for management traffic.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Use the web interface of the primary Panorama management server peer to perform these steps for each Log Collector:</td>
</tr>
<tr>
<td></td>
<td>1. Select <strong>Panorama &gt; Managed Collectors</strong> and edit the Log Collector.</td>
</tr>
<tr>
<td></td>
<td>2. Configure the network settings of the Eth1 and/or Eth2 interfaces. For each interface, select the corresponding tab and configure one or both of the following field sets based on the IP protocols of your network.</td>
</tr>
<tr>
<td></td>
<td>- IPv4—<strong>IP Address</strong>, <strong>Netmask</strong>, and <strong>Default Gateway</strong></td>
</tr>
<tr>
<td></td>
<td>- IPv6—<strong>IPv6 Address/Prefix Length</strong> and <strong>Default IPv6 Gateway</strong></td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>OK</strong> and <strong>Commit</strong>, set the <strong>Commit Type</strong> to <strong>Panorama</strong>, and click <strong>Commit</strong> again. This step is required before you can assign the Eth1 and Eth2 interfaces to logging functions.</td>
</tr>
<tr>
<td></td>
<td>4. Select <strong>Panorama &gt; Managed Collectors</strong> and edit the Log Collector.</td>
</tr>
<tr>
<td></td>
<td>5. Select the interfaces (MGT, Eth1, or Eth2) that the Log Collector will use for <strong>Device Log Collection</strong> and <strong>Collector Group Communication</strong> (default is MGT).</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>OK</strong> to save your changes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Add a Firewall as a Managed Device.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Use the web interface of the primary Panorama management server peer to perform this task for each firewall that will forward logs to Log Collectors.</td>
</tr>
</tbody>
</table>
**Deploy Panorama with Dedicated Log Collectors (Continued)**

**Step 9** Configure a Collector Group.
If each Collector Group will have one Log Collector, repeat this step for each Collector Group before continuing. If you will assign all the Log Collectors to one Collector Group, perform this step only once.

<table>
<thead>
<tr>
<th>Use the web interface of the primary Panorama management server peer to <strong>Configure a Collector Group:</strong></th>
</tr>
</thead>
</table>
| 1. Select **Panorama > Collector Groups, Add** a Collector Group, and enter a **Name** for it.  
   If you add multiple Log Collectors to a single Collector group, **Enable log redundancy across collectors** as a best practice. For redundancy, each Log Collector in the Collector Group requires the same number of disks.  |
| 2. *(Optional)* Select the **Monitoring** tab and configure the settings if you will use SNMP to monitor Log Collector statistics and traps.  |
| 3. Select the **Device Log Forwarding** tab and, in the Collector Group Members section, assign one or more Log Collectors.  
   All the Log Collectors for any particular Collector Group must be the same models, such as all M-100 appliances or all M-500 appliances.  |
| 4. In the Log Forwarding Preferences section, assign firewalls according to the number of Log Collectors in this Collector Group:  
   - Single—Assign the firewalls that will forward logs to that Log Collector, as illustrated in **Figure: Single Dedicated Log Collector Per Collector Group.**  
   - Multiple—Assign each firewall to both Log Collectors for redundancy. When you configure the preferences, make Log Collector 1 the first priority for half the firewalls and make Log Collector 2 the first priority for the other half, as illustrated in **Figure: Multiple Dedicated Log Collectors Per Collector Group.**  |
| 5. Click **OK** and **Commit**, set the **Commit Type** to **Panorama**, and click **Commit** again.  |
| 6. Click **Commit**, set the **Commit Type** to **Collector Group**, select the Collector Groups you added, and click **Commit** again.  |
| 7. Select **Panorama > Managed Collectors** to verify that the Log Collector configuration is synchronized with Panorama.  
   The Configuration Status column should display In Sync and the Run Time Status column should display connected.  |

**Step 10** Configure log forwarding.

| Use the web interface of the primary Panorama management server peer to:  
| 1. **Configure Log Forwarding to Panorama.**  
| 2. **Verify Log Forwarding to Panorama.**  
| 3. *(Optional)* **Configure Log Forwarding from Panorama to External Destinations.** |
Deploy Panorama with Default Log Collectors

The following figures illustrate Panorama in a centralized log collection deployment. In these examples, the Panorama management server comprises two M-Series appliances in Panorama mode that are deployed in an active/passive high availability (HA) configuration. The firewalls send logs to the predefined (default) local Log Collector on each Panorama M-Series appliance. This is the recommended deployment if the firewalls generate up to 10,000 logs/second. (For details on deployment options, see Plan a Log Collection Deployment.)

If you will assign more than one Log Collector to a Collector Group, see Caveats for a Collector Group with Multiple Log Collectors to understand the requirements, risks, and recommended mitigations.

After implementing this deployment, if the logging rate increases beyond 10,000 logs per second, Palo Alto Networks recommends that you add Dedicated Log Collectors (M-Series appliances in Log Collector mode) as described in Deploy Panorama with Dedicated Log Collectors. Such an expansion might require reassigning firewalls from the default Log Collectors to Dedicated Log Collectors.

Figure: Single Default Log Collector Per Collector Group

Figure: Multiple Default Log Collectors Per Collector Group
Perform the following steps to deploy Panorama with default Log Collectors. Skip any steps you have already performed (such as the initial setup).

<table>
<thead>
<tr>
<th>Deploy Panorama with Default Log Collectors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Perform the initial setup of each M-Series appliance.</td>
</tr>
<tr>
<td>1. Rack mount the M-Series appliance. Refer to the M-100 or M-500 Hardware Reference Guide for instructions.</td>
</tr>
<tr>
<td>2. <strong>Perform Initial Configuration of the M-Series Appliance.</strong> To reduce the traffic load on the management (MGT) interface and to improve security for management traffic, Palo Alto Networks recommends configuring Panorama to use the Eth1 and Eth2 interfaces for log collection and Collector Group communication.</td>
</tr>
<tr>
<td>3. <strong>Configure each array.</strong> This task is required to make the RAID disks available for logging. Optionally, you can add disks to Increase Storage on the M-Series Appliance.</td>
</tr>
<tr>
<td>4. <strong>Register Panorama and Install Licenses.</strong></td>
</tr>
<tr>
<td>5. <strong>Install Content and Software Updates for Panorama.</strong></td>
</tr>
<tr>
<td>6. <strong>Set Up HA on Panorama.</strong></td>
</tr>
</tbody>
</table>
Manage Log Collection

Deploy Panorama with Default Log Collectors (Continued)

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Perform the following steps to prepare Panorama for log collection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Connect to the primary Panorama in one of the following ways:</td>
</tr>
<tr>
<td></td>
<td>• Attach a serial cable from your computer to the Console</td>
</tr>
<tr>
<td></td>
<td>port on the primary Panorama. Then use terminal emulation</td>
</tr>
<tr>
<td></td>
<td>software (9600-8-N-1) to connect.</td>
</tr>
<tr>
<td></td>
<td>• Use terminal emulation software such as PuTTY to open an</td>
</tr>
<tr>
<td></td>
<td>SSH session to the IP address that you specified for the</td>
</tr>
<tr>
<td></td>
<td>MGT interface of the primary Panorama during initial</td>
</tr>
<tr>
<td></td>
<td>configuration.</td>
</tr>
<tr>
<td>2.</td>
<td>Log in to the CLI when prompted. Use the default admin</td>
</tr>
<tr>
<td></td>
<td>account and the password that you specified during initial</td>
</tr>
<tr>
<td></td>
<td>configuration.</td>
</tr>
<tr>
<td>3.</td>
<td>Enable the primary Panorama to connect to the secondary</td>
</tr>
<tr>
<td></td>
<td>Panorama by entering the following command, where &lt;IPAddress2&gt;</td>
</tr>
<tr>
<td></td>
<td>represents the MGT interface of the secondary Panorama:</td>
</tr>
<tr>
<td></td>
<td>&gt; configure</td>
</tr>
<tr>
<td></td>
<td># set deviceconfig system panorama-server &lt;IPAddress2&gt;</td>
</tr>
<tr>
<td></td>
<td># commit</td>
</tr>
<tr>
<td></td>
<td># commit</td>
</tr>
<tr>
<td>4.</td>
<td>Log in to the CLI of the secondary Panorama.</td>
</tr>
<tr>
<td>5.</td>
<td>Enable the secondary Panorama to connect to the primary Panorama</td>
</tr>
<tr>
<td></td>
<td>by entering the following command, where &lt;IPAddress1&gt; represents</td>
</tr>
<tr>
<td></td>
<td>the MGT interface of the primary Panorama:</td>
</tr>
<tr>
<td></td>
<td>&gt; configure</td>
</tr>
<tr>
<td></td>
<td># set deviceconfig system panorama-server &lt;IPAddress1&gt;</td>
</tr>
<tr>
<td></td>
<td># commit</td>
</tr>
<tr>
<td></td>
<td># exit</td>
</tr>
<tr>
<td>6.</td>
<td>In the CLI of the secondary Panorama, enter the following command</td>
</tr>
<tr>
<td></td>
<td>to display the serial number, and then record it:</td>
</tr>
<tr>
<td></td>
<td>&gt; show system info</td>
</tr>
<tr>
<td></td>
<td>You need the serial number to add the Log Collector of the</td>
</tr>
<tr>
<td></td>
<td>secondary Panorama as a managed collector to the primary</td>
</tr>
<tr>
<td></td>
<td>Panorama.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Edit the Log Collector that is local to the primary Panorama.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Use the web interface of the primary Panorama to perform these</td>
</tr>
<tr>
<td></td>
<td>steps:</td>
</tr>
<tr>
<td></td>
<td>1. Select Panorama &gt; Managed Collectors and select the</td>
</tr>
<tr>
<td></td>
<td>default Log Collector.</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional) Select the interfaces (MGT, Eth1, or Eth2) to use for</td>
</tr>
<tr>
<td></td>
<td>Device Log Collection and Collector Group Communication.</td>
</tr>
<tr>
<td></td>
<td>By default, Panorama uses the MGT interface for these</td>
</tr>
<tr>
<td></td>
<td>functions.</td>
</tr>
<tr>
<td></td>
<td>The Eth1 and Eth2 interfaces are available only if you</td>
</tr>
<tr>
<td></td>
<td>configured them for the Panorama management server during</td>
</tr>
<tr>
<td></td>
<td>initial configuration.</td>
</tr>
<tr>
<td>3.</td>
<td>Select Disks and Add each logging disk pair.</td>
</tr>
<tr>
<td>4.</td>
<td>Click OK to save your changes.</td>
</tr>
</tbody>
</table>

© Palo Alto Networks, Inc.
Step 4 Configure the Log Collector that is local to the secondary Panorama.

Panorama treats this Log Collector as remote because it’s not local to the primary Panorama. Therefore you must manually add it on the primary Panorama.

Use the web interface of the primary Panorama to Configure a Managed Collector:

1. Select Panorama > Managed Collectors and Add the Log Collector.
2. Enter the serial number (Collector S/N) you recorded for the Log Collector of the secondary Panorama.
3. Enter the IP address or FQDN of the primary and secondary Panorama HA peers in the Panorama Server IP field and Panorama Server IP 2 field respectively. These fields are required.
4. Configure the network settings of each interface that the Log Collector will use. The Management interface is required. If you configured the Panorama management server to use the Eth1 and Eth2 interfaces, configure these interfaces on the Log Collector also.
   For each interface, select the corresponding tab and configure one or both of the following field sets based on the IP protocols of your network.
   - IPv4—IP Address, Netmask, and Default Gateway
   - IPv6—IPv6 Address/Prefix Length and Default IPv6 Gateway
5. (Optional) For the Management interface, select SNMP if you will use an SNMP manager to monitor Log Collector statistics. Using SNMP requires additional steps besides configuring the Log Collector (see Monitor Panorama and Log Collector Statistics Using SNMP).
6. Click OK and Commit, set the Commit Type to Panorama, and click Commit again. This step is required before you can enable logging disks or assign the Eth1 and Eth2 interfaces to logging functions.
7. (Optional) Select Panorama > Managed Collectors, edit the Log Collector, and select the interfaces (MGT, Eth1, or Eth2) that it will use for Device Log Collection and Collector Group Communication (default is MGT).
8. Select Disks and Add each logging disk pair.
9. Click OK and Commit, set the Commit Type to Panorama, and click Commit again.

Step 5 Add a Firewall as a Managed Device.

Use the web interface of the primary Panorama to perform this task for each firewall that will forward logs to the Log Collectors.
### Deploy Panorama with Default Log Collectors (Continued)

**Step 6** Edit the default Collector Group that is predefined on the primary Panorama.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select <strong>Panorama &gt; Collector Groups</strong> and select the <strong>default</strong> Collector Group. If you add multiple Log Collectors to a single Collector group, <strong>Enable log redundancy across collectors</strong> as a best practice.</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional) Select the <strong>Monitoring</strong> tab and configure the settings if you will use SNMP to monitor Log Collector statistics and traps.</td>
</tr>
<tr>
<td>3.</td>
<td>Select <strong>Device Log Forwarding</strong>. The Collector Group Members section displays the local Log Collector of the primary Panorama because it is pre-assigned to the default Collector Group. Optionally, <strong>Add</strong> the local Log Collector of the secondary Panorama.</td>
</tr>
</tbody>
</table>
| 4.   | In the Log Forwarding Preferences section, assign firewalls according to the number of Log Collectors in this Collector Group:  
  * Single—Assign the firewalls that will forward logs to the default Log Collector of the primary Panorama, as illustrated in Figure: Single Default Log Collector Per Collector Group.  
  * Multiple—Assign each firewall to both Log Collectors for redundancy. When you configure the preferences, make Log Collector 1 the first priority for half the firewalls and make Log Collector 2 the first priority for the other half, as illustrated in Figure: Multiple Default Log Collectors Per Collector Group. |
| 5.   | Click **OK** to save your changes. |

**Step 7** Configure a Collector Group that contains the Log Collector of the secondary Panorama. Required if each Collector Group has only one Log Collector.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | Use the web interface of the primary Panorama to **Configure a Collector Group**:  
  * Select **Panorama > Collector Groups** and **Add** the Collector Group.  
  * Enter a **Name** to identify the Collector Group.  
  * (Optional) Select the **Monitoring** tab and configure the settings if you will use an SNMP manager to monitor Log Collector statistics and traps.  
  * Select the **Device Log Forwarding** tab and, in the Collector Group Members section, **Add** the default Log Collector of the secondary Panorama.  
  * In the Log Forwarding Preferences section, assign the firewalls that will forward logs to the default Log Collector of the secondary Panorama, as illustrated in Figure: Single Default Log Collector Per Collector Group.  
  * Click **OK** to save your changes. |
| Step 8  | Commit your changes. | Use the web interface of the primary Panorama to perform the following steps:  
1. Click **Commit**, set the **Commit Type** to **Panorama**, and click **Commit** again.  
2. Click **Commit**, set the **Commit Type** to **Collector Group**, select the Collector Groups you added, and click **Commit** again. |
| Step 9 | Manually fail over so that the secondary Panorama becomes active. | Use the web interface of the primary Panorama to perform the following steps:  
1. Select **Panorama > High Availability**.  
2. Click **Suspend local Panorama** in the Operational Commands section. |
| Step 10 | On the secondary Panorama, configure the network settings of the Log Collector that is local to the primary Panorama. | Use the web interface of the secondary Panorama to perform the following steps:  
1. In the Panorama web interface, select **Panorama > Managed Collectors** and select the Log Collector that is local to the primary Panorama.  
2. Enter the IP address or FQDN of the secondary Panorama in the **Panorama Server IP** field and the IP address or FQDN of the primary Panorama in the **Panorama Server IP 2** field. These fields are required.  
3. Select the **Management** tab and complete one or both of the following field sets (based on the IP protocols of your network) with the management interface values of the primary Panorama:  
   - IPv4—**IP Address**, **Netmask**, and **Default Gateway**  
   - IPv6—**IPv6 Address/Prefix Length** and **Default IPv6 Gateway**  
4. Click **OK** and **Commit**, set the **Commit Type** to **Panorama**, and click **Commit** again. Wait until the HA synchronization finishes before proceeding.  
5. Click **Commit**, set the **Commit Type** to **Collector Group**, select the Collector Groups you added, and click **Commit** again. |
| Step 11 | Manually fail back so that the primary Panorama becomes active. | Use the web interface of the secondary Panorama to perform the following steps:  
1. Select **Panorama > High Availability**.  
2. Click **Suspend local Panorama** in the Operational Commands section. |
Deploy Panorama with Default Log Collectors (Continued)

**Step 12** Configure log forwarding.

Use the web interface of the primary Panorama to:

1. Configure Log Forwarding to Panorama.
2. Verify Log Forwarding to Panorama.
3. *(Optional)* Configure Log Forwarding from Panorama to External Destinations.

You can configure separate external server profiles for different log types and severity levels. You can also assign separate profiles to each Panorama HA peer. For example, you might want each peer to forward logs to a different syslog server. To make each Panorama peer forward logs to different external services, log in to the web interface of each peer, select **Panorama > Collector Groups**, select the Collector Group, select **Collector Log Forwarding**, assign the server profiles, and click **OK**.

---

**Deploy Panorama Virtual Appliances with Local Log Collection**

The following figure illustrates Panorama in a centralized log collection deployment. In this example, the Panorama management server comprises two Panorama virtual appliances that are deployed in an active/passive high availability (HA) configuration. This configuration suits firewall management within a VMware virtual infrastructure in which Panorama processes up to 10,000 logs/second. (For details on deployment options, see **Plan a Log Collection Deployment**.) The firewalls send logs to the Panorama management server (to its virtual disk or Network File System [NFS] datastore). By default, the active and passive peers both receive logs, though you can modify log forwarding and buffering defaults so that only the active peer does. By default, the Panorama virtual appliance uses approximately 11GB on its internal disk partition for log storage, though you can expand log storage capacity on the Panorama Virtual Appliance if necessary.

If the logging rate increases beyond 10,000 logs per second, it is recommended that you add Dedicated Log Collectors (M-Series appliances in Log Collector mode). **Deploy Panorama with Dedicated Log Collectors** describes a deployment with Dedicated Log Collectors managed by Panorama virtual appliances or by M-Series appliances in Panorama mode.
Perform the following steps to deploy Panorama virtual appliances with local log collection. Skip any steps you have already performed (for example, the initial setup).

<table>
<thead>
<tr>
<th>Deploy Panorama Virtual Appliances with Local Log Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Manage Licenses and Updates

You can use Panorama to centrally manage licenses, software updates, and content updates on firewalls and Dedicated Log Collectors (M-Series appliances in Log Collector mode). When you deploy licenses or updates, Panorama checks in with the Palo Alto Networks licensing server or update server, verifies the request validity, and then allows retrieval and installation of the license or update. This capability facilitates deployment by eliminating the need to repeat the same tasks on each firewall or Dedicated Log Collector. It is particularly useful for managing firewalls that don’t have direct internet access or for managing Dedicated Log Collectors, which don’t have a web interface.

Before deploying updates, see Panorama, Log Collector, and Firewall Version Compatibility for important details about update version compatibility. You must activate a support subscription directly on each firewall; you cannot use Panorama to deploy support subscriptions. To activate licenses or install updates on the Panorama management server, see Register Panorama and Install Licenses and Install Content and Software Updates for Panorama.

▲ Manage Licenses on Firewalls Using Panorama
▲ Deploy Updates to Firewalls and Log Collectors Using Panorama
Manage Licenses on Firewalls Using Panorama

The following steps describe how to retrieve new licenses using an auth-code and push the license keys to managed firewalls. It also describes how to manually update (refresh) the license status of firewalls that do not have direct internet access. For firewalls that have direct internet access, Panorama automatically performs a daily check-in with the licensing server, retrieves license updates and renewals, and pushes them to the firewalls. The check-in is hard-coded to occur between 1 and 2 A.M.; you cannot change this schedule.

You cannot use Panorama to activate the support license of firewalls. You must access the firewalls individually to activate their support licenses.

To activate licenses for Panorama itself, see Register Panorama and Install Licenses.

<table>
<thead>
<tr>
<th>Manage Licenses on Firewalls Using Panorama</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Activate newly purchased licenses.</td>
</tr>
<tr>
<td>1. Select Panorama &gt; Device Deployment &gt; Licenses and click <strong>Activate</strong>.</td>
</tr>
<tr>
<td>2. Enter the <strong>Auth Code</strong> that Palo Alto Networks provided for each firewall that has a new license.</td>
</tr>
<tr>
<td>3. Click <strong>Activate</strong>.</td>
</tr>
<tr>
<td>4. (WildFire subscriptions only) Perform a commit on each firewall that has a new WildFire subscription to complete the activation:</td>
</tr>
<tr>
<td>• Commit any pending changes. You must access each firewall web interface to do this.</td>
</tr>
<tr>
<td>• Make a minor change and perform a commit. For example, update a rule description and commit the change. If the firewalls belong to the same device group, you can push the rule change from Panorama to initiate a commit on all those firewalls instead of accessing each firewall separately.</td>
</tr>
<tr>
<td>Check that the WildFire Analysis profile rules include the advanced file types that the WildFire subscription supports. If no rule changes are required, make a minor edit to a rule description and perform a commit.</td>
</tr>
</tbody>
</table>

| • Update the license status of firewalls. |
| 1. Select Panorama > Device Deployment > Licenses. |
| Each entry on the page indicates whether the license is active or inactive and displays the expiration date for active licenses. |
| 2. If you previously activated authentication codes for the support subscription directly on the firewalls, click **Refresh** and select the firewalls from the list. Panorama retrieves the license, deploys it to the firewalls and updates the licensing status on the Panorama web interface. |
Deploy Updates to Firewalls and Log Collectors Using Panorama

You can use Panorama to qualify software and content updates by deploying them to a subset of firewalls or Dedicated Log Collectors before installing the updates on the rest of your managed appliances. If you want to schedule periodic content updates, Panorama requires a direct internet connection. To deploy software or content updates on demand (unscheduled), the procedure differs based on whether Panorama is connected to the internet. Panorama displays a warning if you manually deploy a content update when a scheduled update process has started or will start within five minutes.

