Contact Information

Corporate Headquarters:
Palo Alto Networks
4401 Great America Parkway
Santa Clara, CA 95054
http://www.paloaltonetworks.com/contact/contact/

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-100 appliance for centralized administration of Palo Alto Networks firewalls.

If you have an M-100 appliance, this guide takes over after you finish rack mounting your M-100 appliance.

For more information, refer to the following sources:

▲ For instructions on configuring the features on the firewall, go to the PAN-OS Administrator's Guide. The Palo Alto Networks Administrator's Guide will also help you with Panorama configuration items that are similar to the firewall and are not covered in this guide.

▲ For access to the complete technical documentation set, go to https://paloaltonetworks.com/documentation.

▲ For access to the knowledge base and discussion forums, go to https://live.paloaltonetworks.com.

▲ For the latest release notes, go to the software downloads page at https://support.paloaltonetworks.com/Updates/SoftwareUpdates.

▲ To contact support, for information on the support programs, or to manage your account or devices, go to https://support.paloaltonetworks.com.

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

Palo Alto Networks, Inc.
www.paloaltonetworks.com
© 20013-2015 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at http://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Revision Date: May 11, 2015
# Table of Contents

## Centralized Configuration and Deployment Management
- Context Switch—Firewall or Panorama .................................................. 12
- Templates and Template Stacks ................................................................. 12
- Device Groups ......................................................................................... 14

## Centralized Logging and Reporting
- Logging Options ...................................................................................... 18
- Managed Collectors and Collector Groups ................................................. 19
- Caveats for a Collector Group with Multiple Log Collectors .................. 20
- Centralized Reporting .............................................................................. 21

## Panorama Commit Operations ................................................................. 22

## Role-Based Access Control ................................................................. 24
- Administrative Roles .............................................................................. 24
- Authentication Profiles and Sequences ................................................... 26
- Access Domains ..................................................................................... 26
- Administrative Authentication ................................................................. 26

## Panorama Recommended Deployments ............................................... 28
- Panorama for Centralized Management and Reporting ......................... 28
- Panorama in a Distributed Log Collection Deployment .......................... 29

## Plan Your Deployment ........................................................................... 30

## Set Up Panorama .................................................................................. 33
- Complete the Panorama Virtual Appliance Setup ....................................... 40
- Expand Log Storage Capacity on the Panorama Virtual Appliance ........ 38
- Install Panorama on the ESXi Server ....................................................... 35
- Perform Initial Configuration of the Panorama Virtual Appliance ........... 36
- Setup Prerequisites for the Panorama Virtual Appliance ......................... 34
- Set Up the Panorama Virtual Appliance .................................................. 34
- Switch from Panorama Mode to Log Collector Mode ............................... 45
- Increase Storage on the M-100 Appliance ............................................... 47
- Migrate from a Panorama Virtual Appliance to an M-100 Appliance ........ 49

## About Panorama ..................................................................................... 10

## Panorama Platforms .............................................................................. 11

## Set Up the M-100 Appliance ................................................................. 42

## Panorama in a Distributed Log Collection Deployment ....................... 29

## Panorama Overview ............................................................................ 9

## Contact Information ............................................................................... 2

## About this Guide .................................................................................... 2
Prerequisites for Migrating to an M-100 Appliance .......................... 49
Plan to Migrate to an M-100 Appliance .................................... 49
Migrate to an M-100 Appliance ............................................... 50
Resume Firewall Management after Migrating to an M-100 Appliance .... 52

Register Panorama and Install Licenses .................................... 53
Register Panorama .............................................................. 53
Activate a Panorama Support License ..................................... 54
Activate/Retrieve a Device Management License on the Panorama Virtual Appliance .............................................................. 55
Activate/Retrieve a Device Management License on the M-100 Appliance .............................................................. 55

Install Content and Software Updates for Panorama ...................... 65
Install Updates for Panorama with HA Configuration ................... 65
Install Updates for Panorama without Internet Connection ............. 65