By default, you can download up to two software or content updates of each type to Panorama. When you start any download beyond that maximum, Panorama deletes the oldest update of the selected type. To change the maximum, see Manage Panorama Storage for Software and Content Updates.

- **Supported Updates**
- **Schedule a Content Update Using Panorama**
- **Deploy an Update to Log Collectors when Panorama is Internet-connected**
- **Deploy an Update to Log Collectors when Panorama is not Internet-connected**
- **Deploy an Update to Firewalls when Panorama is Internet-connected**
- **Deploy an Update to Firewalls when Panorama is not Internet-connected**

### Supported Updates

The software and content updates you can install vary based on which subscriptions are active on each firewall or Log Collector:

<table>
<thead>
<tr>
<th>Product Type</th>
<th>Software Updates</th>
<th>Content Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Collector</td>
<td>Panorama</td>
<td>Applications (Log Collectors don’t need Threats signatures)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Antivirus</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BrightCloud URL filtering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WildFire</td>
</tr>
<tr>
<td>Firewall</td>
<td>PAN-OS</td>
<td>Applications</td>
</tr>
<tr>
<td></td>
<td>GlobalProtect agent/app</td>
<td>Applications and Threats</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Antivirus</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BrightCloud URL filtering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WildFire</td>
</tr>
</tbody>
</table>
**Schedule a Content Update Using Panorama**

Panorama requires a direct internet connection for scheduling **Supported Updates** on firewalls and Log Collectors. Otherwise, you can perform only on-demand updates. (To schedule Antivirus, WildFire, or BrightCloud URL updates for Log Collectors, they must run Panorama 7.0.3 or a later release.) Each firewall or Log Collector receiving an update generates a log to indicate that the installation succeeded (Config log) or failed (System log). To schedule updates on the Panorama management server, see **Install Updates for Panorama with an Internet Connection**.

Before deploying updates, see **Panorama, Log Collector, and Firewall Version Compatibility** for important details about content release version compatibility. Refer to the **Release Notes** for the minimum content release version you must install for a Panorama release.

Panorama can download only one update at a time for updates of the same type; stagger the updates to ensure they succeed. If you schedule multiple updates of the same type to download during the same time interval, only the first download will succeed.

If your firewalls connect directly to the Palo Alto Networks Update Server, you can also use Panorama templates (**Device > Dynamic Updates**) to push content update schedules to the firewalls. If you want to delay the installation of updates for a period after they are released, you must deploy schedules using templates. In rare instances, a content update will have errors so specifying a delay increases the likelihood that Palo Alto Networks will identify and remove such updates from the Update Server before firewalls install them.

Perform the following steps for each update type you want to schedule.

<table>
<thead>
<tr>
<th>Schedule a Content Update Using Panorama</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Select Panorama &gt; Device Deployment &gt; Dynamic Updates, click Schedules, and Add a schedule.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Specify a Name (to identify the schedule), the update Type, and the update frequency (Recurrence). The frequency options depend on the update Type.</td>
</tr>
<tr>
<td>- PAN-OS software uses the Panorama timezone for update scheduling.</td>
</tr>
<tr>
<td>- If you set the Type to App and Threat, Log Collectors install and need only the Applications content, not the Threats content. Firewalls use both Applications and Threats content. For details, see <strong>Panorama, Log Collector, and Firewall Version Compatibility</strong>.</td>
</tr>
<tr>
<td>- The WildFire Private (WF-Private) type is available only if you set the WildFire Private Cloud field (Panorama &gt; Setup &gt; WildFire) to a WF-500 appliance, not to the WildFire cloud.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Select one of the following schedule actions and then select the firewalls or Log Collectors:</td>
</tr>
<tr>
<td>- <strong>Download And Install</strong> (Best Practice)—Select Devices (firewalls) or Log Collectors.</td>
</tr>
<tr>
<td>- <strong>Download Only</strong>—Panorama downloads the update but does not install it.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Click OK and Commit, for the Commit Type select Panorama, and click Commit again.</td>
</tr>
</tbody>
</table>
Deploy an Update to Log Collectors when Panorama is Internet-connected

For a list of software and content updates you can install on Log Collectors, see Supported Updates.

<table>
<thead>
<tr>
<th>Deploy an Update to Log Collectors when Panorama is Internet-connected</th>
<th></th>
</tr>
</thead>
</table>
| **Step 1** | Before you upgrade Log Collectors, ensure that you are running the appropriate Panorama software release on the Panorama management server. Palo Alto Networks highly recommends that Panorama and Log Collectors run the same Panorama software release and that Panorama, Log Collectors, and all managed firewalls run the same content release version. Panorama must be running the same (or later) software release as Log Collectors but must have the same or an earlier content release version:  
  - **Software release version**—If your Panorama management server is not already running the same or a later software release than the release to which you intend to update Log Collectors, then you must install the same or a later Panorama release on Panorama (see Install Content and Software Updates for Panorama) before you update any Log Collectors.  
  - **Content release version**—For content release versions, you should ensure that all Log Collectors are running the latest content release version or, at minimum, are running a later version than is running on Panorama; if not, then first update managed firewalls (using Panorama) and then update Log Collectors before you update the content release version on the Panorama management server.  
To check software and content versions:  
  - **Panorama management server**—To determine what software and content versions are running on the Panorama management server, log in to the Panorama web interface and go to General Information settings (Dashboard).  
  - **Log Collectors**—To determine what software and content versions are running on Log Collectors, log in to the CLI of each Log Collector and run the `show system info` command. |
| **Step 2** | Install the latest content updates. Refer to the Release Notes for the minimum content release versions required for a Panorama software release.  
1. Check Now (Panorama > Device Deployment > Dynamic Updates) for the latest updates. If an update is available, the Action column displays a Download link.  
2. If not already installed, Download the appropriate content updates. After a successful download, the link in the Action column changes from Download to Install.  
3. Install the content update (Applications or Applications and Threats update before any others):  
   Click Install, select the Log Collectors, and click OK. Regardless whether your subscription includes both Applications and Threats content, Panorama installs and needs only the Applications content. For details, see Panorama, Log Collector, and Firewall Version Compatibility.  
4. Repeat step 3 for any other updates (Antivirus, WildFire, or URL Filtering) as needed, one at a time, and in any sequence. |
### Deploy an Update to Log Collectors when Panorama is Internet-connected (Continued)

| Step 3 | Determine the software upgrade path for each Log Collector that you intend to update. You cannot skip installation of any major release versions in the path to your target Panorama release. For example, if you intend to upgrade from Panorama 6.0.13 to Panorama 7.1.3, you must:
|        | - Download and install Panorama 6.1.0.
|        | - Download and install Panorama 7.0.1 and reboot (7.0.1 is the base image for the 7.0 release; not 7.0.0).
|        | - Download Panorama 7.1.0. Optionally, install this base image and reboot before you install the target maintenance release.
|        | - Download and install Panorama 7.1.3 and reboot.
|        | Check which Software Version is running on each Log Collector you intend to upgrade (Panorama > Managed Collectors) and take note of each release you need to download in your path to Panorama 7.1.
|        | If upgrading more than one Log Collector, streamline the process by determining the upgrade paths for all Log Collectors you intend to upgrade before you start downloading images.
|        | We highly recommend that you review the known issues and changes to default behavior in the Release Notes and upgrade/downgrade considerations in the New Features Guide for each release through which you pass as part of your upgrade path.

| Step 4 | For all Log Collectors you intend to update, use the upgrade path(s) identified in Step 3 to upgrade Log Collectors to your target Panorama release.
|        | 1. On Panorama, Check Now (Panorama > Device Deployment > Software) for the latest updates. If an update is available, the Action column displays a Download link.
|        | 2. For each release in your upgrade path, Download the model-specific file for the release version to which you are upgrading. For example, to upgrade an M-Series appliance to Panorama 7.0.1, download the Panorama_m-7.0.1 image. After a successful download, the Action column changes from Download to Install for that image.
|        | 3. Click Install for the first (or next) version in your upgrade path and select the appropriate Log Collectors.
|        | 4. Select one of the following depending on the version you are installing within your upgrade path (Step 3):
|        |   - **Upload only to device (do not install)**
|        |   - **Reboot device after install**
|        |   As a best practice, when upgrading to a Panorama 7.1 maintenance release (Panorama 7.1.1 or a later release), install the Panorama 7.1.0 base image and reboot the appliance before you download and install the maintenance release.
|        | 5. Click OK to start the installation (or upload).
|        | 6. Repeat steps 3 through 6 until Log Collectors are running the desired release.
### Deploy an Update to Log Collectors when Panorama is Internet-connected (Continued)

**Step 5** Verify the software and content update versions that are installed on the Log Collector.

Log in to the Log Collector CLI and enter the `show system info` operational command. The output will resemble the following:

```
sw-version: 7.1.3
app-version: 571-1738
app-release-date: 2016/01/29 15:46:03
av-version: 1168-1550
av-release-date: 2016/01/21 14:31:27
threat-version: 548-1738
threat-release-date: 2016/01/29 15:46:03
```
Deploy an Update to Log Collectors when Panorama is not Internet-connected

For a list of software and content updates you can install on Log Collectors, see Supported Updates.

| Deploy an Update to Log Collectors when Panorama is not Internet-connected |
|---|---|
| **Step 1** Before you upgrade Log Collectors, ensure that you are running the appropriate Panorama software release on the Panorama management server. | Panorama must be running the same (or later) software release as Log Collectors but must have the same or an earlier content release version:
- **Software release version**—If your Panorama management server is not already running the same or a later software release than the release to which you intend to update Log Collectors, then you must install the same or a later Panorama release on Panorama (see Install Content and Software Updates for Panorama) before you update any Log Collectors.
- **Content release version**—For content release versions, ensure that all Log Collectors are running the latest content release version or, at minimum, are running a later version than you will install or that is running on Panorama; if not, then first update managed firewalls (using Panorama) and then update Log Collectors before you update the content release version on the Panorama management server (see Install Content and Software Updates for Panorama).

For important software and content compatibility details, see Panorama, Log Collector, and Firewall Version Compatibility.

To check the software and content versions:
- **Panorama management server**—Log in to the Panorama web interface and go to General Information settings (Dashboard).
- **Log Collectors**—Log in to the CLI of each Log Collector and run the `show system info` command.

| **Step 2** Determine which content updates you need to install. | You must install content updates before software updates.

Palo Alto Networks highly recommends that Panorama, Log Collectors, and all managed firewalls run the same content release version. |
|---|---|
| **Step 2** Determine which content updates you need to install. | 1. Log in to the CLI of each Log Collector and run the `show system info` command to view the current update versions.
2. For each content update, determine whether you need updates and take note of which content updates you need to download in **Step 4**.

Ensure that Panorama is running the same but not a later content release version than is running on managed firewalls and Log Collectors.
3. **(As needed)** Before you update content versions on Log Collectors, first upgrade managed firewalls to the same or later content release versions. |
**Deploy an Update to Log Collectors when Panorama is not Internet-connected (Continued)**

**Step 3** Determine the software upgrade path for each Log Collector that you intend to upgrade to Panorama 7.1.

You cannot skip installation of any major release versions in the path to your target Panorama release. For example, if you intend to upgrade from Panorama 6.0.12 to Panorama 7.1.3, you must:

- Download and install Panorama 6.1.0 and reboot.
- Download and install Panorama 7.0.1 and reboot (7.0.1 is the base image for the 7.0 release; not 7.0.0).
- Download Panorama 7.1.0. Optionally, install this base image and reboot before you install the target maintenance release.
- Download and install Panorama 7.1.3 and reboot.

**Step 4** Download the content and software updates to a host that can connect and upload the files to Panorama either over SCP or HTTPS.

1. Log in to Panorama, select **Panorama > Managed Collectors**, and note the current Software Version for the Log Collectors you intend to upgrade.

   We highly recommend that you review the known issues and changes to default behavior in the **Release Notes** and upgrade/downgrade considerations in the **New Features Guide** for each release through which you pass as part of your upgrade path.

2. Use a host with internet access to log in to the **Palo Alto Networks Customer Support website**.

3. **Download content updates**:
   - Click **Updates > Dynamic Updates** in the Resources section.
   - **Download** the desired content updates and save the files to the host. Perform this step for each content type you will update.

4. **Download software updates**:
   - Return to the main page of the Palo Alto Networks Customer Support website and click **Updates > Software Updates** in the Resources section.
   - Review the **Download** column to determine the version to install. The update package filenames for M-Series appliances begin with "Panorama_m" followed by the release number: Panorama_m-<release>.
     - You can quickly locate Panorama images by selecting **Panorama M Images** (for M-Series appliances) from the Filter By drop-down.
   - **Click** the appropriate filename and save the file to the host.
Deploy Updates to Firewalls and Log Collectors Using Panorama

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Install content updates on Log Collectors.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Install the Applications or Applications and Threats update first and then install any other updates (Antivirus, WildFire, or URL Filtering) as needed, one at a time, and in any sequence.</td>
</tr>
<tr>
<td></td>
<td>Regardless whether your subscription includes both Applications and Threats content, Panorama installs and needs only the Applications content. For details, see Panorama, Log Collector, and Firewall Version Compatibility.</td>
</tr>
<tr>
<td></td>
<td>1. In Panorama, select Panorama &gt; Device Deployment &gt; Dynamic Updates.</td>
</tr>
<tr>
<td></td>
<td>2. Click Upload, select the update Type, Browse to the appropriate content update file on the host, and click OK.</td>
</tr>
<tr>
<td></td>
<td>3. Click Install From File, select the update Type, and select the File Name of the update you just uploaded.</td>
</tr>
<tr>
<td></td>
<td>4. Select the Log Collectors.</td>
</tr>
<tr>
<td></td>
<td>5. Click OK to start the installation.</td>
</tr>
<tr>
<td></td>
<td>6. Repeat these steps for each content update.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Install software updates.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. In Panorama, select Panorama &gt; Device Deployment &gt; Software.</td>
</tr>
<tr>
<td></td>
<td>2. Click Upload, Browse to the appropriate software update file on the host, and click OK.</td>
</tr>
<tr>
<td></td>
<td>3. Click Install in the Action column for the release you just uploaded.</td>
</tr>
<tr>
<td></td>
<td>4. Select the Log Collectors on which to install the update.</td>
</tr>
<tr>
<td></td>
<td>5. Select one of the following based on the update version you are installing within the upgrade path (Step 3):</td>
</tr>
<tr>
<td></td>
<td>- Upload only to device (do not install)</td>
</tr>
<tr>
<td></td>
<td>- Reboot device after install</td>
</tr>
<tr>
<td></td>
<td>As a best practice, when upgrading to a Panorama 7.1 maintenance release (Panorama 7.1.1 or a later Panorama 7.1 release), install the Panorama 7.1.0 base image and reboot the appliance before you upload and install the maintenance release.</td>
</tr>
<tr>
<td></td>
<td>6. Click OK to start the installation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Verify the software and content versions that are installed on each Log Collector.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Log in to the Log Collector CLI and enter the show system info operational command. The output will resemble the following:</td>
</tr>
<tr>
<td></td>
<td>sw-version: 7.1.3  app-version: 571-1738  app-release-date: 2016/01/29 15:46:03</td>
</tr>
<tr>
<td></td>
<td>av-version: 1168-11550  av-release-date: 2016/01/21 14:31:27</td>
</tr>
<tr>
<td></td>
<td>threat-version: 548-1738  threat-release-date: 2016/01/29 15:46:03</td>
</tr>
</tbody>
</table>

Deploy an Update to Log Collectors when Panorama is not Internet-connected (Continued)
Deploy an Update to Firewalls when Panorama is Internet-connected

Before deploying software updates to firewalls, you must upgrade Panorama and then upgrade Log Collectors. For a list of software and content updates you can install on firewalls, see Supported Updates.

You cannot deploy GlobalProtect data file updates on demand; you can only schedule the updates using the firewall web interface or a Panorama template.

Deploy an Update to Firewalls when Panorama is not Internet-connected

For a list of software and content updates you can install on firewalls, see Supported Updates.

### Deploy an Update to Firewalls when Panorama is not Internet-connected

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Before you upgrade managed firewalls, ensure that you are running the appropriate Panorama software release on the Panorama management server and Log Collectors. Palo Alto Networks highly recommends that Panorama and Log Collectors run the same Panorama software release and that Panorama, Log Collectors, and all managed firewalls run the same content release version. For important software and content compatibility details, see Panorama, Log Collector, and Firewall Version Compatibility.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panorama must be running the same (or later) software release as the firewalls but must have the same or an earlier content release version:</td>
<td></td>
</tr>
<tr>
<td>Software release version—if you Panorama management server or Log Collectors are not already running the same or a later software release than the release to which you intend to update firewalls, then you must install the same or a later Panorama release on Panorama and then on Log Collectors (see Install Content and Software Updates for Panorama) before you update any firewalls.</td>
<td></td>
</tr>
<tr>
<td>Content release version—for content release versions, you should ensure that all firewalls are running the latest content release version or, at minimum, are running a later version than is running on Panorama and Log Collectors; if not, then update managed firewalls and then Deploy an Update to Log Collectors when Panorama is not Internet-connected before you update the content release version on the Panorama management server (see Install Content and Software Updates for Panorama). To check the software and content versions:</td>
<td></td>
</tr>
<tr>
<td>Panorama management server—log in to the Panorama web interface and go to General Information settings (Dashboard).</td>
<td></td>
</tr>
<tr>
<td>Log Collectors—log in to the CLI of each Log Collector and run the show system info command.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Save a backup of the current configuration file on each managed firewall you plan to upgrade. Although the firewall automatically creates a configuration backup, it is a best practice to create and externally store a backup before you upgrade.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Log in to Panorama and Export Panorama and devices config bundle (Panorama &gt; Setup &gt; Operations) to generate and export the latest configuration backup of Panorama and of each managed appliance.</td>
<td></td>
</tr>
<tr>
<td>2. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the upgrade.</td>
<td></td>
</tr>
</tbody>
</table>
### Deploy an Update to Firewalls when Panorama is not Internet-connected (Continued)

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Determine which content updates you need to install. Refer to the <a href="#">Release Notes</a> for the minimum content release version you must install for a PAN-OS release.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>You must install content updates before software updates. Palo Alto Networks highly recommends that Panorama, Log Collectors, and all managed firewalls run the same content release version.</td>
</tr>
</tbody>
</table>

| Warning | For each content update, determine whether you need updates and take note of which content updates you need to download in Step 5. Ensure that Panorama is running the same but not a later content release version than is running on managed firewalls and Log Collectors. |

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Determine the software upgrade path for each firewall that you intend to upgrade to PAN-OS 7.1. You cannot skip installation of any major release versions in the path to your target PAN-OS release. For example, if you intend to upgrade from PAN-OS 6.0.12 to PAN-OS 7.1.3, you must:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Download and install PAN-OS 6.1.0 and reboot.</td>
</tr>
<tr>
<td></td>
<td>• Download and install PAN-OS 7.0.1 and reboot (7.0.1 is the base image for the 7.0 release; not 7.0.0).</td>
</tr>
<tr>
<td></td>
<td>• Download PAN-OS 7.1.0. Optionally, install this base image and reboot before you install the target maintenance release.</td>
</tr>
<tr>
<td></td>
<td>• Download and install PAN-OS 7.1.3 and reboot.</td>
</tr>
</tbody>
</table>

| Select Panorama > Managed Devices, and note the current Software Version for the firewalls you need to upgrade. |
| We highly recommend that you review the known issues and changes to default behavior in the [Release Notes](#) and upgrade/downgrade considerations in the [New Features Guide](#) for each release through which you pass as part of your upgrade path. |
### Deploy an Update to Firewalls when Panorama is not Internet-connected (Continued)

| Step 5 | Download the content and software updates to a host that can connect and upload the files to Panorama either over SCP or HTTPS.  
By default, you can upload a maximum of two software or content updates of each type to a Panorama appliance and if you download a third update of the same type, Panorama will delete the update for the earliest version of that type. If you need to upload more than two software updates or content updates of a single type, use the `set max-num-images count <number>` CLI command to increase the maximum. |
| --- | --- |
| 1. | Use a host with internet access to log in to the Palo Alto Networks Customer Support website.  
2. | Download content updates:  
   a. Click Updates > Dynamic Updates in the Resources section.  
   b. Download the latest content release version (or, at a minimum, a later version than you will install or is running on the Panorama management server) and save the file to the host. Perform this step for each content type you need to update.  
3. | Download software updates:  
   a. Return to the main page of the Palo Alto Networks Customer Support website and click Updates > Software Updates in the Resources section.  
   b. Review the Download column to determine the version(s) you need to install. The filename of the update packages indicates the model. For example, to upgrade a PA-200, PA-3050, and PA-5060 firewall to PAN-OS 7.1.0, download the `PanOS_200-7.1.0`, `PanOS_3000-7.1.0`, and `PanOS_5000-7.1.0` images.  
   c. Click the filename and save the file(s) to the host. |

| Step 6 | Install content updates on managed firewalls.  
If you need to install content updates, you must do so before you install software updates. Additionally, you must install content updates on firewalls first and then on Log Collectors before you update the content release version on Panorama. |
| --- | --- |
| 1. | Select Panorama > Device Deployment > Dynamic Updates.  
2. | Click Upload, select the update Type, Browse to the appropriate content update file, and click OK.  
3. | Click Install From File, select the update Type, and select the File Name of the content update you just uploaded.  
4. | Select the firewalls on which to install the update.  
5. | Click OK to start the installation.  
6. | Repeat these steps for each content update. |
### Deploy an Update to Firewalls when Panorama is not Internet-connected (Continued)

<table>
<thead>
<tr>
<th>Step 7</th>
<th>(Firewalls serving as GlobalProtect portals only) Upload and activate a GlobalProtect agent/app software update on firewalls. You activate the update on firewalls so that users can download it to their client systems.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Use a host with internet access to log in to the Palo Alto Networks Customer Support website.</td>
</tr>
<tr>
<td>2.</td>
<td>Download the appropriate GlobalProtect agent/app software update.</td>
</tr>
<tr>
<td>4.</td>
<td>Click Upload, Browse to the appropriate GlobalProtect agent/app software update on the host to which you downloaded the file, and click OK.</td>
</tr>
<tr>
<td>5.</td>
<td>Click Activate From File and select the File Name of the GlobalProtect agent/app update you just uploaded.</td>
</tr>
<tr>
<td>6.</td>
<td>You can activate only one version of agent/app software at a time. If you activate a new version but some agents require a previous version, you will have to reactivate the earlier version again for those agents to download the previous update.</td>
</tr>
<tr>
<td>7.</td>
<td>Select the firewalls on which to activate the update.</td>
</tr>
<tr>
<td>8.</td>
<td>Click OK to activate.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Upload PAN-OS software updates.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select Panorama &gt; Device Deployment &gt; Software.</td>
</tr>
<tr>
<td>2.</td>
<td>Click Upload, Browse to the appropriate software update file on the host, and click OK.</td>
</tr>
</tbody>
</table>
### Deploy an Update to Firewalls when Panorama is not Internet-connected (Continued)

#### Step 9 Install PAN-OS software updates.

To avoid downtime when updating the software on high availability (HA) firewalls, update one HA peer at a time.