Access and Navigate Panorama Management Interfaces .................. 62
Log in to the Panorama CLI .................................................. 63

Set Up Administrative Access to Panorama ................................ 65
Configure an Administrator with Kerberos SSO, External, or Local Authentication .............................................................. 65
Configure an Administrator with Certificate-Based Authentication for the Web Interface .............................................................. 69
Configure an Administrator with SSH Key-Based Authentication for the CLI .............................................................. 71
Configure RADIUS Vendor-Specific Attributes for Administrator Authentication .............................................................. 72

Manage Firewalls ............................................................... 75
Add a Firewall as a Managed Device ........................................ 76
Manage Device Groups .......................................................... 77
Add a Device Group .............................................................. 77
Create a Device Group Hierarchy ............................................. 78
Create Objects for Use in Shared or Device Group Policy .............. 79
Revert to Inherited Object Values .......................................... 80
Manage Unused Shared Objects .............................................. 81
Manage Precedence of Inherited Objects .................................. 82
Move or Clone a Policy Rule or Object to a Different Device Group .. 83
Select a URL Filtering Vendor on Panorama .............................. 84
Push a Policy Rule to a Subset of Firewalls ............................... 85
Manage the Rule Hierarchy .................................................... 85

Manage Templates and Template Stacks .................................... 88
Template Capabilities and Exceptions ..................................... 88
Add a Template ...................................................................... 88
Configure a Template Stack .................................................. 90
Process by Which a Firewall Receives a Virtual System from a Template .............................................................. 92
Override a Template Setting .................................................. 92
Disable/Remove Template Settings ......................................... 93

Transition a Firewall to Panorama Management .......................... 94
Plan the Transition to Panorama Management .............................. 94
Migrate a Firewall to Panorama Management ............................ 95

Use Case: Configure Firewalls Using Panorama ........................... 99
Table of Contents

Manage Log Collection .......................................................... 109
   Configure a Managed Collector ........................................... 110
   Manage Collector Groups .................................................. 115
   Configure a Collector Group ............................................. 115
   Move a Log Collector to a Different Collector Group .................. 119
   Remove a Firewall from a Collector Group ............................. 121
   Configure Log Forwarding to Panorama ................................. 122
   Verify Log Forwarding to Panorama ..................................... 124
   Modify Log Forwarding and Buffering Defaults ......................... 125
   Configure Log Forwarding from Panorama to External Destinations . 127
   Log Collection Deployments ............................................. 129
      Plan a Log Collection Deployment ................................ 129
      Deploy Panorama with Dedicated Log Collectors .................... 132
      Deploy Panorama with Default Log Collectors ....................... 138
      Deploy Panorama Virtual Appliances with Local Log Collection  145

Manage Licenses and Updates ............................................... 149
   Manage Licenses on Firewalls Using Panorama ......................... 150
   Deploy Updates to Devices Using Panorama ........................... 152
      Supported Updates by Device Type ................................ 152
      Schedule a Content Update to Devices Using Panorama .......... 153
   Install a Software Update on Firewall HA Pairs ...................... 153
   Deploy an Update to Devices when Panorama Has an Internet Connection 154
   Deploy an Update to Devices when Panorama Has No Internet Connection 156

Monitor Network Activity .................................................. 159
   Use Panorama for Visibility ............................................. 160
      Monitor the Network with the ACC and AppScope .................. 160
      Analyze Log Data ...................................................... 162
   Generate, Schedule, and Email Reports ............................... 162
   Use Case: Monitor Applications Using Panorama ..................... 166
   Use Case: Respond to an Incident Using Panorama .................... 170
      Incident Notification .................................................. 170
      Review the Widgets in the ACC ..................................... 171
      Review Threat Logs ................................................... 172
      Review WildFire Logs ................................................ 173
      Review Data Filtering Logs .......................................... 174
      Update Security Rules ................................................. 174

Panorama High Availability ................................................ 177
   Panorama HA Prerequisites .............................................. 178
Table of Contents

Administer Panorama ........................................... 191
  Manage Configuration Backups .................................. 192
  Schedule Export of Configuration Files ......................... 193
  Manage Panorama and Firewall Configuration Backups ........ 194
  Configure the Number of Configuration Backups Panorama Stores .......... 195
  Load a Configuration Backup on a Managed Firewall .......... 195
  Compare Changes in Panorama Configurations .................. 196
  Validate a Panorama Configuration ............................ 197
  Restrict Access to Configuration Changes ....................... 198
    Types of Locks .............................................. 198
    Locations for Taking a Lock .................................. 198
    Take a Lock ................................................. 199
    View Lock Holders ........................................... 199
    Enable Automatic Acquisition of the Commit Lock ............. 199
    Remove a Lock ............................................. 200
  Add Custom Logos to Panorama ................................ 201
  View Panorama Task Completion History ........................ 202
  Manage Storage Quotas and Expiration Periods for Logs and Reports 203
    Log and Report Storage ..................................... 203
    Log and Report Expiration Periods ........................... 203
    Configure Storage Quotas and Expiration Periods for Logs and Reports 204
  Monitor Panorama ............................................. 206
    Panorama System and Configuration Logs ...................... 206
    Monitor Panorama and Log Collector Statistics Using SNMP .... 207
  Reboot or Shut Down Panorama ................................ 210
  Configure Panorama Password Profiles and Complexity .......... 211

Troubleshooting ............................................... 213
  Troubleshoot Panorama System Issues .......................... 214
    Generate Diagnostic Files for Panorama ....................... 214
    Diagnose Panorama Suspended State .......................... 214
    Monitor the File System Integrity Check ..................... 215

Priority and Failover on Panorama in HA ........................ 179
Failover Triggers .............................................. 181
  HA Heartbeat Polling and Hello Messages ...................... 181
  HA Path Monitoring ........................................... 181
 Logging Considerations in Panorama HA .......................... 183
  Logging Failover on a Panorama Virtual Appliance .......... 183
  Logging Failover on an M-100 Appliance ...................... 184
 Synchronization Between Panorama HA Peers ...................... 185
 Manage a Panorama HA Pair ...................................... 186
  Set Up HA on Panorama ........................................ 186
  Test Panorama HA Failover ..................................... 188
  Switch Priority after Panorama Failover to Resume NFS Logging .. 188
  Restore the Primary Panorama to the Active State ........... 189

Panorama System and Configuration Logs ........................ 206
  Monitor Panorama ............................................. 206
  Manage Storage Quotas and Expiration Periods for Logs and Reports 203
    Log and Report Storage ..................................... 203
    Log and Report Expiration Periods ........................... 203
    Configure Storage Quotas and Expiration Periods for Logs and Reports 204
  Configure Panorama Password Profiles and Complexity .......... 211

Troubleshooting ............................................... 213
  Troubleshoot Panorama System Issues .......................... 214
    Generate Diagnostic Files for Panorama ....................... 214
    Diagnose Panorama Suspended State .......................... 214
    Monitor the File System Integrity Check ..................... 215

Reboot or Shut Down Panorama .................................. 210
  Configure Panorama Password Profiles and Complexity .......... 211