For active/active firewalls, it doesn’t matter which peer you update first.

For active/passive firewalls, you must update the passive peer first, suspend the active peer (fail over), update the active peer, and then return the active peer to a functional state (fail back).

1. Perform the steps that apply to your firewall configuration to install the PAN-OS software update you just uploaded.
   - **Non-HA firewalls**—Click **Install** in the Action column, select all the firewalls you are upgrading, select **Reboot device after install**, and click **OK**.
   - **Active/Active HA firewalls**:
     a. Click **Install**, clear **Group HA Peers**, select either HA peer, select **Reboot device after install**, and click **OK**. Wait for the firewall to finish rebooting before proceeding.
     b. Click **Install**, clear **Group HA Peers**, select the HA peer that you didn’t update yet, select **Reboot device after install**, and click **OK**.
   - **Active/Passive HA firewalls**—In this example, the active firewall is named fw1 and the passive firewall is named fw2:
     a. Click **Install**, clear **Group HA Peers**, select fw2, select **Reboot device after install**, and click **OK**. Wait for fw2 to finish rebooting before proceeding.
     b. Access fw1, select **Device > High Availability > Operational Commands**, and click **Suspend local device**.
     c. Access fw2 and, on the Dashboard, High Availability widget, verify that the **Local** firewall state is **active** and the **Peer** firewall is **suspended**.
     e. Access fw1, select **Device > High Availability > Operational Commands**, and click **Make local device functional**. Wait two minutes before proceeding.
     f. On fw1, select the Dashboard tab and, in the High Availability widget, verify that the **Local** firewall state is **active** and the **Peer** firewall is **passive**.

2. After you complete the above steps for a PAN-OS release update, repeat Step 8 and Step 9 to upload the next PAN-OS release in your upgrade path as needed until all firewalls are running the appropriate PAN-OS 7.1 release.

#### Step 10 Verify the software and content versions that are installed on each managed firewall.

1. Select **Panorama > Managed Devices**.
2. Locate the firewall and review the values in the Software Version, Apps and Threat, Antivirus, URL Filtering, and GlobalProtect Client columns.
Monitor Network Activity

Panorama provides a comprehensive, graphical view of network traffic. Using the visibility tools on Panorama—the Application Command Center (ACC), logs, and the report generation capabilities—you can centrally analyze, investigate and report on all network activity, identify areas with potential security impact, and translate them into secure application enablement policies.

This section covers the following topics:

- Use Panorama for Visibility
- Use Case: Monitor Applications Using Panorama
- Use Case: Respond to an Incident Using Panorama
Use Panorama for Visibility

In addition to its central deployment and firewall configuration features, Panorama also allows you to monitor and report on all traffic that traverses your network. While the reporting capabilities on Panorama and the firewall are very similar, the advantage that Panorama provides is that it is a single pane view of aggregated information across all your managed firewalls. This aggregated view provides actionable information on trends in user activity, traffic patterns, and potential threats across your entire network.

Using the Application Command Center (ACC), the App-Scope, the log viewer, and the standard, customizable reporting options on Panorama, you can quickly learn more about the traffic traversing the network. The ability to view this information allows you to evaluate where your current policies are adequate and where they are insufficient. You can then use this data to augment your network security strategy. For example, you can enhance the security rules to increase compliance and accountability for all users across the network, or manage network capacity and minimize risks to assets while meeting the rich application needs for the users in your network.

The following topics provide a high-level view of the reporting capabilities on Panorama, including a couple of use cases to illustrate how you can use these capabilities within your own network infrastructure. For a complete list of the available reports and charts and the description of each, refer to the online help.

- Monitor the Network with the ACC and AppScope
- Analyze Log Data
- Generate, Schedule, and Email Reports

Monitor the Network with the ACC and AppScope

Both the ACC and the AppScope allow you to monitor and report on the data recorded from traffic that traverses your network.

The ACC on Panorama displays a summary of network traffic. Panorama can dynamically query data from all the managed firewalls on the network and display it in the ACC. This display allows you to monitor the traffic by applications, users, and content activity—URL categories, threats, security policies that effectively block data or files—across the entire network of Palo Alto Networks next-generation firewalls.

The AppScope helps identify unexpected or unusual behavior on the network at a glance. It includes an array of charts and reports—Summary Report, Change Monitor, Threat Monitor, Threat Map, Network Monitor, Traffic Map—that allow you to analyze traffic flows by threat or application, or by the source or destination for the flows. You can also sort by session or byte count.

Use the ACC and the AppScope to answer questions such as:

<table>
<thead>
<tr>
<th>ACC</th>
<th>Monitor &gt; AppScope</th>
</tr>
</thead>
<tbody>
<tr>
<td>• What are the top applications used on the network and how many are high-risk applications? Who are the top users of high-risk applications on the network?</td>
<td>• What are the application usage trends—what are the top five applications that have gained use and the top five that have decreased in use?</td>
</tr>
<tr>
<td>• What are the top URL categories being viewed in the last hour?</td>
<td>• How has user activity changed over the current week as compared to last week or last month?</td>
</tr>
</tbody>
</table>
Monitor Network Activity

<table>
<thead>
<tr>
<th>ACC</th>
<th>Monitor &gt; AppScope</th>
</tr>
</thead>
<tbody>
<tr>
<td>• What are the top bandwidth-using applications? Who are the users/hosts that consume the highest bandwidth?</td>
<td>• Which users and applications take up most of the network bandwidth? And how has this consumption changed over the last 30 days?</td>
</tr>
<tr>
<td>• What content or files are being blocked and are there specific users who trigger this File Blocking/Data Filtering rule?</td>
<td>• What are the threats on the network, and how are these incoming and outgoing traffic threats distributed geographically?</td>
</tr>
<tr>
<td>• What is the amount of traffic exchanged between two specific IP addresses or generated by a specific user? Where is the destination server or client located geographically?</td>
<td></td>
</tr>
</tbody>
</table>

You can then use the information to maintain or enforce changes to the traffic patterns on your network. See Use Case: Monitor Applications Using Panorama for a glimpse into how the visibility tools on Panorama can influence how you shape the acceptable use policies for your network.

Here are a few tips to help you navigate the ACC:

- **Switch from a Panorama view to a Device view**—Use the **Context** drop-down to access the web interface of any managed device from Panorama. Select the **Device Group** for which you want to monitor traffic. Switch the **Data Source** to access the data from Panorama or managed firewalls. **Export** the current view of the ACC.

- **Change Device Group and Data Source**—The default **Data Source** used to display the statistics on the charts in the ACC is **Panorama local data**, and the default **Device Group** setting is **All**. Using the local data on Panorama provides a quick load time for the charts. You can, however, change the data source to **Remote Device Data** if all the managed firewalls are on PAN-OS 7.0 or a later release. If the managed firewalls have a mix of PAN-OS 7.0 and earlier releases, you can only view Panorama data. When configured to use Remote Device Data, Panorama will poll all the managed firewalls and present an aggregated view of the data. The onscreen display indicates the total number of firewalls being polled and the number of firewalls that have responded to the query for information.
Use Panorama for Visibility

- **Select the Tabs and Widgets to View**—The ACC includes three tabs and an array of widgets that allow you to find the information that you care about. With the exception of the application usage widget and host information widget, all the other widgets display data only if the corresponding feature has been licensed on the firewall, and you have enabled logging.

- **Tweak Time Frame and Refine Data**—The reporting time period in the ACC ranges from the last 15 minutes to the last hour, day, week, month, or any custom-defined time. By default, each widget displays the top 10 items and aggregates all the remaining items as others. You can sort the data in each widget using various attributes—for example, sessions, bytes, threats, content, and URLs. You can also set local filters to filter the display within the table and graph in a widget, and then promote the widget filter as a global filter to pivot the view across all the widgets in the ACC.

**Analyze Log Data**

The **Monitor** tab on Panorama provides access to log data; these logs are an archived list of sessions that have been processed by the managed firewalls and forwarded to Panorama.

Log data can be broadly grouped into two types: those that detail information on traffic flows on your network such as applications, threats, host information profiles, URL categories, content/file types and those that record system events, configuration changes and alarms.

Based on the log forwarding configuration on the managed firewalls, the **Monitor > Logs** tab can include logs for traffic flows, threats, URL filtering, data filtering, host information profile (HIP) matches, and WildFire submissions. You can review the logs to verify a wealth of information on a given session or transaction. Some examples of this information are the user who initiated the session, the action (allow or deny) that the firewall performed on the session, and the source and destination ports, zones, and addresses. The System and Config logs can indicate a configuration change or an alarm that the firewall triggered when a configured threshold was exceeded.

*If Panorama will manage firewalls running software versions earlier than PAN-OS 7.0, specify a WildFire server from which Panorama can gather analysis information for WildFire samples that those firewalls submit. Panorama uses the information to complete WildFire Submissions logs that are missing field values introduced in PAN-OS 7.0. Firewalls running earlier releases won’t populate those fields. To specify the server, select **Panorama > Setup > WildFire**, edit the General Settings, and enter the **WildFire Private Cloud** name. The default is **wildfire-public-cloud**, which is the WildFire cloud hosted in the United States.*

**Generate, Schedule, and Email Reports**

Panorama allows you to generate reports manually as needed, or schedule reports to run at specific intervals. You can save and export reports, or you can configure Panorama to email reports to specific recipients. The ability to share reports using email is particularly useful if you want to share reporting information with administrators who do not have access to Panorama.

*It is recommended that you install matching software releases on Panorama and the firewalls for which you will generate reports. For example, if the Panorama management server runs Panorama 6.1, install PAN-OS 6.1 on its managed firewalls before generating the reports. This practice avoids issues that might occur if you create reports that include fields supported in the Panorama release but not supported in an earlier PAN-OS release on the firewalls.*

You can create the following types of reports:
<table>
<thead>
<tr>
<th>Report Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Predefined</strong></td>
<td>A suite of predefined reports in the <strong>Monitor &gt; Reports</strong> tab that are available in four categories: Applications, Threats, URL Filtering, and Traffic.</td>
</tr>
<tr>
<td><strong>User-activity</strong></td>
<td>The user activity report is a predefined report that is used to create an on-demand report to document the application use and URL activity broken down by URL category for a specific user with estimated browse time calculations. This report is available in the <strong>Monitor &gt; PDF Reports &gt; User Activity Reports</strong> tab.</td>
</tr>
<tr>
<td><strong>Custom</strong></td>
<td>Create and schedule custom reports that display exactly the information you want by filtering the conditions and columns to include. To view the databases available for generating custom reports, see the <strong>Monitor &gt; Manage Custom Reports</strong> tab. You can generate reports to query data from <strong>Summary Databases</strong> on Panorama (<strong>Panorama Data</strong>) or on the managed firewalls (<strong>Remote Device Data</strong>), or use the <strong>Detailed Logs</strong> on Panorama or on the managed firewalls. You can also create Report Groups (<strong>Monitor &gt; PDF Reports &gt; Report Groups</strong> tab) to compile predefined reports and custom reports as a single PDF.</td>
</tr>
<tr>
<td><strong>PDF Summary</strong></td>
<td>Aggregate up to 18 predefined reports, graphs, and custom reports into one PDF document.</td>
</tr>
</tbody>
</table>

**Generate, Schedule, and Email Reports**

**Step 1** Generate reports.

The steps to generate a report depend on the type:

- **Create a custom report.**
  a. Select **Monitor > Manage Custom Reports**.
  b. Click **Add** and enter a **Name** for the report.
  c. Select a **Database** for the report. You can use a summary database or detailed logs on Panorama or on the managed firewalls.
  d. Select the **Scheduled** check box.
  e. Define your filtering criteria. Select the **Time Frame**, the **Sort By** order, **Group By** preference, and select the columns that must display in the report.

  Selecting the **Sort By** order is required to generate an accurate report. If you do not select a **Sort By** order, the generated custom report is populated with the most recent log matches for the selected database.

  f. (Optional) Select the **Query Builder** attributes to further refine the selection criteria.
  g. To test the report settings, select **Run Now**. If necessary, modify the settings to change the information that the report displays.
  h. Click **OK** to save the custom report.

- **Run a PDF Summary Report.**
  a. Select **Monitor > PDF Reports > Manage PDF Summary**.
  b. Click **Add** and enter a **Name** for the report.
  c. Use the drop-down for each report group and select one or more of the elements to design the PDF Summary Report. You can include up to 18 elements.
  d. Click **OK** to save the settings.
Use Panorama for Visibility

<table>
<thead>
<tr>
<th>Generate, Schedule, and Email Reports (Continued)</th>
</tr>
</thead>
</table>
| **Step 2**  Configure a Report Group.  
It can include predefined reports, PDF Summary reports, and custom reports. Panorama compiles all the included reports into a single PDF.  |
| 1. Select Monitor > PDF Reports > Report Groups.  
2. Click Add and enter a Name for the report group.  
3. (Optional) Select the Title Page check box and add a Title for the PDF output.  
5. Click Add to include the selected reports in the report group.  
6. Click OK to save the settings. |

<table>
<thead>
<tr>
<th><strong>Step 3</strong>  Configure an Email server profile.</th>
</tr>
</thead>
</table>
| 1. Select Panorama > Server Profiles > Email.  
2. Click Add and enter a Name for the profile.  
3. For each Simple Mail Transport Protocol (SMTP) server (up to four), click Add and enter the information required to connect to the server and send email:  
   • Name—A name to identify the SMTP server (1-31 characters). This field is just a label and doesn't have to be the hostname of an existing server.  
   • Email Display Name—The name to display in the From field of the email.  
   • From—The email address where notification emails will be sent from.  
   • To—The email address to which notification emails will be sent.  
   • Additional Recipient—To send notifications to a second account, enter the additional address here.  
   • Email Gateway—The IP address or hostname of the SMTP gateway to use to send the emails.  
4. Click OK to save the profile. |

<table>
<thead>
<tr>
<th><strong>Step 4</strong>  Schedule the report for email delivery.</th>
</tr>
</thead>
</table>
| 1. Select Monitor > PDF Reports > Email Scheduler.  
2. Click Add and enter a Name for the email scheduler profile.  
3. Select the Report Group, the Email server profile you just created (Email Profile), and the Recurrence for the report.  
4. To verify that the email settings are accurate, click Send test email.  
5. Click OK and Commit, for the Commit Type select Panorama, and click Commit again. |
Use Case: Monitor Applications Using Panorama

This example takes you through the process of assessing the efficiency of your current policies and determining where you need to adjust them to fortify the acceptable use policies for your network.

When you log in to Panorama, the **Top Applications** widget on the **Dashboard** gives a preview of the most used applications over the last hour. To display the widget, select **Widgets > Application > Top Applications** in the toolbar. You can either glance over the list of top applications and mouse over each application block for which you want to review the details, or you can select the **ACC** tab to view the same information as an ordered list. The following image is a view of the **Top Applications** widget on the **Dashboard**.

![Top Applications Widget](image)

The data source for this display is the application statistics database; it does not use the Traffic logs and is generated whether or not you have enabled logging for security rules. This view into the traffic on your network depicts everything that is allowed on your network and is flowing through unblocked by any policy rules that you have defined.

In the **ACC** tab, you can select and toggle the **Data Source** to be local on **Panorama** or you can query the managed firewalls (**Remote Device Data**) for the data; Panorama automatically aggregates and displays the information. For a speedier flow, consider using Panorama as the data source (with log forwarding to Panorama enabled) because the time to load data from the managed firewalls varies by the time period for which you choose to view data and the volume of traffic that is generated on your network. If your managed firewalls have a combination of PAN-OS 7.0 and earlier versions, **Remote Device Data** is not available.

The **Dashboard** example in **Figure: Top Applications Widget** shows BitTorrent as a popular application. If you click the BitTorrent application block, Panorama opens the **ACC > Network Activity** tab with BitTorrent applied as a global filter and shows information on the application, users who accessed the application, and the details on the risk level and characteristics of the application.
In the **User Activity** widget, you can see how many users are using BitTorrent and the volume of traffic being generated. If you have enabled User-ID, you can view the names of the users who are generating this traffic, and drill in to review all the sessions, content or threats associated with each user.

In the **Threat Activity** tab, view the **Compromised Hosts** widget to see what correlation objects were matched on, and view the match evidence associated with the user and application. You can also view the threat name, category and ID in the **Threat Activity** widget.

With BitTorrent set as a global filter, use the **Destination IP Activity** and the **Destination Regions** widgets to verify where the traffic was destined. You can also view the ingress and egress zones and the security rule that is letting this connection through.

For more detailed information, jump into the Traffic logs for a filtered view and review each log entry for ports used, packets sent, bytes sent and received. Adjust the columns to view more information or less information based on your needs.

The **Monitor > App-Scope> Traffic Map** tab displays a geographical map of the traffic flow and provides a view of incoming versus outgoing traffic. You can also use the **Monitor > App-Scope > Change Monitor** tab to view changes in traffic patterns. For example, compare the top applications used over this hour to the last week or month to determine if there is a pattern or trend.

With all the information you have now uncovered, you can evaluate what changes to make to your policy configurations. Here are some suggestions to consider:

- Be restrictive and create a pre-rule on Panorama to block all BitTorrent traffic. Then use Panorama device groups to create and push this policy rule to one or more firewalls.
• Enforce bandwidth use limits and create a QoS profile and policy rule that de-prioritizes non-business traffic. Use Panorama device groups and templates to configure QoS and then push rules to one or more firewalls.

• Reduce risk to your network assets and create an application filter that blocks all file sharing applications that are peer-to-peer technology with a risk factor of 4 or 5. Make sure to verify that the BitTorrent application is included in that application filter, and will therefore be blocked.

• Schedule a custom report group that pulls together the activity for the specific user and that of top applications used on your network to observe that pattern for another week or two before taking action.

Besides checking for a specific application, you can also check for any unknown applications in the list of top applications. These are applications that did not match a defined App-ID signature and display as unknown-udp and unknown-tcp. To delve into these unknown applications, click on the name to drill down to the details for the unclassified traffic.

Use the same process to investigate the top source IP addresses of the hosts that initiated the unknown traffic along with the IP address of the destination host to which the session was established. For unknown traffic, the traffic logs, by default, perform a packet capture (pcap) when an unknown application is detected. The green arrow in the left column represents the packet capture snippet of the application data. Clicking on the green arrow displays the pcap in the browser.

Having the IP addresses of the servers (destination IP), the destination port, and the packet captures, you will be better positioned to identify the application and make a decision on how you would like to take action on your network. For example, you can create a custom application that identifies this traffic instead of labeling it as unknown TCP or UDP traffic. Refer to the article Identifying Unknown Applications for more information on identifying unknown application and Custom Application Signatures for information on developing custom signatures to discern the application.
Use Case: Respond to an Incident Using Panorama

Network threats can originate from different vectors, including malware and spyware infections due to drive-by downloads, phishing attacks, unpatched servers, and random or targeted denial of service (DoS) attacks, to name a few methods of attack. The ability to react to a network attack or infection requires processes and systems that alert the administrator to an attack and provide the necessary forensics evidence to track the source and methods used to launch the attack.

The advantage that Panorama provides is a centralized and consolidated view of the patterns and logs collected from the managed firewalls across your network. You can use the information from the automated correlation engine alone or in conjunction with the reports and logs generated from a Security Information Event Manager (SIEM), to investigate how an attack was triggered and how to prevent future attacks and loss of damage to your network.

The questions that this use case probes are:

- How are you notified of an incident?
- How do you corroborate that the incident is not a false positive?
- What is your immediate course of action?
- How do you use the available information to reconstruct the sequence of events that preceded or followed the triggering event?
- What are the changes you need to consider for securing your network?

This use case traces a specific incident and shows how the visibility tools on Panorama can help you respond to the report.

- Incident Notification
- Review the Widgets in the ACC
- Review Threat Logs
- Review WildFire Logs
- Review Data Filtering Logs
- Update Security Rules

Incident Notification

There are several ways that you could be alerted to an incident depending on how you've configured the Palo Alto Networks firewalls and which third-party tools are available for further analysis. You might receive an email notification that was triggered by a log entry recorded to Panorama or to your syslog server, or you might be informed through a specialized report generated on your SIEM solution, or a third-party paid service or agency might notify you. For this example, let's say that you receive an email notification from Panorama. The email informs you of an event that was triggered by an alert for a Zero Access gen\textbf{ent.Gen Command And Control Traffic} that matched against a spyware signature. Also listed in the email are the IP address of the source and destination for the session, a threat ID and the timestamp of when the event was logged.
Review the Widgets in the ACC

In the ACC > Threat Activity tab, check the Compromised Hosts widget and Threat Activity widget for any critical or high severity threats. In the Compromised Hosts widget, look into the Matching Objects and click a Match Count value to view the match evidence for the associated incident.