Monitor the File System Integrity Check ........................ 215

Palo Alto Networks
<table>
<thead>
<tr>
<th>Table of Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Panorama Storage for Software and Content Updates</td>
</tr>
<tr>
<td>Recover from Split Brain in Panorama HA Deployments</td>
</tr>
<tr>
<td>Troubleshoot Log Storage and Connection Issues</td>
</tr>
<tr>
<td>Verify Panorama Port Usage</td>
</tr>
<tr>
<td>Resolve Zero Log Storage for a Collector Group</td>
</tr>
<tr>
<td>Replace a Failed Disk on an M-100 Appliance</td>
</tr>
<tr>
<td>Replace the Virtual Disk on a Panorama Virtual Appliance</td>
</tr>
<tr>
<td>Recover Logs after Failure/RMA of M-100 Appliance in Log Collector Mode</td>
</tr>
<tr>
<td>Recover Logs after Failure/RMA of M-100 Appliance in Panorama Mode</td>
</tr>
<tr>
<td>Recover Logs after Panorama Failure/RMA in Non-HA Deployments</td>
</tr>
<tr>
<td>Regenerate Metadata for M-100 Appliance RAID Pairs</td>
</tr>
<tr>
<td>Replace an RMA Firewall</td>
</tr>
<tr>
<td>Partial Device State Generation for Firewalls</td>
</tr>
<tr>
<td>Before Starting RMA Firewall Replacement</td>
</tr>
<tr>
<td>Restore the Firewall Configuration after Replacement</td>
</tr>
<tr>
<td>Diagnose Template Commit Failures</td>
</tr>
<tr>
<td>View Task Success or Failure Status</td>
</tr>
</tbody>
</table>
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 device 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 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 platforms: as a virtual appliance and as a dedicated hardware appliance. For more information, see Panorama Platforms.
Panorama Platforms

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

- **Panorama virtual appliance**—The Panorama virtual appliance is installed on a VMware server. It allows for a simple installation and facilitates server consolidation for sites that need a virtual management appliance. It also supports integration with a Network File System (NFS) for increased storage and (> 2TB) log retention capabilities.

  The Panorama virtual appliance best suits environments with up to 10 firewalls and logging rates of up to 10,000 logs/second.

- **M-100 appliance**—A dedicated hardware appliance intended for large scale deployments. In environments with high logging rates and log retention requirements, this platform enables scaling of your log collection infrastructure. The appliance supports RAID 1 mirroring to protect against disk failures, and the default configuration ships with two 1TB drives; with additional RAID pairs, the M-100 appliance can support up to 4TB of log storage.

  The M-100 appliance allows for separation of the central management function from the log collection function by supporting the following deployment modes:

  - **Panorama mode**: The appliance performs both the central management and the log collection functions. This is the default mode.

  - **Log Collector mode**: The appliance functions as a Dedicated Log Collector, which either an M-100 appliance in Panorama mode or a Panorama virtual appliance can manage.

    When deployed in Log Collector mode, the appliance does not have a web interface; administrative access is CLI only. However, you manage the appliance using the Panorama management server (M-100 appliance in Panorama mode or a Panorama virtual appliance). CLI access to an M-100 appliance in Log Collector mode is only necessary for initial setup and debugging.

The platform choice depends on your need for a virtual appliance, the number of Palo Alto Networks firewalls you plan to manage, and your log collection requirements as detailed in the following table:

<table>
<thead>
<tr>
<th>Considerations</th>
<th>Panorama Virtual Appliance</th>
<th>M-100 Appliance in Panorama Mode</th>
<th>M-100 Appliance in Log Collector Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of managed firewalls</td>
<td>10 or fewer firewalls</td>
<td>Up to 1,000 firewalls</td>
<td>Up to 1,000 firewalls</td>
</tr>
<tr>
<td>Log collection rate</td>
<td>&lt;10,000 logs/second</td>
<td>&lt;10,000 logs/second</td>
<td>&gt; 10,000 logs/second (Max 50,000 logs/second per Log Collector)</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 bootup).
- 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 device-specific settings. Alternatively, you can push a broader common base configuration and in the individual firewalls override certain pushed settings with device-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 are not in multi-vsys mode.
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 devices 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

![Device Group Hierarchy Diagram](image-url)
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 Platform</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></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>
</tbody>
</table>
Centralized Configuration and Deployment Management

Panorama 7.0 Administrator’s Guide

Palo Alto Networks

Evaluation Order | Rule Scope and Description | Administration Platform
--- | --- | ---
Device group post-rules | 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. | These rules are visible on firewalls but you can only manage them in Panorama.

| intrazone-default | 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. | 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 device 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.

| interzone-default | These rules are visible on firewalls but you can only manage them in Panorama. | These rules are visible on firewalls but you can only manage them in Panorama.