Review Threat Logs

To begin investigating the alert, use the threat ID to search the Threat logs on Panorama (Monitor > Logs > Threat). From the Threat logs, you can find the IP address of the victim, export the packet capture (PCAP) by clicking the download icon in the log entry, and use a network analyzer tool such as WireShark to review the packet details. In the HTTP case, look for a malformed or bogus HTTP REFERER in the protocol, suspicious host, URL strings, the user agent, the IP address and port in order to validate the incident. Data from these pcaps is also useful in searching for similar data patterns and creating custom signatures or modifying security policy to better address the threat in the future.

As a result of this manual review, if you feel confident about the signature, consider transitioning the signature from an alert action to a block action for a more aggressive approach. In some cases, you may choose to add the attacker IP to an IP block list to prevent further traffic from that IP address from reaching the internal network.

To continue with the investigation on the incident, use the information on the attacker and the victim IP address to find out more information, such as:

- Where is the attacker located geographically? Is the IP address an individual IP address or a NATed IP address?
- Was the event caused by a user being tricked into going to a website, a download, or was it sent through an email attachment?
- Is the malware being propagated? Are there other compromised hosts/endpoints on the network?
- Is it a zero-day vulnerability?

The log details for each log entry display the related logs for the event. This information points you to the Traffic, Threat, URL Filtering or other logs that you can review and correlate the events that led to the incident. For example, filter the Traffic log (Monitor > Logs > Traffic) using the IP address as both the source and the destination IP to get a complete picture of all the external and internal hosts.CLIENTS with which this victim IP address has established a connection.
Use Case: Respond to an Incident Using Panorama

Monitor Network Activity

Review WildFire Logs

In addition to the Threat logs, use the victim IP address to filter though the WildFire Submissions logs. The WildFire Submissions logs contain information on files uploaded to the WildFire service for analysis. Because spyware typically embeds itself covertly, reviewing the WildFire Submissions logs tells you whether the victim recently downloaded a suspicious file. The WildFire forensics report displays information on the URL from which the file or .exe was obtained, and the behavior of the content. It informs you if the file is malicious, if it modified registry keys, read/wrote into files, created new files, opened network communication channels, caused application crashes, spawned processes, downloaded files, or exhibited other malicious behavior. Use this information to determine whether to block the application that caused the infection (web-browsing, SMTP, FTP), make more stringent URL Filtering rules, or restrict some applications/actions (for example, file downloads to specific user groups).

Access to the WildFire logs from Panorama requires the following: a WildFire subscription, a File Blocking profile that is attached to a Security rule, and Threat log forwarding to Panorama. If Panorama will manage firewalls running software versions earlier than PAN-OS 7.0, specify a WildFire server from which Panorama can gather analysis information for WildFire samples that those firewalls submit. Panorama uses the information to complete WildFire Submissions logs that are missing field values introduced in PAN-OS 7.0. Firewalls running earlier releases won't populate those fields. To specify the server, select Panorama > Setup > WildFire, edit the General Settings, and enter the WildFire Private Cloud name. The default is wildfire-public-cloud, which is the WildFire cloud hosted in the United States.

Review Data Filtering Logs

The Data Filtering log (Monitor > Logs > Data Filtering) is another valuable source for investigating malicious network activity. While you can periodically review the logs for all the files that you are being alerted on, you can also use the logs to trace file and data transfers to or from the victim IP address or user, and verify the direction and flow of traffic: server to client or client to server. To recreate the events that preceded and followed an event, filter the logs for the victim IP address as a destination, and review the logs for network activity.

Because Panorama aggregates information from all managed firewalls, it presents a good overview of all activity in your network. Some of the other visual tools that you can use to survey traffic on your network are the Threat Map, Traffic Map, and the Threat Monitor. The threat map and traffic map (Monitor > AppScope > Threat Map or Traffic Map) allow you to visualize the geographic regions for incoming and outgoing traffic. It is particularly useful for viewing unusual activity that could indicate a possible attack from outside, such as a DDoS attack. If, for example, you do not have many business transactions with Eastern Europe, and the map reveals an abnormal level of traffic to that region, click into the corresponding area of the map to launch and view the ACC information on the top applications, traffic details on the session count, bytes sent and received, top sources and destinations, users or IP addresses, and the severity of the threats detected, if any. The threat monitor (Monitor > AppScope > Threat Monitor) displays the top ten threats on your network, or the list of top attackers or top victims on the network.
Monitor Network Activity

Use Case: Respond to an Incident Using Panorama

Update Security Rules

With all the information you have now uncovered, you can sketch together how the threat impacts your network—the scale of the attack, the source, the compromised hosts, the risk factor—and evaluate what changes, if any, to follow through. Here are some suggestions to consider:

- Forestall DDoS attacks by enhancing your DoS Protection profile to configure random early drop or to drop SYN cookies for TCP floods. Consider placing limits on ICMP and UDP traffic. Evaluate the options available to you based on the trends and patterns you noticed in your logs, and implement the changes using Panorama templates.

Create a dynamic block list (Objects > Dynamic Block Lists), to block specific IP addresses that you have uncovered from several intelligence sources: analysis of your own threat logs, DDoS attacks from specific IP addresses, or a third-party IP block list.

The list must be a text file that is located on a web server. Using device groups on Panorama, push the object to the managed firewalls so that the firewalls can access the web server and import the list at a defined frequency. After creating a dynamic block list object, define a Security rule that uses the address object in the source and destination fields to block traffic from or to the IP address, range, or subnet defined. This approach allows you to block intruders until you resolve the issue and make larger policy changes to secure your network.

- Determine whether to create shared policy rules or device group rules to block specific applications that caused the infection (web-browsing, SMTP, FTP), make more stringent URL Filtering rules, or restrict some applications/actions (for example, file downloads to specific user groups).

- On Panorama, you can also switch to the firewall context and configure the firewall for Botnet reports that identify potential botnet-infected hosts on the network.
Panorama High Availability

Panorama High Availability (HA) is a configuration in which two Panorama servers are placed in a group (two-firewall cluster) to provide redundancy in the event of a system or network failure. Panorama in HA provides continuity in the task of centrally administering and monitoring the firewalls to secure your network.

- Panorama HA Prerequisites
- Priority and Failover on Panorama in HA
- Failover Triggers
- Logging Considerations in Panorama HA
- Synchronization Between Panorama HA Peers
- Manage a Panorama HA Pair
Panorama HA Prerequisites

To configure Panorama in HA, you require a pair of identical Panorama servers with the following requirements on each:

- **The same form factor**—Must both be hardware-based appliances (M-Series appliances) or virtual appliances. The M-Series appliances must be the same model: both M-100 appliances or both M-500 appliances. For HA, the M-Series appliances must be in Panorama mode; M-Series appliances in Log Collector mode do not support HA.

- **The same Panorama OS version**—Must run the same Panorama version to synchronize configuration information and maintain parity for a seamless failover.

- **The same set of licenses**—Must have the same firewall management capacity license.

- **(Panorama virtual appliance only) Unique serial number**—Must have unique serial numbers; if the serial number is the same for both Panorama instances, they will be in suspended mode until you resolve the issue.

The Panorama servers in the HA configuration are peers and you can use either (active or passive) to centrally manage the firewalls and Log Collectors with a few exceptions (see Synchronization Between Panorama HA Peers). The HA peers use the management port to synchronize the configuration elements pushed to the managed firewalls and Log Collectors and to maintain state information. Typically, Panorama HA peers are geographically located in different sites, so you need to make sure that the management port IP address assigned to each peer is routable through your network. HA connectivity uses TCP port 28 with encryption enabled. If encryption is not enabled, ports 28769 and 28260 are used for HA connectivity and to synchronize configuration between the HA peers. We recommend less than 500ms latency between the peers. To determine the latency, use Ping during a period of normal traffic.
Priority and Failover on Panorama in HA

Each Panorama peer in the HA pair is assigned a priority value. The priority value of the primary or secondary peer determines which will be eligible for being the main point of administration and log management. The peer set as primary assumes the active state, and the secondary becomes passive. The active peer handles all the configuration changes and pushes them to the managed firewalls; the passive peer cannot make any configuration changes or push configuration to the managed firewalls. However, either peer can be used to run reports or to perform log queries.

The passive peer is synchronized and ready to transition to the active state if a path, link, system, or network failure occur on the active Panorama.

When a failover occurs, only the state (active or passive) of the Panorama peer changes; the priority (primary and secondary) does not. For example, when the primary peer fails, its status changes from active-primary to passive-primary.

A peer in the active-secondary state can perform all functions with two exceptions:

- It cannot manage firewall or Log Collector deployment functions such as license updates or software upgrades.
- It cannot log to an NFS until you manually change its priority to primary. (Panorama virtual appliance only)

The following table lists the capabilities of Panorama based on its state and priority settings:
<table>
<thead>
<tr>
<th>Capability</th>
<th>active-primary</th>
<th>passive-primary</th>
<th>active-secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch device context</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Perform distributed reporting</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Manage shared policy</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Log to local disk</td>
<td>✓</td>
<td>✓ (Optional on the Panorama virtual appliance only)</td>
<td>✓ (Optional on the Panorama virtual appliance only)</td>
</tr>
<tr>
<td>Log to an NFS partition</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(Panorama virtual appliance only)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deploy software and licenses</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Export Panorama configuration</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

For more information, see Panorama HA Prerequisites or Set Up HA on Panorama.
Failover Triggers

When a failure occurs on the active Panorama and the passive Panorama takes over the task of managing the firewalls, the event is called a failover. A failover is triggered when a monitored metric on the active Panorama fails. This failure transitions the state on the primary Panorama from active-primary to passive-primary, and the secondary Panorama becomes active-secondary.

The conditions that trigger a failover are:

- The Panorama peers cannot communicate with each other and the active peer does not respond to health and status polls; the metric used is HA Heartbeat Polling and Hello Messages.
  - When the Panorama peers cannot communicate with each other, the active one monitors whether the peers are still connected before a failover is triggered. This check helps in avoiding a failover and causing a split-brain scenario, where both Panorama peers are in an active state.
- One or more of the destinations (IP addresses) specified on the active peer cannot be reached; the metric used is HA Path Monitoring.

In addition to the failover triggers listed above, a failover also occurs when the administrator places the Panorama peer in a suspended state or when preemption occurs. Preemption is a preference for the primary Panorama to resume the active role after recovering from a failure (or user-initiated suspension). By default, preemption is enabled and when the primary Panorama recovers from a failure and becomes available, the secondary Panorama relinquishes control and returns to the passive state. When preemption occurs, the event is logged in the System log.

If you are logging to an NFS datastore, do not disable preemption because it allows the primary peer (that is mounted to the NFS) to resume the active role and write to the NFS datastore. For all other deployments, preemption is only required if you want to make sure that a specific Panorama is the preferred active peer.

HA Heartbeat Polling and Hello Messages

The HA peers use hello messages and heartbeats to verify that the peer is responsive and operational. Hello messages are sent from one peer to the other at the configured Hello Interval to verify the state of the other. The heartbeat is an ICMP ping to the HA peer, and the peer responds to the ping to establish that the peers are connected and responsive. By default, the interval for the heartbeat is 1000 milliseconds and 8000ms for hello messages.

HA Path Monitoring

Path monitoring checks the network connectivity and link state for an IP address or group of IP addresses (path group). The active peer uses ICMP pings to verify that one or more destination IP addresses can be reached. For example, you can monitor the availability of interconnected networking devices like a router or a switch, connectivity to a server, or some other vital device that is in the flow of traffic. Make sure that the node/device configured for monitoring is not likely to be unresponsive, especially when it comes under load, as this could cause a path monitoring failure and trigger a failover.
The default ping interval is 5000ms. An IP address is considered unreachable when three consecutive pings (the default value) fail, and a peer failure is triggered when any or all of the IP addresses monitored become unreachable. By default, if any one of the IP addresses becomes unreachable, the HA state transitions to non-functional.
Logging Considerations in Panorama HA

Setting up Panorama in an HA configuration provides redundancy for log collection. Because the managed firewalls are connected to both Panorama peers over SSL, when a state change occurs, each Panorama sends a message to the managed firewalls. The firewalls are notified of the Panorama HA state and can forward logs accordingly.

By default, when the managed firewalls cannot connect to Panorama (M-Series appliance and the Panorama virtual appliance), they buffer the logs; when the connection is restored, they resume sending logs from where it was last left off.

The logging options on the hardware-based Panorama and on the Panorama virtual appliance differ:
- Logging Failover on a Panorama Virtual Appliance
- Logging Failover on an M-Series Appliance

Logging Failover on a Panorama Virtual Appliance

On the Panorama virtual appliance, you have the following log failover options:

<table>
<thead>
<tr>
<th>Log Storage Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual disk</td>
<td>By default, the managed firewalls send logs as independent streams to each Panorama HA peer. By default, if a peer becomes unavailable, the managed firewalls buffer the logs and when the peer reconnects it resumes sending logs from where it had left off (subject to disk storage capacity and duration of the disconnection). Logging to a virtual disk provides redundancy in logging. However, the maximum log storage capacity is 8TB for Panorama running on VMware vCloud Air or ESXi 5.5 and later versions. The maximum capacity is 2TB for Panorama running on earlier ESXi versions. The option to forward logs only to the active peer is configurable (see Modify Log Forwarding and Buffering Defaults). However, Panorama does not support log aggregation across the HA pair. So, if you log to a virtual disk or local disk, for monitoring and reporting you must query the Panorama peer that collects the logs from the managed firewalls.</td>
</tr>
<tr>
<td>Network File System (NFS)</td>
<td>When configured to use an NFS, only the active-primary Panorama mounts to the NFS-based log partition and can receive logs. On failover, the primary device goes into a passive-primary state. In this scenario, until preemption occurs, the active-secondary Panorama manages the firewalls, but it does not receive the logs and it cannot write to the NFS. To allow the active-secondary peer to log to the NFS, you must manually switch it to primary so that it can mount to the NFS partition. For instructions, see Switch Priority after Panorama Failover to Resume NFS Logging.</td>
</tr>
</tbody>
</table>
Logging Failover on an M-Series Appliance

If you are using a pair of M-Series appliances (must be in Panorama mode), the managed firewalls can send logs to only one peer in the HA pair, either the active or the passive peer. Unlike the virtual Panorama deployment, you cannot configure the firewalls to send logs to both peers, however, the RAID-enabled disks on the M-Series appliance protect against disk failure and loss of logs.

If you have a distributed log collection set up where the managed firewalls are sending logs to a Dedicated Log Collector, the Panorama peers in HA will query all the managed Log Collectors for aggregated log information.

For more information, see Panorama HA Prerequisites or Set Up HA on Panorama.
Synchronization Between Panorama HA Peers

The Panorama HA peers synchronize the running configuration each time you commit changes on the active Panorama peer. The candidate configuration is synchronized between the peers each time you save the configuration on the active peer or just before a failover occurs.

Settings that are common across the pair, such as shared objects and policy rules, device group objects and rules, template configuration, certificates and SSL/TLS service profiles, and administrative access configuration, are synchronized between the Panorama HA peers.

The settings that are not synchronized are those that are unique to each peer, such as the following:

- Panorama HA configuration—Priority setting, peer IP address, path monitoring groups and IP addresses
- Panorama configuration—Management port IP address, FQDN settings, login banner, NTP server, time zone, geographic location, DNS server, permitted IP addresses for accessing Panorama, Simple Network Management Protocol (SNMP) system settings, and dynamic content update schedules
- Scheduled configuration exports
- NFS partition configuration and all disk quota allocation for logging
- Disk quota allocation for the different types of logs and databases on the Panorama local storage (SSD)

If you use a master key to encrypt the private keys and certificates on Panorama, you must use the same master key on both HA peers. If the master keys differ, Panorama cannot synchronize the HA peers.

For more information, see Panorama HA Prerequisites or Set Up HA on Panorama.
Manage a Panorama HA Pair

- Set Up HA on Panorama
- Test Panorama HA Failover
- Switch Priority after Panorama Failover to Resume NFS Logging
- Restore the Primary Panorama to the Active State

To install software or content updates, see Install Updates for Panorama in an HA Configuration.

Set Up HA on Panorama

Review the Panorama HA Prerequisites before performing the following steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Set up connectivity between the MGT ports on the HA peers.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Panorama peers communicate with each other using the MGT port. Make sure that the IP addresses you assign to the MGT port on the Panorama servers in the HA pair are routable and that the peers can communicate with each other across your network. To set up the MGT port, see Perform Initial Configuration of the Panorama Virtual Appliance or Perform Initial Configuration of the M-Series Appliance. Pick a Panorama peer in the pair and complete the remaining tasks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Enable HA and (optionally) enable encryption for the HA connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Select Panorama &gt; High Availability and edit the Setup section.</td>
</tr>
<tr>
<td></td>
<td>2. Select Enable HA.</td>
</tr>
<tr>
<td></td>
<td>3. In the Peer HA IP Address field, enter the IP address assigned to the peer Panorama.</td>
</tr>
<tr>
<td></td>
<td>4. In the Monitor Hold Time field, enter the length of time (milliseconds) that the system will wait before acting on a control link failure (range is 1000-60000, default is 3000).</td>
</tr>
<tr>
<td></td>
<td>5. If you do not want encryption, clear the Encryption Enabled check box and click OK: no more steps are required. If you do want encryption, select the Encryption Enabled check box, click OK, and perform the following tasks:</td>
</tr>
<tr>
<td></td>
<td>a. Select Panorama &gt; Certificate Management &gt; Certificates.</td>
</tr>
<tr>
<td></td>
<td>b. Select Export HA key. Save the HA key to a network location that the peer Panorama can access.</td>
</tr>
<tr>
<td></td>
<td>c. On the peer Panorama, navigate to Panorama &gt; Certificate Management &gt; Certificates, select Import HA key, browse to the location where you saved the key, and import it.</td>
</tr>
</tbody>
</table>
Step 3  Set the HA priority.

1. In Panorama > High Availability, edit the Election Settings section.
2. Define the Device Priority as Primary or Secondary. Make sure to set one peer as primary and the other as secondary. If both peers have the same priority setting, the peer with the higher serial number will be placed in a suspended state.
3. Define the Preemptive behavior. By default preemption is enabled. The preemption selection—enabled or disabled—must be the same on both peers.
   - If you are using an NFS for logging and you have disabled preemption, to resume logging to the NFS see Switch Priority after Panorama Failover to Resume NFS Logging.

Step 4  To configure path monitoring, define one or more path groups. The path group lists the destination IP addresses (nodes) that Panorama must ping to verify network connectivity.

Perform the following steps for each path group that includes the nodes that you want to monitor.

1. Select Panorama > High Availability and, in the Path Group section, click Add.
2. Enter a Name for the path group.
3. Select a Failure Condition for this group:
   - any triggers a path monitoring failure if any one of the IP addresses becomes unreachable.
   - all triggers a path monitoring failure only when none of the IP addresses are reachable.
4. Add each destination IP address you want to monitor.
5. Click OK. The Path Group section displays the new group.

Step 5  (Optional) Select the failure condition for path monitoring on Panorama.

1. Select Panorama > High Availability and edit the Path Monitoring section.
2. Select a Failure Condition:
   - all triggers a failover only when all monitored path groups fail.
   - any triggers a failover when any monitored path group fails.
3. Click OK.

Step 6  Save your configuration changes.

Click Commit, for the Commit Type select Panorama, and click Commit again.

Step 7  Configure the other Panorama peer.

Repeat Step 2 through Step 6 on the other peer in the HA pair.

Step 8  Verify that the Panorama servers are paired in HA.

After you configure both Panorama servers for HA:

1. Access the Dashboard on each Panorama, and view the High Availability widget.
2. Verify the Panorama servers are paired and synchronized:
   - Active Panorama—The state of the Local peer must be active and the Running Config must be synchronized.
   - Passive Panorama—The state of the Local peer must be passive and the Running Config must be synchronized.
Test Panorama HA Failover

To test that your HA configuration works properly, trigger a manual failover and verify that the peer transitions states successfully.

<table>
<thead>
<tr>
<th>Test Panorama HA Failover</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Log in to the active Panorama peer.</td>
<td>You can verify the state of the Panorama server in the bottom right corner of the web interface.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Suspend the active Panorama peer.</td>
<td>Select Panorama &gt; High Availability, and then click the Suspend local Panorama link in the Operational Commands section.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Verify that the passive Panorama peer has taken over as active.</td>
<td>On the Panorama Dashboard, High Availability widget, verify that the state of the Local passive server is active and the state of the Peer is suspended.</td>
</tr>
</tbody>
</table>
| **Step 4** Restore the suspended peer to a functional state. Wait for a couple minutes, and then verify that preemption has occurred, if preemptive is enabled. | On the Panorama you previously suspended:  
1. Select Panorama > High Availability and, in the Operational Commands section, click Make local Panorama functional.  
2. In the High Availability widget on the Dashboard, confirm that this (Local) Panorama has taken over as the active peer and that the other peer is now in a passive state. |

Switch Priority after Panorama Failover to Resume NFS Logging

The Panorama virtual appliance running on an ESXi server can use a Network File System (NFS) datastore for logging. In an HA configuration, only the primary Panorama peer is mounted to the NFS-based log partition and can write to the NFS. When a failover occurs and the passive Panorama becomes active, its state becomes active-secondary. Although a secondary Panorama peer can actively manage the firewalls, it cannot receive logs or write to the NFS because it does not own the NFS partition. When the firewalls cannot forward logs to the primary Panorama peer, each firewall writes the logs to its local disk. The firewalls maintain a pointer for the last set of log entries that they forwarded to Panorama so that when the passive-primary Panorama becomes available again, they can resume forwarding logs to it.

Use the instructions in this section to manually switch priority on the active-secondary Panorama peer so that it can begin logging to the NFS partition. The typical scenarios in which you might need to trigger this change are as follows:

- Preemption is disabled. By default, preemption is enabled on Panorama and the primary peer resumes as active when it becomes available again. When preemption is disabled, you need to switch the priority on the secondary peer to primary so that it can mount the NFS partition, receive logs from the managed firewalls, and write to the NFS partition.
- The active Panorama fails and cannot recover from the failure in the short term. If you do not switch the priority, when the maximum log storage capacity on the firewall is reached, the oldest logs will be overwritten to enable it to continue logging to its local disk. This situation can lead to loss of logs.

<table>
<thead>
<tr>
<th>Switch Priority after Panorama Failover to Resume NFS Logging</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Log in to the currently passive-primary Panorama, select Panorama &gt; Setup &gt; Operations and, in the Device Operations section, click Shutdown Panorama.</td>
<td></td>
</tr>
</tbody>
</table>
Panorama High Availability  Manage a Panorama HA Pair

Switch Priority after Panorama Failover to Resume NFS Logging

<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Log in to the active-secondary Panorama, select <strong>Panorama &gt; High Availability</strong>, edit the Election Settings, and set the <strong>Priority</strong> to <strong>Primary</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>OK</strong> and <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Panorama</strong>, and click <strong>Commit</strong> again. Do not reboot when prompted.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Log in to the <strong>Panorama CLI</strong> and enter the following command to change the ownership of the NFS partition to this peer: <code>request high-availability convert-to-primary</code></td>
</tr>
<tr>
<td>Step 5</td>
<td>Select <strong>Panorama &gt; Setup &gt; Operations</strong> and, in the Device Operations section, click <strong>Reboot Panorama</strong>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Power on the Panorama peer that you powered off in <strong>Step 1</strong>. This peer will now be in a passive-secondary state.</td>
</tr>
</tbody>
</table>

Restore the Primary Panorama to the Active State

By default, the preemptive capability on Panorama allows the primary Panorama to resume functioning as the active peer as soon as it becomes available. However, if preemption is disabled, the only way to force the primary Panorama to become active after recovering from a failure, a non-functional, or a suspended state, is by suspending the secondary Panorama peer.

Before the active-secondary Panorama goes into a suspended state, it transfers the candidate configuration to the passive Panorama so that all your uncommitted configuration changes are saved and can be accessed on the other peer.

Restore the Primary Panorama to the Active State

<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| Step 1 | **Suspend Panorama.**  
1. Log in to the Panorama peer that you want to place in a suspended state.  
2. Select **Panorama > High Availability**, and click the **Suspend local Panorama** link in the Operational Commands section. |
| Step 2 | Verify that the status indicates that the Panorama was suspended at user request.  
On the **Dashboard, High Availability** widget, verify that the **Local** state is **suspended**.  
A failover is triggered when you suspend a peer, and the other Panorama takes over as the active peer. |
| Step 3 | **Restore the suspended Panorama to a functional state.**  
1. In the **Panorama > High Availability** tab, Operational Commands section, click the **Make local Panorama functional** link.  
2. On the **Dashboard, High Availability** widget, confirm that the Panorama has transitioned to either the active or passive state. |
Administer Panorama

This section describes how to administer and maintain Panorama. It includes the following topics:

▲ Preview, Validate, or Commit Configuration Changes
▲ Manage Panorama and Firewall Configuration Backups
▲ Compare Changes in Panorama Configurations
▲ Manage Locks for Restricting Configuration Changes
▲ Add Custom Logos to Panorama
▲ Use the Panorama Task Manager
▲ Manage Storage Quotas and Expiration Periods for Logs and Reports
▲ Monitor Panorama
▲ Reboot or Shut Down Panorama
▲ Configure Panorama Password Profiles and Complexity

For instructions on completing initial setup, including defining network access settings, licensing, upgrading the Panorama software version, and setting up administrative access to Panorama, see Set Up Panorama.
You can preview, validate, and commit changes in the candidate configuration on Panorama or changes that Panorama pushes to managed firewalls and managed collectors. For details on the commit and validation processes, see Panorama Commit and Validation Operations.

### Preview, Validate, or Commit Configuration Changes

**Step 1** Select the target systems for the preview, validation, or commit operation.

As a best practice, commit changes to Panorama before committing changes to firewalls or Log Collectors.

1. Click **Commit** at the top of the web interface.
2. Select the **Commit Type**:
   - Panorama—Commit your changes to the Panorama configuration.
   - Template—Select the templates or template stacks from which Panorama will push device and network configurations to firewalls. Optionally, deselect firewalls that you want the commit to exclude.
   - Device Group—Select the device groups from which Panorama will push policies and objects to firewalls. Optionally, deselect firewalls and virtual systems that you want the commit to exclude.
   - Collector Group—Select the Collector Groups that contain the Log Collectors to which Panorama will push configurations.
3. Configure the options, which vary by **Commit Type**. You can enter a **Description** for all types. A brief summary of what changed in the configuration is useful to other administrators who want to know without performing a configuration audit.

**Step 2** (Panorama commit only) Optionally, preview the changes that the commit will activate before performing the commit. This can be useful if, for example, you don’t remember all the changes and you’re not sure you want to activate all of them.

Panorama displays the changes in a new window that shows the running and candidate configurations side by side, using colors to highlight the differences line by line.

1. Click **Preview Changes**.
2. Select the **Lines of Context**, which is the number of lines from the compared configuration files to display before and after the highlighted differences. These lines help you correlate the preview output to settings in the web interface.
   Because the preview results display in a new window, your browser must allow pop-up windows. If the preview window does not open, refer to your browser documentation for the steps to unblock pop-up windows.
3. Close the preview window when you finish reviewing the changes.

**Step 3** (Panorama, device group, or template commit only) Optionally, validate the changes before committing to ensure the commit will succeed.

1. Click **Validate Changes**. The results display all the errors and warnings that an actual commit would.
2. Resolve any errors that the validation results identify.

**Step 4** Commit your configuration changes.

Click **Commit**.

Use the Panorama Task Manager to see details about commits that are pending (optionally, you can cancel these), in progress, completed, or failed.
Manage Panorama and Firewall Configuration Backups

The running configuration on Panorama comprises all the settings that you have committed and that are therefore active. The candidate configuration is a copy of the running configuration plus any inactive changes that you made since the last commit. Backing up versions of the running or candidate configuration enables you to later restore those versions. For example, if a commit validation shows that the current candidate configuration has more errors than you want to fix, you can restore a previous candidate configuration or revert to the running configuration.

After a commit on a local firewall that runs PAN-OS 5.0 or later, a backup is sent of its running configuration to Panorama. Any commits performed on the local firewall will trigger the backup, including commits that an administrator performs locally on the firewall or automatic commits that PAN-OS initiates (such as an FQDN refresh). By default, Panorama stores up to 100 backups for each firewall, though this is configurable. To store Panorama and firewall configuration backups on an external host, you can schedule exports from Panorama or export on demand. You can also import configurations from firewalls into Panorama device groups and templates to Transition a Firewall to Panorama Management.

- Schedule Export of Configuration Files
- Back Up Panorama and Firewall Configurations
- Restore a Panorama Configuration
- Configure the Maximum Number of Configuration Backups on Panorama
- Load a Configuration Backup on a Managed Firewall

Schedule Export of Configuration Files

Panorama saves a backup of its running configuration as well as the running configurations of all managed firewalls. The backups are in XML format with file names that are based on serial numbers (of Panorama or the firewalls). Use these instructions to schedule daily exports of the backups to a remote host. Panorama exports the backups as a single gzip file. You require superuser privileges to schedule the export.

Schedule the Export of Configuration Files

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select Panorama &gt; Scheduled Config Export and click Add.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enter a Name and Description for the scheduled file export and Enable it.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Using the 24-hour clock format, enter a daily Scheduled Export Start Time or select one from the drop-down.</td>
</tr>
</tbody>
</table>
### Manage Panorama and Firewall Configuration Backups

#### Administer Panorama

#### Back Up Panorama and Firewall Configurations

Creating Panorama configuration backups enables you to later restore a Panorama Configuration. This is useful when you want to revert Panorama to all the settings of an earlier configuration; you can perform the restoration as a single operation instead of manually reconfiguring each setting in the current configuration.

As a best practice, back up any important configuration to a host external to Panorama.

When you commit changes, Panorama automatically saves a new version of the running configuration. If a system event or administrator action causes Panorama to reboot, it automatically reverts to the current version of the running configuration, which Panorama stores in a file named running-config.xml. However, Panorama does not automatically save the candidate configuration to persistent storage. You must manually save the candidate configuration as a default snapshot file (.snapshot.xml) or as a custom-named snapshot file.

### Schedule the Export of Configuration Files (Continued)

**Step 4** Set the export Protocol to Secure Copy (SCP) or File Transfer Protocol (FTP).

**Step 5** Enter the details for accessing the server, including: **Hostname** or IP address, **Port**, **Path** for uploading the file, **Username**, and **Password**.

The **Path** supports the following characters: . (period), +, { and }, /, -, _, 0-9, a-z, and A-Z. Spaces are not supported in the file **Path**.

If you are exporting to a BSD server, you will need to modify the SSHD password prompt to 

\(<username>@<hostname> <password>:\)

**Step 6** (SCP only) **Click Test SCP server connection.** To enable the secure transfer of data, you must verify and accept the host key of the SCP server. Panorama doesn't establish the connection until you accept the host key. If Panorama has an HA configuration, perform this step on each HA peer so that each one accepts the host key of the SCP server. If Panorama can successfully connect to the SCP server, it creates and uploads the test file named **ssh-export-test.txt**.

**Step 7** Click **OK** and **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.

---

### Back Up Panorama and Firewall Configurations

**Step 1** Save a snapshot of the candidate configuration if it contains changes that you want to preserve in the event Panorama reboots. Panorama stores the snapshot locally.

- To create or overwrite the default snapshot file (.snapshot.xml), click **Save** at the top of the web interface.
- To create a candidate configuration snapshot that does not overwrite the default snapshot:
  - Select **Panorama > Setup > Operations** and **Save named Panorama configuration snapshot**.
  - Enter a **Name** for the snapshot or select an existing snapshot to overwrite.
  - Click **OK** and **Close**.
Restoring a Panorama configuration overwrites the current candidate configuration with another configuration. This is useful when you want to revert Panorama to all the settings of an earlier configuration; you can perform the restoration as a single operation instead of manually reconfiguring each setting in the current configuration.

Panorama automatically saves a new version of the running configuration whenever you commit changes, and you can restore any of those versions. However, you must manually save a candidate configuration to later restore it (see Back Up Panorama and Firewall Configurations).

### Restore a Panorama Configuration

1. Select **Panorama > Setup > Operations** and **Revert to running Panorama configuration**.
2. Click **Yes** to confirm the operation.
**Manage Panorama and Firewall Configuration Backups**

**Administer Panorama**

**Configure the Maximum Number of Configuration Backups on Panorama**

<table>
<thead>
<tr>
<th>Configure the Number of Configuration Backups Panorama Stores</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Select <strong>Panorama &gt; Setup &gt; Management</strong> and edit the Logging and Reporting Settings.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Enter the <strong>Number of Versions for Config Backups</strong> (range is 1–1,048,576; default is 100).</td>
</tr>
<tr>
<td><strong>Step 3</strong> Click <strong>OK</strong> and <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Panorama</strong>, and click <strong>Commit</strong> again.</td>
</tr>
</tbody>
</table>

**Configure the Number of Configuration Backups Panorama Stores**

<table>
<thead>
<tr>
<th>Configure the Number of Configuration Backups Panorama Stores</th>
</tr>
</thead>
</table>

**Step 1** Select **Panorama > Setup > Operations** and **Revert to last saved Panorama configuration**.

**Step 2** Click **Yes** to confirm the operation.

**Step 3** (Optional) To overwrite the running configuration with the snapshot, click **Commit**, set the **Commit Type** to **Panorama**, and click **Commit** again.

**Configure the Maximum Number of Configuration Backups on Panorama**

<table>
<thead>
<tr>
<th>Configure the Maximum Number of Configuration Backups on Panorama</th>
</tr>
</thead>
</table>

**Step 1** Select **Panorama > Setup > Management** and edit the Logging and Reporting Settings.

**Step 2** Enter the **Number of Versions for Config Backups** (range is 1–1,048,576; default is 100).

**Step 3** Click **OK** and **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.

**Configure the Maximum Number of Configuration Backups on Panorama**

<table>
<thead>
<tr>
<th>Configure the Maximum Number of Configuration Backups Panorama Stores</th>
</tr>
</thead>
</table>

**Step 1** Select **Panorama > Setup > Operations** and **Revert to last saved Panorama configuration**.

**Step 2** Click **Yes** to confirm the operation.

**Step 3** (Optional) To overwrite the running configuration with the snapshot, click **Commit**, set the **Commit Type** to **Panorama**, and click **Commit** again.

**Configure the Maximum Number of Configuration Backups on Panorama**

<table>
<thead>
<tr>
<th>Configure the Maximum Number of Configuration Backups Panorama Stores</th>
</tr>
</thead>
</table>

**Step 1** Select **Panorama > Setup > Operations** and **Load Panorama configuration version**.

**Step 2** Select a configuration **Version** and click **OK**.

**Step 3** (Optional) To overwrite the running configuration with the version you just restored, click **Commit**, set the **Commit Type** to **Panorama**, and click **Commit** again.

**Configure the Maximum Number of Configuration Backups on Panorama**

<table>
<thead>
<tr>
<th>Configure the Maximum Number of Configuration Backups Panorama Stores</th>
</tr>
</thead>
</table>

**Step 1** Select **Panorama > Setup > Operations** and **Load named Panorama configuration snapshot**.

**Step 2** Select the snapshot **Name** and click **OK**.

**Step 3** (Optional) To overwrite the running configuration with the snapshot you just imported, click **Commit**, set the **Commit Type** to **Panorama**, and click **Commit** again.

**Configure the Maximum Number of Configuration Backups on Panorama**

<table>
<thead>
<tr>
<th>Configure the Maximum Number of Configuration Backups Panorama Stores</th>
</tr>
</thead>
</table>

**Step 1** Select **Panorama > Setup > Operations** and **Load named Panorama configuration snapshot**.

**Step 2** Select the snapshot **Name** of the configuration file you just imported, and click **OK**.

**Step 3** (Optional) To overwrite the running configuration with the snapshot you just imported, click **Commit**, set the **Commit Type** to **Panorama**, and click **Commit** again.
Load a Configuration Backup on a Managed Firewall

Use Panorama to load a configuration backup on a managed firewall. You can choose to revert to a previously saved or committed configuration on the firewall. Panorama pushes the selected version to the managed firewall, thereby overwriting the current candidate configuration on the firewall.

<table>
<thead>
<tr>
<th>Load a Configuration Backup on a Managed Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Select Panorama &gt; Managed Devices.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Select Manage in the Backups column.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Select from the Saved Configurations or Committed Configurations.</td>
</tr>
<tr>
<td>• Click a version number to view the contents of that version.</td>
</tr>
<tr>
<td>• <strong>Load</strong> a configuration version.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Click <strong>Commit</strong>, for the Commit Type select Panorama, and click <strong>Commit</strong> again.</td>
</tr>
</tbody>
</table>
Compare Changes in Panorama Configurations

To compare configuration changes on Panorama, you can select any two sets of configuration files: the candidate configuration, the running configuration, or any other configuration version that has been previously saved or committed on Panorama. The side-by-side comparison enables you to:

- Preview the configuration changes before committing them to Panorama. You can, for example, preview the changes between the candidate configuration and the running configuration. As a best practice, select the older version on the left pane and the newer version on the right pane, to easily compare and identify modifications.
- Perform a configuration audit to review and compare the changes between two sets of configuration files.

<table>
<thead>
<tr>
<th>Compare Changes in Panorama Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Choose Panorama &gt; Config Audit.</td>
</tr>
<tr>
<td>2. For each drop-down, select a configuration for the comparison.</td>
</tr>
<tr>
<td>3. Select the number of lines that you want to include for Context and click Go. Panorama uses color shading to highlight items you added (green), modified (yellow), or deleted (red).</td>
</tr>
</tbody>
</table>

| Configure the number of versions Panorama stores for configuration audits. |
| 1. Select Panorama > Setup > Management and edit the Logging and Reporting Settings. |
| 2. Enter the Number of Versions for Config Audit (range is 1–1,048,576; default is 100). |
| 3. Click OK and Commit, for the Commit Type select Panorama, and click Commit again. |

| View and compare Panorama configuration files before committing. |
| 1. Click Commit. |
| 2. Preview Changes. |
| 3. Select the number of lines of context you want to see, and click OK. |
Manage Locks for Restricting Configuration Changes

Locking the candidate or running configuration prevents other administrators from changing the configuration until you manually remove the lock or Panorama removes it automatically (after a commit). Locks ensure that administrators don't make conflicting changes to the same settings or interdependent settings during concurrent login sessions.

If you are changing settings that are unrelated to the settings other administrators are changing in concurrent sessions, you don’t need configuration locks to prevent commit conflicts. Panorama queues commit operations and performs them in the order that administrators initiate the commits. For details, see Panorama Commit and Validation Operations.

A template or device group commit will fail if a firewall assigned to the template or device group has a commit or config lock that an administrator set locally on that firewall.

### Manage Configuration Locks

- **View details about current locks.**
  For example, you can check whether other administrators have set locks and read comments they entered to explain the locks.
  
  **Click the locked padlock (🔒) at the top of the web interface.** The adjacent number indicates the number of current locks.

- **Lock a configuration.**
  Read-only administrators who cannot modify firewall or Panorama configurations cannot set locks.
  
  1. Click the padlock icon at the top of the web interface. The icon varies based on whether existing locks are (🔒) or are not (🔓) set.
  2. **Take a Lock** and select the lock **Type**:
     - **Config**—Blocks other administrators from changing the candidate configuration.
     - **Commit**—Blocks other administrators from changing the running configuration.
  3. Select the **Location** to determine the scope of the lock:
     - **Shared**— Restricts changes to the entire Panorama configuration, including all device groups and templates.
     - **Template**—Restricts changes to the firewalls included in the selected template. (You can’t take a lock for a template stack, only for individual templates within the stack.)
     - **Device group**—Restricts changes to the selected device group but not its descendant device groups.
  4. **(Optional)** As a best practice, enter a **Comment** to describe your reason for setting the lock.
  5. Click **OK** and **Close**.
Manage Configuration Locks (Continued)

- **Unlock a configuration.**
  
  Only a superuser or the administrator who locked the configuration can manually unlock it. However, Panorama automatically removes a lock after completing the commit operation that the administrator who set the lock initiated.
  
  1. Click the locked padlock (🔒) at the top of the web interface.
  2. Select the lock entry in the list.
  3. Click **Remove Lock**, **OK**, and **Close**.

- **Configure Panorama to automatically lock the running configuration when you change the candidate configuration. This setting applies to all Panorama administrators.**
  
  1. Select **Panorama > Setup > Management** and edit the General Settings.
  2. Select **Automatically Acquire Commit Lock** and then click **OK** and **Commit**.
Add Custom Logos to Panorama

You can upload image files to customize the following areas on Panorama:
- Background image on the login screen
- Header on the top left corner of the web interface; you can also hide the Panorama default background
- Title page and footer image in PDF reports

Supported image types include .jpg, .gif, and .png. Image files for use in PDF reports cannot contain an alpha channel. The size of the image must be less than 128 Kilobytes (131,072 bytes); the recommended dimensions are displayed on screen. If the dimension is larger than the recommended size, the image will be automatically cropped.

<table>
<thead>
<tr>
<th>Add Custom Logos to Panorama</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
</tr>
</tbody>
</table>
Use the Panorama Task Manager

Click Tasks at the bottom of the web interface to open the Task Manager, which displays details about all the operations that administrators initiated (for example, manual commits) or that Panorama or a managed firewall initiated (for example, scheduled report generation) since the last Panorama or firewall reboot. You can use the Task Manager to troubleshoot failed operations, investigate warnings associated with completed commits, or cancel pending commits.

## Use the Task Manager

### Step 1
Click Tasks.

### Step 2
Show the Running (in progress) tasks or All tasks (the default), optionally filter by type (Reports; Log Requests; or commit, download, and installation Jobs), and select Panorama (default) or the firewall for which you want to see the tasks.

### Step 3
Perform any of the following actions:

- **Display or hide task details**—By default, the Task Manager displays the Type, Status, Start Time, and Messages for each task. To see the End Time and Job ID for a task, you must manually display those columns. To display or hide a column, open the drop-down in any column header, select Columns, and select or clear the columns as desired.

- **Investigate warnings or failures**—Read the entries in the Messages column for task details. If the column says *Too many messages*, click the entry in the Type column to see more information.

- **Display a commit description**—If an administrator entered a description for a commit, click Commit Description in the Messages column to display it.

- **Check the position of a commit in the queue**—The Messages column indicates the queue position of commits that are in progress.

- **Cancel pending commits**—Clear Commit Queue to cancel all pending commits (available only to predefined administrative roles). To cancel an individual commit, click x in the Action column (the commit remains in the queue until Panorama dequeues it). You cannot cancel commits that are in progress.
Manage Storage Quotas and Expiration Periods for Logs and Reports

- Log and Report Storage
- Log and Report Expiration Periods
- Configure Storage Quotas and Expiration Periods for Logs and Reports

Log and Report Storage

You can edit the default storage quotas for each log type but not for reports. When a log quota reaches the maximum size, Panorama starts overwriting the oldest log entries with the new log entries. The Panorama virtual appliance and M-Series appliance have different locations for storing logs and different predefined storage capacities for reports:

- **Panorama virtual appliance**—Panorama writes all logs to its assigned storage space, which can be any of the following:
  - The approximately 11GB storage allocated by default on the virtual disk that you created when installing Panorama.
  - An additional virtual disk: see Add a Virtual Disk to Panorama on an ESXi Server or Add a Virtual Disk to Panorama in vCloud Air.
  - An NFS partition: see Mount the Panorama ESXi Server to an NFS Datastore.