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 appear in green, while local firewall rules appear in blue between the pre-rules and post-rules.
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-100 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 platform.

<table>
<thead>
<tr>
<th>Panorama Platform</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 10GB 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 that can support up to 2TB of storage.</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>
Panorama Overview

Centralized Logging and Reporting

<table>
<thead>
<tr>
<th>Panorama Platform</th>
<th>Logging Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>M-100 appliance</td>
<td>The default shipping configuration includes 1TB disks in a RAID pair, which you can increase to 4TB RAID storage (see Increase Storage on the M-100 Appliance). When the M-100 appliance is in Panorama mode, you can enable the RAID disks and use these disks as the default Log Collector. If you have M-100 appliance in Log Collector mode (dedicated Log Collectors), you use Panorama to assign firewalls to the Dedicated Log Collectors. In a deployment with multiple Dedicated Log Collectors, Panorama queries all managed Log Collectors to generate an aggregated view of traffic and cohesive reports. For easy scaling, begin with a single Panorama and incrementally add Dedicated Log Collectors as your needs expand.</td>
</tr>
</tbody>
</table>

Managed Collectors and Collector Groups

A Log Collector can be local to an M-100 appliance in Panorama mode (default Log Collector) or can be an M-100 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-100 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 one or more 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. Each Panorama can manage up to 64 Log Collectors in a Collector Group. However, Palo Alto Networks recommends placing only one Log Collector in a Collector Group unless more than 4TB of storage space is required in a Collector Group. For details, 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.

If you use Panorama to manage firewalls running both PAN-OS 5.0 and a PAN-OS version earlier than 5.0, note the following compatibility requirements:

- Only devices running PAN-OS v5.0 can send logs to a Dedicated Log Collector.
- Devices running PAN-OS versions earlier than 5.0 can only send logs to a Panorama virtual appliance or to an M-100 appliance in Panorama mode.

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-100 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 Collector Groups.
Caveats for a Collector Group with Multiple Log Collectors

Although Palo Alto Networks recommends placing only one Log Collector in a Collector Group, if you have a scenario where you need more than 4TB of log storage capacity in a Collector Group for the required log retention period, you will need to Configure a Collector Group with multiple Log Collectors (up to eight. For example, if a single managed firewall generates 12 TB of logs, you will require at least three Log Collectors in the Collector Group that receives those logs.

If a Collector Group contains multiple Log Collectors, the available storage space is used as one logical unit and the logs are uniformly distributed across all the Log Collectors in the Collector Group. The log distribution is based on the disk capacity of the Log Collectors (which ranges from 1TB to 4TB, depending on the number of disk pairs) 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. Therefore, Palo Alto Networks recommends the following mitigations if using multiple Log Collectors in a Collector Group:

- Obtain an On-Site-Spare (OSS) to enable prompt replacement if a Log Collector failure occurs.
In addition to forwarding logs to Panorama, enable 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 Operations

When editing the configuration on Panorama, you are changing the candidate configuration file. The candidate configuration is a copy of the running configuration along with the modifications that you saved using the Save option. The Panorama web interface displays all the configuration changes immediately. However, Panorama does not implement the changes until you commit them. The commit process validates the changes in the candidate configuration file and saves it as the running configuration on Panorama.

<table>
<thead>
<tr>
<th>Commit Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panorama</td>
<td>Commits the changes on the current candidate configuration to the running configuration on Panorama. You must first commit your changes on Panorama, before committing any configuration updates (templates or device groups) to the managed firewalls or Collector Groups.</td>
</tr>
<tr>
<td>Template</td>
<td>Commits network and device configurations from a Panorama template or template stack to the selected firewalls.</td>
</tr>
<tr>
<td>Device Group</td>
<td>Commits policies and objects configured from Panorama to the selected firewalls/virtual systems.</td>
</tr>
<tr>
<td>Collector Group</td>
<td>Commits changes to the specified Collector Groups that Panorama manages.</td>
</tr>
</tbody>
</table>

When you perform a commit, Panorama pushes the entire configuration to the managed firewalls or Log Collectors. When the commit completes, a result displays: Commit succeeded or Commit succeeded with warnings.