The storage space for reports is 200MB.

- **M-Series appliance**—Panorama saves logs to its internal SSD and RAID-enabled disks. The M-Series appliance uses its internal SSD to store the Config logs and System logs that Panorama and its Log Collectors generate, and also to store the Application Statistics (App Stats) logs that Panorama automatically receives at 15 minute intervals from all managed firewalls. Panorama saves all other log types to its RAID-enabled disks. The RAID disks are either local to the M-Series appliance in Panorama mode or are in a Dedicated Log Collector (M-Series appliance in Log Collector mode). To edit the storage quotas for logs on the RAID disks, you must modify the Collector Group configuration. The storage space for reports is 500MB for Panorama 6.1 or later releases and 200 MB for earlier releases.

Log and Report Expiration Periods

You can configure automatic deletion based on time for the logs that the Panorama management server and Log Collectors collect from firewalls, as well as the logs and reports that Panorama and the Log Collectors generate locally. This is useful in deployments where periodically deleting monitored information is desired or necessary. For example, deleting user information after a certain period might be mandatory in your organization for legal reasons. You configure separate expiration periods for:

- Reports—Panorama deletes reports nightly at 2:00 a.m., when it generates scheduled reports.
- Each log type—Panorama evaluates logs as it receives them, and deletes logs that exceed the configured expiration period.
Manage Storage Quotas and Expiration Periods for Logs and Reports

- Each summary log type—Panorama evaluates logs after the various summary periods (hourly, daily, and weekly), and deletes logs that exceed the configured expiration period.

Weekly summary logs that fall short of the expiration threshold when log deletion occurs could age past the threshold before the next log deletion. For example, if you configure Traffic Summary logs to expire after 20 days and a weekly Traffic Summary log is 19 days old when Panorama deletes expired logs, then it doesn’t delete that log. The next time the Panorama checks for weekly logs to delete, 7 days later, that log will be 26 days old.

Panorama synchronizes expiration periods across high availability (HA) pairs. Because only the active HA peer generates logs, the passive peer has no logs or reports to delete unless failover occurs and it starts generating logs.

Even if you don’t set expiration periods, when a log quota reaches the maximum size, Panorama starts overwriting the oldest log entries with the new log entries.

Configure Storage Quotas and Expiration Periods for Logs and Reports

Configure Storage Quotas and Expiration Periods for Logs and Reports

| Step 1 | Configure the storage quotas and expiration periods for:
| Logs of all types that a Panorama virtual appliance receives from firewalls.
| App Stats logs that Panorama (a virtual appliance or M-Series appliance) receives from firewalls.
| System and Config logs that Panorama (a virtual appliance or M-Series appliance) and its Log Collectors generate locally.

The Panorama management server stores these logs.

| Step 2 | Configure the expiration period for reports that Panorama (a virtual appliance or M-Series appliance) generates.

1. Select Panorama > Setup > Management and edit the Logging and Reporting Settings.
2. In the Log Storage tab, enter the storage Quota (%) for each log type. When you change a percentage value, the page refreshes to display the corresponding absolute value (Quota GB/MB column) based on the total allotted storage on Panorama.
3. Enter the Max Days (expiration period) for each log type (range is 1-2,000). By default, the fields are blank, which means the logs never expire.

3. Click OK to save your changes.

To reset the quotas and expiration periods to the factory defaults, click Restore Quota Defaults at the bottom right of the dialog.
Administer Panorama

Manage Storage Quotas and Expiration Periods for Logs and Reports

| Step 3 | Configure the storage quotas and expiration periods for logs of all types (except App Stats logs) that a Panorama M-Series appliance receives from firewalls. The Log Collectors store these logs. You configure these storage quotas at the Collector Group level, not for individual Log Collectors. |
|        | 1. Select **Panorama > Collector Groups** and select the Collector Group.  
  2. In the **General** tab, click the **Log Storage** value. This field doesn’t display a value unless you assigned Log Collectors to the Collector Group. If the field displays 0MB after you assign Log Collectors, verify that you enabled the disk pairs when configuring the Log Collector and that you committed the changes (**Panorama > Managed Collectors > Disks**).  
  3. Enter the storage **Quota(%)** for each log type. When you change a percentage value, the page refreshes to display the corresponding absolute value (Quota GB/MB column) based on the total storage allotted to the Collector Group.  
  4. Enter the **Max Days** (expiration period) for each log type (range is 1–2,000). By default, the fields are blank, which means the logs never expire. To reset the quotas and expiration periods to the factory defaults, click **Restore Quota Defaults** at the bottom right of the dialog.  
  5. Click **OK** to save your changes. |

| Step 4 | Commit your changes.  
  1. Click **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.  
  2. (M-Series appliance only) Click **Commit**, for the **Commit Type** select **Collector Group**, select the Collector Group you modified, and click **OK**. |

| Step 5 | Verify that Panorama applied the storage quota changes.  
  1. Select **Panorama > Setup > Management** and, in the Logging and Reporting Settings, verify that the **Log Storage** values are correct for the logs that the Panorama management server stores.  
  2. Select **Panorama > Collector Groups**, select the Collector Group you modified, and verify that the **Log Storage** values in the **General** tab are correct for the logs that the Log Collectors store. You can also verify the Collector Group storage quotas by logging in to a Log Collector CLI and entering the operational command **show log-diskquota-pct**. |
Monitor Panorama

To monitor Panorama and its managed collectors, you can periodically view their System and Config logs (filter the logs), configure a Simple Network Management Protocol (SNMP) manager to collect (GET) Panorama statistics on a regular basis, or configure SNMP traps or email alerts that notify you when a monitored metric changes state or reaches a threshold on Panorama. Email alerts and SNMP traps are useful for immediate notification about critical system events that need your attention. To configure email alerts or SNMP traps, see Configure Log Forwarding from Panorama to External Destinations.

- Panorama System and Configuration Logs
- Monitor Panorama and Log Collector Statistics Using SNMP

Panorama System and Configuration Logs

You can configure Panorama to send notifications when a system event or configuration change occurs. By default, Panorama logs every configuration change to the Config logs. In the System logs, each event has a severity level to indicate its urgency and impact. When you Configure Log Forwarding from Panorama to External Destinations, you can forward all system events or just events of certain severity levels. The following table summarizes the severity levels:

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Indicates a failure and the need for immediate attention, such as a hardware failure, including high availability (HA) failover and link failures.</td>
</tr>
<tr>
<td>High</td>
<td>Serious issues that will impair the operation of the system, including disconnection of a Log Collector or a commit failure.</td>
</tr>
<tr>
<td>Medium</td>
<td>Mid-level notifications, such as Antivirus package upgrades, or a Collector Group commit.</td>
</tr>
<tr>
<td>Low</td>
<td>Minor severity notifications, such as user password changes.</td>
</tr>
<tr>
<td>Informational</td>
<td>Notification events such as log in or log out, any configuration change, authentication success and failure notifications, commit success, and all other events that the other severity levels don’t cover.</td>
</tr>
</tbody>
</table>

The M-Series appliance stores Config and System logs on its SSD. The Panorama virtual appliance stores the logs on the assigned storage volume (see Set Up the Panorama Virtual Appliance). If you need longer-term log storage for auditing, you can also Configure Log Forwarding from Panorama to External Destinations.

For information on using Panorama to monitor firewall logs, see Monitor Network Activity.
Monitor Panorama and Log Collector Statistics Using SNMP

You can configure an SNMP manager to request information from a Panorama management server and configure Panorama to respond. For example, the SNMP manager can request the high availability (HA) mode, Panorama state, and Panorama version. If the Panorama management server is an M-Series appliance in Panorama mode (not a virtual appliance), it can also provide logging statistics: average logs per second, storage duration of each log type, and log disk usage. Panorama doesn't synchronize SNMP configurations between HA peers; you must enable SNMP requests and responses on each peer.

You can also configure a Dedicated Log Collector (M-Series appliance in Log Collector mode) to respond to requests for statistics such as connection status, disk drive metrics, software version, average CPU, average logs per second, and log storage duration for each log type. This information is useful when evaluating whether you need to expand log storage capacity.

You can't configure an SNMP manager to control Panorama or Log Collectors (using SET messages); an SNMP manager can only collect statistics (using GET messages). For details on how Panorama implements SNMP, see SNMP Support.

<table>
<thead>
<tr>
<th>Monitor Panorama and Log Collector Statistics Using SNMP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Configure the SNMP Manager to get statistics from Panorama and the Log Collectors.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> Enable SNMP traffic on the management (MGT) interface of the Panorama management server.</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### Monitor Panorama and Log Collector Statistics Using SNMP (Continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
</table>
| **Step 3** | Enable SNMP traffic on the management (MGT) interface of any M-Series appliances in Log Collector mode. | 1. Select Panorama > Managed Collectors and select the Log Collector.  
2. Select the Management tab, select the SNMP check box, and click OK. |
| **Step 4** | Configure the Panorama management server to respond to statistics requests from an SNMP manager. | 1. Select Panorama > Setup > Operations and, in the Miscellaneous section, click SNMP Setup.  
2. Select the SNMP Version and configure the authentication values as follows. For version details, see SNMP Support.  
   - V2c—Enter the **SNMP Community String**, which identifies a community of SNMP managers and monitored devices (Panorama, in this case), and serves as a password to authenticate the community members to each other.  
     Don’t use the default community string **public**; it is well known and therefore not secure.  
   - V3—Create at least one SNMP view group and one user. User accounts and views provide authentication, privacy, and access control when SNMP managers get statistics.  
     - Views—Each view is a paired OID and bitwise mask: the OID specifies a MIB, and the mask (in hexadecimal format) specifies which objects are accessible inside (include matching) or outside (exclude matching) that MIB. Click Add in the first list and enter a **Name** for the group of views. For each view in the group, click Add and configure the view **Name**, **OID**, matching **Option** (include or exclude), and **Mask**.  
     - Users: Click Add in the second list, enter a username in the Users column, select the **View** group from the drop-down, enter the authentication password (**Auth Password**) used to authenticate to the SNMP manager, and enter the privacy password (**Priv Password**) used to encrypt SNMP messages to the SNMP manager.  
3. Click OK to save the settings. |
| **Step 5** | Configure the Dedicated Log Collectors (if any) to respond to SNMP requests. | For each Collector Group:  
1. Select Panorama > Collector Groups and select the Collector Group.  
2. Select the Monitoring tab, configure the same settings as in Step 4, and click OK. |
| **Step 6** | Commit your changes. | 1. Click Commit, for the Commit Type select Panorama, and click Commit again.  
2. Click Commit, for the Commit Type select Collector Group, select the Collector Groups you edited, and click Commit again. |
| **Step 7** | Monitor the Panorama and Log Collector statistics in an SNMP manager. | Refer to the documentation of your SNMP manager. |
Reboot or Shut Down Panorama

The reboot option initiates a graceful restart of Panorama. A shutdown halts the system and powers it off. To restart Panorama, after a shutdown, manually disconnect and re-cable the power cord on the system.

<table>
<thead>
<tr>
<th>Reboot or Shut Down Panorama</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Select Panorama &gt; Setup &gt; Operations.</td>
</tr>
<tr>
<td><strong>Step 2</strong> In the Device Operations section, select Reboot Panorama or Shutdown Panorama.</td>
</tr>
</tbody>
</table>
Configure Panorama Password Profiles and Complexity

To secure the local administrator account, you can define password complexity requirements that are enforced when administrators change or create new passwords. Unlike password profiles, which can be applied to individual accounts, the password complexity rules are firewall-wide and apply to all passwords.

To enforce periodic password updates, create a password profile that defines a validity period for passwords.

<table>
<thead>
<tr>
<th>Configure Panorama Password Profiles and Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Configure minimum password complexity settings.</td>
</tr>
<tr>
<td>1. Select <strong>Panorama &gt; Setup &gt; Management</strong> and edit the Minimum Password Complexity section.</td>
</tr>
<tr>
<td>2. Select <strong>Enabled</strong>.</td>
</tr>
<tr>
<td>3. Define the <strong>Password Format Requirements</strong>. You can enforce the requirements for uppercase, lowercase, numeric, and special characters that a password must contain.</td>
</tr>
<tr>
<td>4. To prevent the account username (or reversed version of the name) from being used in the password, select <strong>Block Username Inclusion (including reversed)</strong>.</td>
</tr>
<tr>
<td>5. Define the password <strong>Functionality Requirements</strong>. If you have configured a password profile for an administrator, the values defined in the password profile will override the values that you have defined in this section.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 2</strong> Create password profiles. You can create multiple password profiles and apply them to administrator accounts as required to enforce security.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Select <strong>Panorama &gt; Password Profiles</strong> and click <strong>Add</strong>.</td>
</tr>
<tr>
<td>2. Enter a <strong>Name</strong> for the password profile and define the following:</td>
</tr>
<tr>
<td>a. <strong>Required Password Change Period</strong>: Frequency, in days, at which the passwords must be changed.</td>
</tr>
<tr>
<td>b. <strong>Expiration Warning Period</strong>: Number of days before expiration that the administrator will receive a password reminder.</td>
</tr>
<tr>
<td>c. <strong>Post Expiration Grace Period</strong>: Number of days that the administrator can still log in to the system after the password expires.</td>
</tr>
<tr>
<td>d. <strong>Post Expiration Admin Login Count</strong>: Number of times that the administrator can log in to the system after the password has expired.</td>
</tr>
</tbody>
</table>
Troubleshooting

The following topics address Panorama issues:

- Troubleshoot Panorama System Issues
- Troubleshoot Log Storage and Connection Issues
- Replace an RMA Firewall
- Troubleshoot Commit Failures
- Troubleshoot Registration or Serial Number Errors
- Troubleshoot Reporting Errors
- View Task Success or Failure Status
Troubleshoot Panorama System Issues

- Generate Diagnostic Files for Panorama
- Diagnose Panorama Suspended State
- Monitor the File System Integrity Check
- Manage Panorama Storage for Software and Content Updates
- Recover from Split Brain in Panorama HA Deployments

Generate Diagnostic Files for Panorama

Diagnostic files aid in monitoring system activity and in discerning potential causes for issues on Panorama. To assist Palo Alto Networks Technical Support in troubleshooting an issue, the support representative might request a tech support file. The following procedure describes how to download a tech support file and upload it to your support case.

**Generate Diagnostic Files for Panorama**

**Step 1** Select Panorama > Support and click Generate Tech Support File.

**Step 2** Download and save the file to your computer.

**Step 3** Upload the file to your case on the Palo Alto Networks Customer Support web site.

Diagnose Panorama Suspended State

If Panorama is in a suspended state, check for the following conditions:

- Verify that the serial number on each Panorama virtual appliance is unique. If the same serial number is used to create two or more instances of Panorama, all instances using the same serial number will be suspended.

- Verify that you have set the HA priority setting on one peer as Primary and the other as Secondary. If the priority setting is identical on both peers, the Panorama peer with a higher numerical value in serial number is placed in a suspended state.

- Verify that both Panorama HA peers are running the same Panorama version (major and minor version number).

Monitor the File System Integrity Check

Panorama periodically performs a file system integrity check (FSCK) to prevent corruption of the Panorama system files. This check occurs after eight reboots or at a reboot that occurs 90 days after the last FSCK was executed. If Panorama is running a FSCK, the web interface and Secure Shell (SSH) login screens will display
Troubleshooting Troubleshoot Panorama System Issues

a warning to indicate that an FSCK is in progress. You cannot log in until this process completes. The time to complete this process varies by the size of the storage system; depending on the size, it can take several hours before you can log back in to Panorama.

To view the progress on the FSCK, set up console access to Panorama and view the status.

Manage Panorama Storage for Software and Content Updates

You can Install Content and Software Updates for Panorama and Deploy Updates to Firewalls and Log Collectors Using Panorama. You cannot configure the amount of space available on Panorama to store updates. When the allotted storage capacity reaches 90%, Panorama alerts you to free up space (delete stored updates) for new downloads or uploads. The maximum number of updates is a global setting that applies to all the updates that Panorama stores. You can use only the CLI to configure this setting. The default value is two updates of each type.

<table>
<thead>
<tr>
<th>Manage Panorama Storage for Software and Content Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Modify the maximum number of updates of each type.</td>
</tr>
<tr>
<td>Access the Panorama CLI and enter the following, where &lt;number&gt; can be between 2 and 64:</td>
</tr>
<tr>
<td>&gt; set max-num-images count &lt;number&gt;</td>
</tr>
<tr>
<td>• View the number of updates that Panorama currently stores.</td>
</tr>
<tr>
<td>Enter:</td>
</tr>
<tr>
<td>&gt; show max-num-images</td>
</tr>
<tr>
<td>• Use the web interface to delete updates to free up space on Panorama.</td>
</tr>
<tr>
<td>1. Select the type of update to delete:</td>
</tr>
<tr>
<td>• Firewall or Log Collector updates:</td>
</tr>
<tr>
<td>– PAN-OS/Panorama software images—Select Panorama &gt; Device Deployment &gt; Software.</td>
</tr>
<tr>
<td>– GlobalProtect agent/app software updates—Select Panorama &gt; Device Deployment &gt; GlobalProtect Client.</td>
</tr>
<tr>
<td>– Content updates—Select Panorama &gt; Device Deployment &gt; Dynamic Updates.</td>
</tr>
<tr>
<td>• Panorama software images—Select Panorama &gt; Software.</td>
</tr>
<tr>
<td>• Panorama content updates—Select Panorama &gt; Dynamic Updates.</td>
</tr>
<tr>
<td>2. Click the X icon in the far right column for the image or update.</td>
</tr>
<tr>
<td>• Use the CLI to delete updates to free up space on Panorama.</td>
</tr>
<tr>
<td>Delete software images by version:</td>
</tr>
<tr>
<td>&gt; delete software version &lt;version_number&gt;</td>
</tr>
<tr>
<td>Delete content updates:</td>
</tr>
<tr>
<td>&gt; delete content update &lt;filename&gt;</td>
</tr>
</tbody>
</table>

Recover from Split Brain in Panorama HA Deployments

When Panorama is configured in a high availability (HA) setup, the managed firewalls are connected to both the active and passive Panorama HA peers. When the connection between the active and the passive Panorama peers fails, before the passive Panorama takes over as the active peer it checks whether any firewall is connected to both the active and the passive peer. If even one firewall is connected to both peers, the failover is not triggered.
In the rare event that a failover is triggered when a set of firewalls are connected to the active peer and a set of firewalls are connected to the passive peer, but none of the firewalls are connected to both peers, it is called a split brain. When a split brain occurs, the following conditions occur:

- Neither Panorama peer is aware of the state nor the HA role of the other peer.
- Both Panorama peers become active and manage a unique set of firewalls.

To resolve a split brain, debug your network issues and restore connectivity between the Panorama HA peers.

However, if you need to make configuration changes to your firewalls without restoring the connection between the peers, here are a couple of options:

- Manually add the same configuration changes on both Panorama peers. This ensures that when the link is reestablished the configuration is synchronized.
- If you need to add/change the configuration at only one Panorama location, make the changes and synchronize the configuration (make sure that you initiate the synchronization from the peer on which you made the changes) when the link between the Panorama peers is re-established. To synchronize the peers, select the Dashboard tab and click the Sync to peer link in the High Availability widget.
- If you need to add/change the configuration for only the connected firewalls at each location, you can make configuration changes independently on each Panorama peer. Because the peers are disconnected, there is no replication and each peer now has a completely different configuration file (they are out of sync). Therefore, to ensure that the configuration changes on each peer are not lost when the connection is restored, you cannot allow the configuration to be automatically re-synchronized. To solve this problem, export the configuration from each Panorama peer and manually merge the changes using an external diff and merge tool. After the changes are integrated, you can import the unified configuration file on the primary Panorama and then synchronize the imported configuration file with the peer.
Troubleshoot Log Storage and Connection Issues

- Verify Panorama Port Usage
- Resolve Zero Log Storage for a Collector Group
- Replace a Failed Disk on an M-Series Appliance
- Replace the Virtual Disk on an ESXi Server
- Replace the Virtual Disk on vCloud Air
- Migrate Logs to a New M-Series Appliance in Log Collector Mode
- Migrate Logs to a New M-Series Appliance in Panorama Mode
- Migrate Log Collectors after Failure/RMA of Non-HA Panorama
- Regenerate Metadata for M-Series Appliance RAID Pairs

Verify Panorama Port Usage

To ensure that Panorama can communicate with managed firewalls, Log Collectors, and its high availability (HA) peer, use the following table to verify the ports that you must open on your network. Panorama uses TCP protocol for port communications.

<table>
<thead>
<tr>
<th>Communicating Systems &amp; Direction of Connection Establishment</th>
<th>Ports Used in Panorama 5.x</th>
<th>Ports Used in Panorama 6.x and later</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panorama and Panorama (HA) Direction: Each peer initiates its own connection to the other</td>
<td>28</td>
<td>28</td>
<td>For HA connectivity and synchronization if encryption is enabled.</td>
</tr>
<tr>
<td>Panorama and Panorama (HA) Direction: Each peer initiates its own connection to the other</td>
<td>28769 and 28260 (5.1) 28769 and 49160 (5.0)</td>
<td>28260 and 28769</td>
<td>For HA connectivity and synchronization if encryption is not enabled.</td>
</tr>
<tr>
<td>Panorama and managed firewalls Direction: Initiated by the firewall</td>
<td>3978</td>
<td>3978</td>
<td>A bi-directional connection where the logs are forwarded from the firewall to Panorama; and configuration changes are pushed from Panorama to the managed firewalls. Context switching commands are sent over the same connection.</td>
</tr>
</tbody>
</table>

On an M-Series appliance running Panorama 6.1 or later releases, you can optionally assign the log collection and Collector Group communication functions to the Eth1 or Eth2 interfaces (instead of to the default MGT interface). The ports listed in the following table apply regardless of which function you assign to which interface. For example, if you assign log collection to MGT and assign Collector Group communication to Eth2, then MGT will use port 3978 and Eth2 will use port 28270. (The Panorama virtual appliance can only use the MGT interface for all these functions.)
Troubleshoot Log Storage and Connection Issues

Resolve Zero Log Storage for a Collector Group

The log storage capacity for the Collector Group might display as 0MB if the disk pairs are not enabled for logging in the Log Collectors. To enable the disk pairs:

<table>
<thead>
<tr>
<th>Communicating Systems &amp; Direction of Connection Establishment</th>
<th>Ports Used in Panorama 5.x</th>
<th>Ports Used in Panorama 6.x and later</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panorama and Log Collector Direction: Initiated by the Log Collector</td>
<td>3978</td>
<td>3978</td>
<td>For management and log collection/reporting. Used for communication between the default Log Collector on a Panorama in Panorama mode, and for communicating with Log Collectors in a distributed log collection deployment.</td>
</tr>
<tr>
<td>Log Collector to Log Collector Direction: Each Log Collector initiates a connection to the other Log Collectors in the Collector Group</td>
<td>49190</td>
<td>28270</td>
<td>For distributing blocks and all binary data between Log Collectors.</td>
</tr>
</tbody>
</table>

**Resolve Zero Log Storage for a Collector Group**

Step 1 Select Panorama > Managed Collectors and edit each Log Collector in the Collector Group as follows.

Step 2 Select Disks and Add each RAID disk pair.

Step 3 Click OK and Commit, set the Commit Type to Panorama, and click Commit again.

Step 4 Click OK and Commit, set the Commit Type to Collector Group, select the Collector Group, and click Commit again.

Step 5 Select Panorama > Managed Collectors and verify that the configuration of each Log Collector is synchronized with Panorama. The Configuration Status column should display In Sync and the Run Time Status column should display connected.

Step 6 Click Statistics in the last column for each Log Collector and verify that the disk pairs are Enabled and Available.

Replace a Failed Disk on an M-Series Appliance

If a disk fails on the M-Series appliance, you must replace the disk and reconfigure it in a RAID 1 array. For details, refer to the M-100 or M-500 appliance Hardware Reference Guide.
Troubleshooting Troubleshoot Log Storage and Connection Issues

Replace the Virtual Disk on an ESXi Server

You can't resize a virtual disk after adding it to a Panorama virtual appliance running on a VMware ESXi server. Because the Panorama virtual appliance allows only one log storage location, you must replace the virtual disk to modify the log storage capacity.

You will lose the logs on the existing disk when you replace it. One way to preserve the logs is to set up a new Panorama virtual appliance for the new disk (see Set Up the Panorama Virtual Appliance) and maintain access to the Panorama containing the old disk for as long as you need its logs. A second way to preserve the logs is to copy them from the old disk to the new disk. Copying can take several hours, depending on how many logs the disk currently stores, and Panorama cannot collect logs during the process. Contact Palo Alto Networks Customer Support for instructions on how to copy logs between disks. A third way to preserve existing logs is to Configure Log Forwarding from Panorama to External Destinations before you replace the virtual disk.

<table>
<thead>
<tr>
<th>Replace the Virtual Disk on an ESXi Server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Remove the old virtual disk.</td>
</tr>
<tr>
<td>1. Access the VMware vSphere Client and select the <strong>Virtual Machines</strong> tab.</td>
</tr>
<tr>
<td>2. Right-click the Panorama virtual appliance and select <strong>Power &gt; Power Off</strong>.</td>
</tr>
<tr>
<td>3. Right-click the Panorama virtual appliance and select <strong>Edit Settings</strong>.</td>
</tr>
<tr>
<td>4. Select the virtual disk in the <strong>Hardware</strong> tab and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td>5. Select one of the Removal Options and click <strong>OK</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Add the new virtual disk.</td>
</tr>
<tr>
<td>1. <strong>Add a Virtual Disk to Panorama on an ESXi Server</strong>.</td>
</tr>
<tr>
<td>Panorama running on ESXi 5.5 and later versions supports a virtual disk of up to 8TB. Panorama running on an earlier ESXi version supports a virtual disk of up to 2TB.</td>
</tr>
<tr>
<td>2. In the vSphere Client, right-click the Panorama virtual appliance and select <strong>Power &gt; Power On</strong>.</td>
</tr>
<tr>
<td>The reboot process might take several minutes and the message <strong>cache data unavailable</strong> will display.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Verify that the modified log storage capacity is correct.</td>
</tr>
<tr>
<td>1. Log in to the Panorama virtual appliance.</td>
</tr>
<tr>
<td>2. Select <strong>Panorama &gt; Setup &gt; Management</strong> and verify that the Logging and Reporting Settings section, Log Storage field, displays the modified log storage capacity accurately.</td>
</tr>
</tbody>
</table>

Replace the Virtual Disk on vCloud Air

You can’t resize a virtual disk after adding it to a Panorama virtual appliance running on VMware vCloud Air. Because the Panorama virtual appliance allows only one log storage location, you must replace the virtual disk to modify the log storage capacity.
You will lose the logs on the existing disk when you replace it. One way to preserve the logs is to set up a new Panorama virtual appliance for the new disk (see Set Up the Panorama Virtual Appliance) and maintain access to the Panorama containing the old disk for as long as you need its logs. A second way to preserve the logs is to copy them from the old disk to the new disk. Copying can take several hours, depending on how many logs the disk currently stores, and Panorama cannot collect logs during the process. Contact Palo Alto Networks Customer Support for instructions on how to copy logs between disks. A third way to preserve existing logs is to Configure Log Forwarding from Panorama to External Destinations before you replace the virtual disk.

<table>
<thead>
<tr>
<th>Replace the Virtual Disk on vCloud Air</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Remove the old virtual disk.</td>
</tr>
<tr>
<td>1. Access the vCloud Air web console and select your Virtual Private Cloud OnDemand region.</td>
</tr>
<tr>
<td>2. Select the Panorama virtual appliance in the Virtual Machines tab.</td>
</tr>
<tr>
<td>3. Select Actions &gt; Edit Resources.</td>
</tr>
<tr>
<td>4. Click x for the virtual disk you are removing.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Add the new virtual disk.</td>
</tr>
<tr>
<td>1. Add another disk.</td>
</tr>
<tr>
<td>2. Set the Storage to up to 8TB and set the storage tier to Standard or SSD-Accelerated.</td>
</tr>
<tr>
<td>3. Save your changes.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Reboot Panorama.</td>
</tr>
<tr>
<td>1. Log in to the Panorama virtual appliance.</td>
</tr>
<tr>
<td>2. Select Panorama &gt; Setup &gt; Operations and Reboot Panorama.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Verify that the modified log storage capacity is correct.</td>
</tr>
<tr>
<td>1. Log in to the Panorama virtual appliance after it reboots.</td>
</tr>
<tr>
<td>2. Select Panorama &gt; Setup &gt; Management and verify that the Logging and Reporting Settings section, Log Storage field, displays the modified log storage capacity accurately.</td>
</tr>
</tbody>
</table>

Migrate Logs to a New M-Series Appliance in Log Collector Mode

If you need to replace an M-Series appliance in Log Collector mode (Dedicated Log Collector), you can migrate the logs it collected from firewalls by moving its RAID disks to a new M-Series appliance. This enables you to recover logs after a system failure on the M-Series appliance or to migrate logs as part of a hardware upgrade (from an M-100 appliance to an M-500 appliance). This procedure applies whether the Panorama management server that manages the Dedicated Log Collector is a Panorama virtual appliance or an M-Series appliance in Panorama mode.
Migrate Logs to a New M-Series Appliance in Log Collector Mode

**Step 1** Perform initial setup of the new M-Series appliance that will be a Dedicated Log Collector.

1. Rack mount the M-Series appliance. Refer to the M-100 or M-500 Appliance Hardware Reference Guide for instructions.

2. **Perform Initial Configuration of the M-Series Appliance.**

   When configuring interfaces, configure only the Management (MGT) interface. Switching to Log Collector mode later in this procedure removes any Eth1 and Eth2 interface configurations. If the Log Collector will use Eth1 and Eth2, add them when setting up the Log Collector later in this procedure.

3. **Register Panorama.**

4. Transfer licenses as follows only if the new M-Series appliance is the same hardware model as the old M-Series appliance. Otherwise, you must purchase new licenses.
   b. Select the **Assets** tab and click the **Spares** link.
   c. Click the Serial Number of the new M-Series appliance.
   d. Click **Transfer Licenses**.
   e. **Select** the old M-Series appliance and click **Submit**.

5. **Activate a Panorama Support License.**

6. **Activate a firewall management license.** If you are migrating from an M-100 appliance to an M-500 appliance, enter the auth-code associated with the migration license.

7. **Install Content and Software Updates for Panorama.**

   The M-500 appliance requires Panorama 7.0 or a later release. For important details about software versions, see [Panorama, Log Collector, and Firewall Version Compatibility](https://www.paloaltonetworks.com/support).

8. Switch from Panorama mode to Log Collector mode:
   a. Access the Log Collector CLI and switch to Log Collector mode:
      
      ```
      > request system system-mode logger
      ```
      b. Enter **Y** to confirm the mode change. The M-Series appliance reboots. If the reboot process terminates your terminal emulation software session, reconnect to the M-Series appliance to display the Panorama login prompt.
      
      If you see a CMS Login prompt, press Enter without typing a username or password.

9. Use the Log Collector CLI to enable connectivity between the Log Collector and Panorama management server. `<IPaddress1>` is for the MGT interface of the primary Panorama and `<IPaddress2>` is for the MGT interface of the secondary Panorama.
   
   ```
   > configure
   # set deviceconfig system panorama-server
   <IPaddress1> panorama-server-2 <IPaddress2>
   # commit
   # exit
   ```
### Troubleshoot Log Storage and Connection Issues

#### Migrate Logs to a New M-Series Appliance in Log Collector Mode (Continued)

| Step 2 | 1. Configure the Log Collector as a managed collector using the Panorama web interface or using the following CLI commands:  
|        |   > configure  
|        |   # set log-collector <LC_serial_number> deviceconfig  
|        |   system hostname <LC_hostname>  
|        |   # exit  
|        |   If the old Log Collector used the Eth1 and Eth2 interfaces for log collection and Collector Group communication, you must define those interfaces on the new Log Collector when you configure it as a managed collector (Panorama > Managed Collectors > Eth1 and Eth2).  
|        | 2. Verify that the Log Collector is connected to Panorama and that the status of its disk pairs is present/available.  
|        |   > show log-collector serial-number <log-collector_SN>  
|        |   The disk pairs will display as disabled at this stage of the restoration process.  
|        | 3. Commit your changes to Panorama. Don't commit the changes to the Collector Group just yet.  
|        |   > configure  
|        |   # commit  
|        |   # exit  
|        |  

| Step 3 | Remove the RAID disks from the old Log Collector.  
|        | 1. Power off the old Log Collector by pressing the Power button until the system shuts down.  
|        | 2. Remove the disk pairs. For details, refer to the disk replacement procedure in the M-100 or M-500 Appliance Hardware Reference Guide.  

| Step 4 | Insert the RAID disks in to the new Log Collector.  
|        | 1. Power off the new Log Collector by pressing the Power button until the system shuts down.  
|        | 2. Insert the disks into the new Log Collector. For details, refer to the disk replacement procedure in the M-100 or M-500 Appliance Hardware Reference Guide.  
|        | The disk carriers of the M-100 appliance are incompatible with those of the M-500 appliance. Therefore, when migrating between these hardware models, you must unscrew each disk from its old carrier and insert the disk in the new carrier before inserting the disk in the new appliance.  
|        | You must maintain the disk pair association. Although you can place a disk pair from slot A1/A2 on the old appliance into slot B1/B2 on the new appliance, you must keep the disks together in the same slot; otherwise, Panorama might not restore the data successfully.  
|        | 3. Power on the new Log Collector by pressing the Power button.
### Migrate Logs to a New M-Series Appliance in Log Collector Mode (Continued)

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Copy log file data from the to the new M-Series appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Contact <a href="https://www.paloaltonetworks.com/support">Palo Alto Networks Support</a> to copy log file data from the decommissioned M-Series appliance to the new M-Series appliance and restart the configd process.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Prepare the disks for migration.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Generate the metadata for each disk pair rebuilds the indexes. Therefore, depending on the data size, this process can take a long time to complete. To expedite the process, you can launch multiple CLI sessions and run the metadata regeneration command in each session to complete the process simultaneously for every pair. For details, see <a href="https://www.paloaltonetworks.com/support">Regenerate Metadata for M-Series Appliance RAID Pairs</a>.</td>
</tr>
</tbody>
</table>

1. Enable the disk pairs by running the following CLI command for each pair:
   - `request system raid add <slot> force no-format`
   - For example:
   - `request system raid add A1 force no-format`
   - `request system raid add A2 force no-format`
   - The `force` and `no-format` arguments are required. The `force` argument associates the disk pair with the new Log Collector. The `no-format` argument prevents reformatting of the drives and retains the logs stored on the disks.

2. Generate the metadata for each disk pair.
   - `request metadata-regenerate slot <slot_number>`
   - For example:
   - `request metadata-regenerate slot 1`

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Migrate the logs.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>You must use the Panorama CLI for this step, not the web interface.</td>
</tr>
</tbody>
</table>

You must assign the new Log Collector to the Collector Group that contains the old Log Collector.

1. Assign the new Log Collector to the Collector Group and commit your changes to Panorama.
   - `configure`
   - `# set log-collector-group <collector_group_name>
     logfwd-setting collectors <new_LC_serial_number>
     # commit
     # exit`

2. For each disk pair, migrate the logs from the old Log Collector to the new Log Collector and attach the disk pair to the new Log Collector.
   - `request log-migration from <old_LC_serial_number> old-disk-pair <log_disk_pair> to <new_LC_serial_number> new-disk-pair <log_disk_pair>`
   - For example:
   - `request log-migration from 003001000010 old-disk-pair A to 00300100038 new-disk-pair A`
## Migrate Logs to a New M-Series Appliance in Log Collector Mode (Continued)

**Step 8** Reconfigure the Collector Group.

1. Use the web interface to assign the new Log Collector to the firewalls that forward logs (Panorama > Collector Groups > Device Log Forwarding). Give the new Log Collector the same priority in the firewall preference lists as the old Log Collector. You use the web interface to perform this step because no CLI command can change the priority assignments of firewall preference lists.

2. Delete the old Log Collector from the Collector Group.
   ```
   > configure
   # delete log-collector-group <group_name>
   logfwd-setting collectors <old_LC_serial_number>
   ```
   For example:
   ```
   # delete log-collector-group DC-Collector-Group
   logfwd-setting collectors 003001000010
   ```

3. Delete the old Log Collector from the Panorama configuration and commit your changes to Panorama.
   ```
   # delete log-collector <old_LC_serial_number>
   # commit
   # exit
   ```

4. Commit the Collector Group changes so that the managed firewalls can send logs to the new Log Collector.
   ```
   > commit-all log-collector-config
   log-collector-group <collector_group_name>
   ```
   For example:
   ```
   > commit-all log-collector-config
   log-collector-group DC-Collector-Group
   ```

---

## Migrate Logs to a New M-Series Appliance in Panorama Mode

If you need to replace an M-Series appliance in Panorama mode (Panorama management server), you can migrate the logs it collected from firewalls by moving its RAID disks to a new M-Series appliance. Moving the disks enables you to recover logs after a system failure on the M-Series appliance or to migrate logs as part of a hardware upgrade (from an M-100 appliance to an M-500 appliance).

This migration procedure covers the following scenarios:

- One Panorama HA peer has a **managed collector (Log Collector) in a Collector Group**.
Both Panorama HA peers have managed collectors that belong to a single Collector Group. For details, see Figure: Multiple Default Log Collectors Per Collector Group.

Both Panorama HA peers have a managed collector and each is assigned to a separate Collector Group. For details, see Figure: Single Default Log Collector Per Collector Group.

### Migrate Logs to a New M-Series Appliance in Panorama Mode

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Forward any logs on the SSD of the old M-Series appliance to an external destination if you want to preserve them. The SSD stores only the System and Config logs that Panorama and Log Collectors generate. You cannot move the SSD between M-Series appliances.</td>
<td>Configure Log Forwarding from Panorama to External Destinations.</td>
</tr>
</tbody>
</table>
| Step 2 | Export the Panorama configuration from the decommissioned M-Series appliance in Panorama mode. | 1. Log in to the Panorama appliance and select **Panorama > Setup > Operations**.  
2. Click **Save named Panorama configuration snapshot**, enter a **Name** to identify the configuration, and click **OK**.  
3. Click **Export named Panorama configuration snapshot**, select the **Name** of the configuration you just saved, and click **OK**. Panorama exports the configuration to your client system as an XML file. |
| Step 3 | Remove the RAID disks from the old M-Series appliance. | 1. Power off the old M-Series appliance by pressing the Power button until the system shuts down.  
2. Remove the disk pairs. For details, refer to the disk replacement procedure in the **M-100 or M-500 Appliance Hardware Reference Guide**. |
## Migrate Logs to a New M-Series Appliance in Panorama Mode (Continued)

### Step 4
Perform initial setup of the new M-Series appliance.

1. Rack mount the M-Series appliance. Refer to the M-100 or M-500 Appliance Hardware Reference Guide for instructions.
2. Perform Initial Configuration of the M-Series Appliance.
3. Register Panorama.
4. Transfer licenses as follows only if the new M-Series appliance is the same hardware model as the old M-Series appliance. Otherwise, you must purchase new licenses.
   a. Log in to the Palo Alto Networks Customer Support web site.
   b. Select the Assets tab and click the Spares link.
   c. Click the Serial Number of the new M-Series appliance.
   d. Click Transfer Licenses.
   e. Select the old M-Series appliance and click Submit.
5. Activate a Panorama Support License.
6. Activate a firewall management license. If you are migrating from an M-100 appliance to an M-500 appliance, enter the auth-code associated with the migration license.
7. Install Content and Software Updates for Panorama.
   - The M-500 appliance requires Panorama 7.0 or a later release. For important details about software versions, see Panorama, Log Collector, and Firewall Version Compatibility.
8. Set the HA priority. The new M-Series appliance must have the same priority as the HA peer you are replacing.

### Step 5
Load the Panorama configuration snapshot that you exported from the decommissioned M-Series appliance into the new M-Series appliance in Panorama mode.

1. Log in to the new M-Series appliance and select Panorama > Setup > Operations.
2. Click Import named Panorama configuration snapshot, Browse to the configuration file you exported from the decommissioned M-Series appliance, and click OK.
3. Click Load named Panorama configuration snapshot, select the Name of the configuration you just imported, select a Decryption Key (the master key for Panorama), and click OK. Panorama overwrites its current candidate configuration with the loaded configuration. Panorama displays any errors that occur when loading the configuration file. If errors occurred, save them to a local file. Resolve each error to ensure the migrated configuration is valid.
4. Perform any additional configuration changes as needed.
   - If the old M-Series appliance used the Eth1 and Eth2 interfaces for log collection and Collector Group communication, you must define those interfaces on the new M-Series appliance (Panorama > Setup > Management).
5. Select Commit > Commit to Panorama and Validate Commit. Resolve any errors before proceeding.
6. Commit your changes to the Panorama configuration.
### Migrate Logs to a New M-Series Appliance in Panorama Mode (Continued)

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Insert the RAID disks in to the new M-Series appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Power off the new M-Series appliance by pressing the Power button until the system shuts down.</td>
</tr>
<tr>
<td></td>
<td>2. Insert the disks into the new M-Series appliance. For details, refer to the disk replacement procedure in the M-100 or M-500 Appliance Hardware Reference Guide.</td>
</tr>
<tr>
<td></td>
<td>The disk carriers of the M-100 appliance are incompatible with those of the M-500 appliance. Therefore, when migrating between these hardware models, you must unscrew each disk from its old carrier and insert the disk in the new carrier before inserting the disk in the new appliance.</td>
</tr>
<tr>
<td></td>
<td>You must maintain the disk pair association. Although you can place a disk pair from slot A1/A2 on the old appliance into slot B1/B2 on the new appliance, you must keep the disks together in the same slot; otherwise, Panorama might not restore the data successfully.</td>
</tr>
<tr>
<td></td>
<td>3. Power on the new M-Series appliance by pressing the Power button.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Copy log file data from the to the new M-Series appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Contact <a href="https://www.paloaltonetworks.com/support">Palo Alto Networks Support</a> to copy log file data from the decommissioned M-Series appliance to the new M-Series appliance and restart the mgmtsrvr process.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Prepare the disks for migration.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Enable the disk pairs by running the following CLI command for each pair:</td>
</tr>
<tr>
<td></td>
<td>&gt; request system raid add &lt;slot&gt; force no-format</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>&gt; request system raid add A1 force no-format</td>
</tr>
<tr>
<td></td>
<td>&gt; request system raid add A2 force no-format</td>
</tr>
<tr>
<td></td>
<td>The <code>force</code> and <code>no-format</code> arguments are required. The <code>force</code> argument associates the disk pair with the new appliance. The <code>no-format</code> argument prevents reformating of the drives and retains the logs stored on the disks.</td>
</tr>
<tr>
<td></td>
<td>2. Generate the metadata for each disk pair.</td>
</tr>
<tr>
<td></td>
<td>&gt; request metadata-regenerate slot &lt;slot_number&gt;</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>&gt; request metadata-regenerate slot 1</td>
</tr>
<tr>
<td></td>
<td>3. Synchronize the configuration of the M-Series appliance HA peers.</td>
</tr>
<tr>
<td></td>
<td>&gt; request high-availability sync-to-remote running-config</td>
</tr>
</tbody>
</table>
### Migrate Logs to a New M-Series Appliance in Panorama Mode (Continued)

#### Step 9
Configure the local Log Collector on the new M-Series appliance.

- **Warning:** For all steps with commands that require a serial number, you must type the entire serial number; pressing the Tab key won’t complete a partial serial number. Don’t enable the disks on the new M-Series appliance at this point. When you successfully migrate the logs, Panorama automatically enables the disks.