Some other commit choices are:

- **Preview Changes**—This option is available when the Commit Type is Panorama. It enables you to compare the candidate configuration with the running configuration in the same way as the Panorama > Config Audit feature (see Compare Changes in Panorama Configurations). After clicking Preview Changes, select the number of lines to include for context, and click OK.

- **Validate Changes**—This option is available when the Commit Type is Panorama, Template, or Device Group. It enables you to Validate a Panorama Configuration before committing it.

- **Include Device and Network Templates**—This option is available when committing a device group from Panorama. It allows you to commit both device group and template or template stack changes to the selected firewalls in a single commit operation. The check box is selected by default. If you prefer to commit these changes as separate operations, clear this check box.

- **Force Template Values**—When performing a template or device group commit, the Force Template Values option overrides all local configuration and removes objects on the selected firewalls or virtual systems that don’t exist in the template or template stack, or are overridden in the local configuration. This is an override that reverts all existing configuration on the managed firewall, and ensures that the firewall inherits only the settings defined in the template or template stack.
Panorama Overview

- **Merge with Candidate Config**—When enabled, this option allows you to merge and commit the Panorama configuration changes with any pending configuration changes that were implemented locally on the target firewall. If this option is not enabled, the candidate configuration on the firewall is not included in the commit operation. As a best practice, leave this option disabled if you allow firewall administrators to modify the configuration directly on a firewall and you don’t want to include their changes when committing changes from Panorama. Another best practice is to use the configuration audit capability on Panorama to review any locally defined configuration changes prior to issuing a commit from Panorama (see Compare Changes in Panorama Configurations).
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. 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-100 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.

- **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 devices. 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>
Panorama Overview

Role-Based Access Control

- **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>Dynamic Role</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panorama administrator</td>
<td>Full access to Panorama except for the following actions:</td>
</tr>
<tr>
<td></td>
<td>• Create, modify, or delete Panorama or device administrators and roles.</td>
</tr>
<tr>
<td></td>
<td>• Export, validate, revert, save, load, or import a configuration in the <strong>Device &gt; Setup &gt; Operations</strong> page.</td>
</tr>
<tr>
<td></td>
<td>• Configure <strong>Scheduled Config Export</strong> functionality in the <strong>Panorama</strong> tab.</td>
</tr>
</tbody>
</table>

### Admin Role Profile Description

- **Panorama**
  
  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.

- **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 devices 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 authentication 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 Access Domains.
- Configure RADIUS Vendor-Specific Attributes for Administrator Authentication.

Administrative Authentication

The following methods are available to authenticate Panorama administrators:
Panorama Overview

Role-Based Access Control

- **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 a fallback 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-100 appliance in a redundant configuration for the following benefits:

- **Centralized management**—Centralized policy and device 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-100 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-100 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-100 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:

- Allows for improved performance in the management functions on Panorama
- Provides high-volume log storage on a dedicated hardware appliance
- Provides horizontal scalability and redundancy with RAID 1 storage
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 devices in the network?

If you already deployed and configured the Palo Alto Networks firewalls on your network, determine whether to transition the devices 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 that Panorama is on the same release version or a later version than the firewalls that it will manage. For example, Panorama with version 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, Palo Alto Networks recommends that Panorama run the same version or a later version. For example, if Panorama runs 6.0.3, it is recommended that all managed firewalls run PAN-OS 6.0.3 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 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 the Log Rate on the Firewall and the article Panorama Logging Suggestions.