1. **Configure the local Log Collector as a managed collector using the Panorama web interface or using the following CLI commands:**
   ```
   configure
   > set log-collector <log-collector_SN> deviceconfig system hostname <log-collector-hostname>
   > exit
   ```
2. **Verify that the local Log Collector is connected to Panorama and that the status of its disk pairs is present/available.**
   ```
   > show log-collector serial-number <log-collector_SN>
   ```
   The disk pairs will display as disabled at this stage of the restoration process.
3. **Commit your changes to Panorama. Don’t commit the changes to the Collector Group just yet.**
   ```
   > configure
   > commit
   ```

#### Step 10
Migrate the logs.

- **Warning:** You must use the Panorama CLI for this step, not the web interface.

You must assign the local Log Collector of the new M-Series appliance to the Collector Group that contains the local Log Collector of the old M-Series appliance.

1. **Add the new local Log Collector as a member of the Collector Group and commit your changes to Panorama.**
   ```
   > set log-collector-group <collector_group_name> logfwd-setting collectors <SNManaged_collector>
   > commit
   > exit
   ```
   The old local Log Collector still appears in the list of members, because you didn’t yet delete it from the configuration.
2. **For each disk pair, migrate the logs to the new appliance.**
   ```
   > request log-migration from <old_LC_serial_number> old-disk-pair <log_disk_pair> to <new_LC_serial_number> new-disk-pair <log_disk_pair>
   ```
   For example:
   ```
   > request log-migration from 003001000010 old-disk-pair A to 00300100038 new-disk-pair A
   ```
3. **Commit the changes to Panorama.**
   ```
   > configure
   > commit
   ```
## Migrate Logs to a New M-Series Appliance in Panorama Mode (Continued)

### Step 11 Reconfigure the Collector Group.

1. **Use the web interface to assign the new Log Collector to the firewalls** that forward logs (**Panorama > Collector Groups > Device Log Forwarding**). Give the new Log Collector the same priority in the firewall preference lists as the old Log Collector.

   ![Note]
   You use the web interface to perform this step because no CLI command can change the priority assignments of firewall preference lists.

2. **Delete the old Log Collector from the Collector Group.**
   
   ```
   # delete log-collector-group <group_name> logfwd-setting collectors <old_LC_serial_number>
   ```
   
   For example:
   ```
   # delete log-collector-group DC-Collector-Group logfwd-setting collectors 003001000010
   ```

3. **Delete the old Log Collector from the Panorama configuration and commit your changes to Panorama.**
   
   ```
   # delete log-collector <old_LC_serial_number>
   # commit
   # exit
   ```

4. **Commit the Collector Group changes so that the managed firewalls can send logs to the new Log Collector.**
   
   ```
   > commit-all log-collector-config log-collector-group <collector_group_name>
   ```
   
   For example:
   ```
   > commit-all log-collector-config log-collector-group DC-Collector-Group
   ```

### Migrate Log Collectors after Failure/RMA of Non-HA Panorama

If a system failure occurs on a Panorama management server that is not deployed in a high availability (HA) configuration, use this procedure to restore the configuration on the replacement Panorama and restore access to the logs on the Dedicated Log Collectors that it manages. The allowed migration scenarios vary by Panorama management server:

<table>
<thead>
<tr>
<th>Old/Failed Panorama</th>
<th>New/Replacement Panorama</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panorama virtual appliance</td>
<td>• Panorama virtual appliance</td>
</tr>
<tr>
<td></td>
<td>• M-100 appliance</td>
</tr>
<tr>
<td></td>
<td>• M-500 appliance</td>
</tr>
<tr>
<td>M-100 appliance</td>
<td>• M-100 appliance</td>
</tr>
<tr>
<td></td>
<td>• M-500 appliance</td>
</tr>
<tr>
<td>M-500 appliance</td>
<td>M-500 appliance</td>
</tr>
</tbody>
</table>
Panorama maintains a ring file that maps the segments and partitions that Dedicated Log Collectors use to store logs. An M-Series appliance in Panorama mode stores the ring file on its internal SSD; a Panorama virtual appliance stores the ring file on its internal disk. When a system failure occurs, a non-HA Panorama cannot automatically recover the ring file. Therefore, when you replace Panorama, you must restore the ring file to access the logs on the Dedicated Log Collectors.

This procedure requires that you backed up and exported your Panorama configuration before the system failure occurred.

Palo Alto Networks recommends deploying Panorama in an HA configuration. The active Panorama peer automatically synchronizes the ring file to the passive peer in an HA configuration, thereby maintaining access to logs on the Dedicated Log Collectors even if you must replace one of the peers.

### Recover Logs after Panorama Failure/RMA in Non-HA Deployments

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Perform initial setup of the new Panorama appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>(Optional; applies only to M-Series appliances) Rack mount the M-Series appliance. Refer to the M-100 or M-500 Appliance Hardware Reference Guide for instructions.</td>
</tr>
<tr>
<td>2.</td>
<td>Perform Initial Configuration of the M-Series Appliance or Perform Initial Configuration of the Panorama Virtual Appliance.</td>
</tr>
<tr>
<td>3.</td>
<td>Register Panorama.</td>
</tr>
<tr>
<td>4.</td>
<td>Transfer licenses as follows only if the new Panorama model is the same model as the old one. Otherwise, you must purchase new licenses.</td>
</tr>
<tr>
<td>a.</td>
<td>Log in to the Palo Alto Networks Customer Support website.</td>
</tr>
<tr>
<td>b.</td>
<td>Select the Assets tab and click the Spares link.</td>
</tr>
<tr>
<td>c.</td>
<td>Click the Serial Number of the new M-Series appliance.</td>
</tr>
<tr>
<td>d.</td>
<td>Click Transfer Licenses.</td>
</tr>
<tr>
<td>e.</td>
<td>Select the old appliance and click Submit.</td>
</tr>
<tr>
<td>5.</td>
<td>Activate a Panorama Support License.</td>
</tr>
<tr>
<td>6.</td>
<td>Activate a firewall management license.</td>
</tr>
<tr>
<td>7.</td>
<td>Install Content and Software Updates for Panorama.</td>
</tr>
</tbody>
</table>

The M-500 appliance requires Panorama 7.0 or a later release. For important details about software versions, see Panorama, Log Collector, and Firewall Version Compatibility.
<table>
<thead>
<tr>
<th>Step 2</th>
<th>Restore the configuration from the old Panorama to the replacement Panorama.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log in to the new Panorama and select Panorama &gt; Setup &gt; Operations.</td>
</tr>
<tr>
<td>2.</td>
<td>Click Import named Panorama configuration snapshot, Browse to the backup configuration file, and click OK.</td>
</tr>
<tr>
<td>3.</td>
<td>Click Load named Panorama configuration snapshot and select the file you just imported.</td>
</tr>
<tr>
<td>4.</td>
<td>Perform any additional configuration changes as needed. If the old M-Series appliance used the Eth1 and Eth2 interfaces for log collection and Collector Group communication, you must define those interfaces on the new M-Series appliance (Panorama &gt; Setup &gt; Management). The Panorama virtual appliance does not use Eth1 or Eth2.</td>
</tr>
<tr>
<td>5.</td>
<td>Click Commit, set the Commit Type to Panorama, and click Commit again.</td>
</tr>
<tr>
<td>6.</td>
<td>Select Panorama &gt; Managed Collectors and verify that the Connected column displays a check mark for the Dedicated Log Collector. If the Dedicated Log Collector doesn't appear, you must reconfigure it and its Collector Group as described in Step 3. Otherwise, skip to Step 4.</td>
</tr>
</tbody>
</table>
Recover Logs after Panorama Failure/RMA in Non-HA Deployments (Continued)

**Step 3**  Reconfigure the Dedicated Log Collector and Collector Group if they are missing on Panorama.

1. Access the CLI of the Dedicated Log Collector and enter the following commands to display the name of its Collector Group.
   a. Enter the command:
      
      ```
      > request fetch ring from log-collector <serial_number>
      ```
      
      The following error will display:
      
      Server error: Failed to fetch ring info from <serial_number>
      
      b. Enter the command:
      
      ```
      > less mp-log ms.log
      ```
      
      The following error will display:
      
      Dec04 11:07:08 Error: pan_cms_convert_resp_ring_to_file(pan_ops_cms.c:3719): Current configuration does not contain group CA-Collector-Group
      
      In this example, the error message indicates that the missing Collector Group has the name CA-Collector-Group.

2. Configure the Collector Group and assign the Dedicated Log Collector to it.
   
   ```
   > configure
   > set log-collector-group <collector-group-name>
   > set log-collector-group.logfwd-setting collector <serial-number>
   ```

3. Commit the changes to Panorama but not to the Collector Group.
   
   ```
   > commit
   > exit
   ```

**Step 4**  Fetch the ring file to restore access to the logs stored on the Dedicated Log Collector.

1. Access the CLI of the new Panorama.

2. Fetch the ring file:
   
   ```
   > request fetch ring from log-collector <serial-number>
   ```
   
   For example:
   
   ```
   > request fetch ring from log-collector 009201000343
   ```
   
   If you don’t know the serial number of the Dedicated Log Collector, log in to its CLI and enter the `show system info` operational command.

3. Commit your changes to the Collector Group.
   
   ```
   > commit-all log-collector-config
   > log-collector-group <collector-group-name>
   ```
Regenerate Metadata for M-Series Appliance RAID Pairs

When a system failure occurs on the M-Series appliance and you need to physically move the disks from one appliance to another, regenerating the metadata is necessary. The metadata is required to locate logs on the disk; when a user issues a log query, the query consults this metadata to access the requested log data.

For each configured RAID disk pair in the M-Series appliance, you must access the appliance CLI and run the following command to regenerate the metadata:

```
request metadata-regenerate slot <slot_number>
```

For example:

```
request metadata-regenerate slot 1
```

The size of the RAID disks determines how long metadata regeneration takes. On average, it takes an hour for every 100GB. When you run the command, the CLI session is locked until the command is fully executed. You can use multiple CLI sessions to save time. For example, to replace four RAID pairs with a total of 4TB of log data, launch four CLI sessions and run the command in each session to regenerate metadata simultaneously for all the pairs/slots in about 10 hours.

During metadata regeneration, the Collector Group to which these disks belong is not available and the disk pair is not available for any logging or reporting operations (writes/queries). However, you can perform other tasks such as handling new firewall connections or managing configuration changes on the managed firewalls. All other Collector Groups that Panorama manages and that aren’t part of this RMA process can perform the assigned logging and reporting functionality as normal.
Replace an RMA Firewall

To minimize the effort required to restore the configuration on a managed firewall involving a Return Merchandise Authorization (RMA), replace the serial number of the old firewall with that of the new firewall on Panorama. To then restore the configuration on the replacement firewall, either import a firewall state that you previously generated and exported from the firewall or use Panorama to generate a partial device state for managed firewalls running PAN-OS 5.0 and later versions. By replacing the serial number and importing the firewall state, you can resume using Panorama to manage the firewall.

- Partial Device State Generation for Firewalls
- Before Starting RMA Firewall Replacement
- Restore the Firewall Configuration after Replacement

Partial Device State Generation for Firewalls

When you use Panorama to generate a partial device state, it replicates the configuration of the managed firewalls with a few exceptions for Large Scale VPN (LSVPN) setups. You create the partial device state by combining two facets of the firewall configuration:

- Centralized configuration that Panorama manages—Panorama maintains a snapshot of the shared policy rules and templates that it pushes to firewalls.
- Local configuration on the firewall—When you commit a configuration change on a firewall, it sends a copy of its local configuration file to Panorama. Panorama stores this file and uses it to compile the partial device state bundle.

In an LSVPN setup, the partial device state bundle that you generate on Panorama is not the same as the version that you export from a firewall (by selecting Device > Setup > Operations and clicking Export device state). If you manually ran the device state export or scheduled an XML API script to export the file to a remote server, you can use the exported device state in your firewall replacement workflow.

If you did not export the device state, the device state that you generate in the replacement workflow will not include the dynamic configuration information, such as the certificate details and registered firewalls, that is required to restore the complete configuration of a firewall functioning as an LSVPN portal. See Before Starting RMA Firewall Replacement for more information.

Panorama does not store the device state; you generate it on request using the CLI commands listed in Restore the Firewall Configuration after Replacement.

Before Starting RMA Firewall Replacement

- The firewall you will replace must have PAN-OS 5.0.4 or a later version. Panorama cannot generate the device state for firewalls running older PAN-OS versions.
- Record the following details about the firewall you will replace:
  - **Serial number**—You must enter the serial number on the Palo Alto Networks Customer Support web site to transfer the licenses from the old firewall to the replacement firewall. You will also enter this
information on Panorama, to replace all references to the old serial number with the new serial number of the replacement firewall.

- **(Recommended) PAN-OS version and the content database version**—Installing the same software and content database versions, including the URL database vendor, enables you to create the same state on the replacement firewall. If you decide to install the latest version of the content database, you might notice differences because of updates and additions to the database. To determine the versions installed on the firewall, access the firewall System logs stored on Panorama.

☐ Prepare the replacement firewall for deployment. Before you import the device state bundle and restore the configuration, you must:
  - Verify that the replacement firewall is the same model as the old firewall and is enabled for similar operational capability. Consider the following operational features: must the replacement firewall have multiple virtual systems, support jumbo frames support, or operate in CC or FIPS mode?
  - Configure network access, transfer the licenses, and install the appropriate PAN-OS and content database versions.

☐ You must use the Panorama CLI to complete this firewall replacement process, and therefore your administrator account must have the `superuser` or `panorama-admin` user role.

☐ If you have an LSVPN configuration, and are replacing a Palo Alto Networks firewall deployed as a satellite or as an LSVPN portal, the dynamic configuration information that is required to restore LSVPN connectivity will not be available when you restore the partial device state generated on Panorama. If you followed the recommendation to frequently generate and export the device state for firewalls in an LSVPN configuration, use the device state that you previously exported from the firewall itself instead of generating one on Panorama.

If you have not manually exported the device state from the firewall, and need to generate a partial device state on Panorama, the missing dynamic configuration impacts the firewall replacement process as follows:

  - **If the firewall you are replacing is a GlobalProtect portal** that is explicitly configured with the serial number of the satellites ([Network > GlobalProtect > Portals > Satellite Configuration](#)), when restoring the firewall configuration, although the dynamic configuration is lost, the portal firewall will be able to authenticate the satellites successfully. The successful authentication will populate the dynamic configuration information and LSVPN connectivity will be reinstated.

  - **If you are replacing a satellite firewall**, it will not be able to connect and authenticate to the portal. This failure occurs either because the serial number was not explicitly configured on the firewall ([Network > GlobalProtect > Portals > Satellite Configuration](#)) or, if the serial number was explicitly configured, because the serial number of the replaced firewall does not match that of the old firewall. To restore connectivity after importing the device state bundle, the satellite administrator must log in to the firewall and enter the credentials (username and password) for authenticating to the portal. After authentication, the dynamic configuration required for LSVPN connectivity is generated on the portal.

However, if the firewall was configured in a high availability configuration, after restoring the configuration, the firewall will automatically synchronize the running configuration with its peer and attain the latest dynamic configuration required to function seamlessly.
## Restore the Firewall Configuration after Replacement

To restore the firewall configuration on the new firewall, you will first perform initial configuration on the new firewall, including setting the operational mode, upgrading the PAN-OS software and content release version to match what was installed on the old firewall. You will then export the device state of the old firewall from Panorama and import it onto the new firewall. Finally, you will go back to Panorama to validate that the new firewall has connected and then sync it with Panorama.

### Restore the Firewall Configuration after Replacement

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Command/Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Perform initial configuration on the new firewall and verify network connectivity.</td>
<td>Use a serial port connection or a Secure Shell (SSH) connection to add an IP address, a DNS server IP address, and to verify that the new firewall can access the Palo Alto Networks updates server.</td>
</tr>
</tbody>
</table>
| 2.   | (Optional) Set the Operational mode on the new firewall to match that on the old firewall. A serial port connection is required for this task. | 1. Enter the following CLI command to access maintenance mode on the firewall: 
   ```
   > debug system maintenance-mode
   ```
   2. For Operational mode, select Set FIPS Mode or Set CCEAL 4 Mode from the main menu. |
| 3.   | Retrieve the license(s) on the new firewall. | Enter the following command to retrieve the licenses: 
   ```
   > request license fetch
   ``` |
| 4.   | (Optional) Match the operational state of the new firewall with that of the old firewall. For example, enable multi-virtual system (multi-vsyst) capability for a firewall that was enabled for multi-vsyst capability. | Enter the commands that pertain to your firewall settings:
   ```
   > set system setting multi-vsyst on
   > set system setting jumbo-frame on
   ``` |
| 5.   | Upgrade the PAN-OS version on the new firewall. You must upgrade to the same PAN-OS installed on the old firewall. You must upgrade the content release versions to the same or later version that is installed on the old firewall. | Enter the following commands:
   1. To upgrade the content release version:
      ```
      > request content upgrade download latest
      > request content upgrade install version latest
      ```
   2. To upgrade the PAN-OS software version:
      ```
      > request system software download version <version>
      > request system software install version <version>
      ``` |
| 6.   | Go to the Panorama CLI and export the device state bundle from the old firewall to a computer using Secure Copy (SCP) or TFTP (you cannot do this from the web interface). If you manually exported the device state from the firewall, you can skip this step. The export command generates the device state bundle as a tar zipped file and exports it to the specified location. This device state will not include the LSVPN dynamic configuration (satellite information and certificate details). | Enter one of the following commands:
   ```
   > scp export device-state device <old serial#> to <login> @ <serverIP>: <path>
   or
   > tftp export device-state device <old serial#> to <login> @ <serverIP>: <path>
   ```
## Restore the Firewall Configuration after Replacement (Continued)

### Step 7
Replace the serial number of the old firewall with that of the new replacement firewall on Panorama. By replacing the serial number on Panorama you allow the new firewall to connect to Panorama after you restore the configuration on the firewall.

1. Enter the following command in Operational mode:
   ```
   > replace device old <old SN#> new <new SN#>
   ```
2. Enter Configuration mode and commit your changes.
   ```
   > configure
   # commit
   ```
3. Exit Configuration mode.
   ```
   # exit
   ```

### Step 8
On the new firewall, import the device state and commit the changes.

1. Access the web interface of the new firewall.
2. Select Device > Setup > Operations and click the Import Device State link in the Configuration Management section.
3. Browse to locate the file and click OK.
4. Click Commit to save you changes to the running configuration on the firewall.

### Step 9
From Panorama, verify that you successfully restored the firewall configuration.

1. Access the Panorama web interface and select Panorama > Managed Devices.
2. Verify that the Connected column for the new firewall has a check mark.

### Step 10
Synchronize the firewall with Panorama.

1. From Panorama, click Commit, set the Commit Type to Device Group, select the device group that contains the firewall, select the Include Device and Network Template check box, and click Commit again.
2. (M-Series only) If your firewalls forward logs to Log Collectors, click Commit, set the Commit Type to Collector Group, select the Collector Group that contains the firewall, and click Commit again.

   If you need to generate reports for a period when the old firewall was still functional after you installed the new firewall, you must generate a separate query for each firewall serial number because replacing the serial number on Panorama does not overwrite the information in logs.
## Troubleshoot Commit Failures

If commit failures occur on Panorama, check for the following conditions:

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Condition</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template or device group commit failure</td>
<td>The ability to receive template and device groups configuration changes from Panorama is disabled on the firewall.</td>
<td>Access the firewall web interface, select <strong>Device &gt; Setup</strong>, edit the Panorama Settings, and then click <strong>Enable Device and Network Template</strong> and <strong>Enable Panorama Policy and Objects</strong>.</td>
</tr>
<tr>
<td>Panorama, template, device group, or Collector Group commit failure</td>
<td>The Panorama management server has an earlier software version than the Dedicated Log Collectors or firewalls that it manages.</td>
<td>Upgrade the Panorama management server to the same or a higher software version than the managed firewalls and Log Collectors. For details, see <strong>Panorama, Log Collector, and Firewall Version Compatibility</strong>.</td>
</tr>
</tbody>
</table>
Troubleshoot Registration or Serial Number Errors

On the M-Series appliance, if the Panorama > Support page doesn't display support license details or the Panorama > Setup > Management page displays Unknown for the Serial Number even after you Register Panorama, perform the following steps:

<table>
<thead>
<tr>
<th>Resolve Registration or Serial Number Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Record the Panorama serial number from the order fulfillment email that Palo Alto Networks sent when you placed your order for Panorama.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Select Panorama &gt; Setup &gt; Management and edit the General Settings.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Enter the Serial Number and click OK.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Click Commit, for the Commit Type select Panorama, and click Commit again.</td>
</tr>
</tbody>
</table>
Troubleshoot Reporting Errors

If Panorama fails to generate a report, or the report is missing expected data, its content versions (for example, the Applications and Threats database) might differ from those on the managed collectors and firewalls. The content versions on Panorama must be the same as or higher than the content versions on the managed collectors and firewalls. For details, see Panorama, Log Collector, and Firewall Version Compatibility.
View Task Success or Failure Status

Click the Task Manager icon at the bottom right of the Panorama web interface to view the success or failure of a task. The Task Manager also displays a detailed message to help debug an issue. For details, see Use the Panorama Task Manager.