- 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 need to forward logs?
  - Do you need redundancy in logging? With Panorama virtual appliances in HA, each peer can log to its virtual disk. The managed devices can send logs to both peers in the HA pair. This option provides redundancy in logging and is best suited to support up to 2TB of log storage capacity.
  - Will you log to a Network File System (NFS)? Only the Panorama virtual appliance supports NFS. Consider using NFS if more than 2TB of log storage capacity is required. If using NFS, note that the managed devices 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-100 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-100 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 platforms, 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>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>(M-100 appliance only) Rack mount the appliance.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Perform initial configuration to enable network access to Panorama. See Set Up the Panorama Virtual Appliance or Set Up the M-100 Appliance.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Register Panorama and Install Licenses.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Install Content and Software Updates for Panorama.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional/recommended) Set up Panorama in a high availability configuration. See Panorama High Availability.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Add a Firewall as a Managed Device.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Add a Device Group or Create a Device Group Hierarchy, Add a Template, and (if applicable) Configure a Template Stack.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>(Optional) Configure log forwarding to Panorama and/or to external services. See Manage Log Collection.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Monitor Network Activity using the visibility and reporting tools on Panorama.</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 appliance).

The following topics describe how to set up Panorama on your network:

- Set Up the Panorama Virtual Appliance
- Set Up the M-100 Appliance
- Migrate from a Panorama Virtual Appliance to an M-100 Appliance
- Register Panorama and Install Licenses
- Install Content and Software Updates for Panorama
- Access and Navigate Panorama Management Interfaces
- Set Up Administrative Access to Panorama
Set Up the Panorama Virtual Appliance

The Panorama virtual appliance consolidates the Panorama management and logging functions into a single virtual appliance. This solution enables use of an existing VMware virtual infrastructure to easily deploy and centrally administer and monitor the Palo Alto Networks firewalls in your network as described in the following sections:

- Setup Prerequisites for the Panorama Virtual Appliance
- Install Panorama on the ESXi Server
- Perform Initial Configuration of the Panorama Virtual Appliance
- Expand Log Storage Capacity on the Panorama Virtual Appliance
- Complete the Panorama Virtual Appliance Setup

You cannot use the Panorama virtual appliance as a Dedicated Log Collector. Only an M-100 appliance in Log Collector mode provides dedicated log collection capabilities (see Set Up the M-100 Appliance). However, you can use the Panorama virtual appliance to manage a Dedicated Log Collector.

Setup Prerequisites for the Panorama Virtual Appliance

To set up a Panorama virtual appliance efficiently, complete the following tasks before you begin:

- Verify that your server meets the minimum system requirements for installing Panorama. These requirements apply to Panorama 5.1 and later releases.

### Prerequisites for the Panorama Virtual Appliance

- 64-bit kernel-based VMware ESXi 4.1 or later
- Use the following guidelines for allocating CPU and memory:
  - Less than 10 managed firewalls: 4 cores and 4GB
  - Between 10 and 50 managed firewalls: 8 cores and 8GB
  - More than 50 managed firewalls: 8 cores and 16 GB
- 40GB disk space
  
  Adding more disk space does not increase the available log storage capacity on Panorama. To expand log capacity, you must add a virtual disk or set up access to an NFS datastore. See Expand Log Storage Capacity on the Panorama Virtual Appliance.
- A client computer with one of the following: VMware vSphere Client or VMware Infrastructure Client that is compatible with your ESXi server

- Register the Panorama serial number on the support site at [https://support.paloaltonetworks.com](https://support.paloaltonetworks.com) (see Register Panorama). Palo Alto Networks will have sent you the serial number by email. After registering the serial number on the support site, you gain access to the Panorama software downloads page.
### Install Panorama on the ESXi Server

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| **Install Panorama on the ESXi Server** | **1.** Go to [https://support.paloaltonetworks.com](https://support.paloaltonetworks.com) and download the Panorama Base Image zip file.  
**2.** Unzip the Panorama base image zip file, and extract the `panorama-esx.ovf` file.  
This .ovf template file is required for installing Panorama. |
| **Step 2** | Access the ESXi server.  
Launch the VMware vSphere Client and connect to the VMware server. |
| **Step 3** | Install Panorama.  
Starting with Panorama 5.1, the Panorama virtual appliance is installed as a 64-bit virtual machine.  
| 1. | Choose **File > Deploy OVF Template**.  
2. | **Browse** to select the `panorama-esx.ovf` file from the recently unzipped Panorama base image, and click **Next**.  
3. | Confirm that the product name and description match the downloaded version, and click **Next**.  
4. | Enter a descriptive name for the Panorama virtual appliance, and click **Next**.  
5. | Select a **Datastore Location** on which to install the Panorama image, and click **Next**.  
Adding additional disk space does not increase the available log storage capacity on Panorama. To expand log capacity, you must add a virtual disk or set up access to an NFS datastore. See Expand Log Storage Capacity on the Panorama Virtual Appliance.  
6. | Select **Thick Provision Lazy Zeroed** as the disk format, and click **Next**.  
7. | Specify which networks in the inventory must be used for the Panorama virtual appliance.  
8. | Confirm the selected options and then click **Finish** to begin the installation process.  
9. | When the installation completes, select the Panorama virtual appliance, and click **Edit Settings...** to define the following settings:  
   a. Verify that you have allocated the appropriate amount of memory: at least 4GB.  
   b. Select **Linux** as the **Guest Operating System** and for the **Version** select **Other Linux (64-bit)**.  
   c. For the SCSI controller, select **LSI Logic Parallel**. |
Set Up the Panorama Virtual Appliance

Continue with Perform Initial Configuration of the Panorama Virtual Appliance.

Perform Initial Configuration of the Panorama Virtual Appliance

Use the Panorama virtual appliance console on the ESXi server to set up network access to the Panorama virtual appliance. To complete initial configuration, you must first configure the management interface, then access the Panorama web interface to add the serial number for the virtual appliance, and define the time zone for the Panorama virtual appliance. For unified reporting, consider using GMT or UTC as the uniform time zone across all the managed devices and Panorama.

Configure the Management Interface of the Panorama Virtual Appliance

| Step 1 | Gather the required information from your network administrator. | • IP address for MGT port  
• Netmask  
• Default gateway  
• DNS server IP address |
| --- | --- | --- |

| Step 2 | Access the console of the Panorama virtual appliance. | 1. Select the **Console** tab on the ESXi server for the virtual Panorama. Press enter to access the login screen.  
2. Enter the default username/password (admin/admin) to log in.  
3. Enter `configure` to switch to Configuration mode. |

| Step 3 | Configure the network access settings for the management interface.  
The management interface is used for management traffic, HA connectivity synchronization, log collection, and communication within Collector Groups. | Enter the following command:  
```
set deviceconfig system ip-address <Panorama-IP>  
netmask <netmask> default-gateway <gateway-IP>  
dns-setting servers primary <DNS-IP>
```
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. |

| Step 4 | Commit your changes and exit the Configuration mode. | 1. Enter `commit`.  
2. Enter `exit`. |
## Configure the Management Interface of the Panorama Virtual Appliance (Continued)

### Step 5 Verify network access to external services required for firewall management, such as the Palo Alto Networks Update Server.

To verify that Panorama has external network access, use the ping utility. Verify connectivity to 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.

## Configure the Serial Number and Time Zone of the Panorama Virtual Appliance

### Step 1 Log in to the Panorama web interface.

Using a secure connection (https) from a web browser, log in using the IP address and password you assigned to the management interface (https://<IP address>).

### Step 2 (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, to enable Secure Shell (SSH) access, select **SSH**. As a best practice, make sure Telnet and HTTP are not selected because these services use plaintext and are not as secure as the other services.
3. Click **OK** and **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.

### Step 3 Configure the 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. Timestamps are recorded when the logs are received on Panorama and when they were generated on the firewalls. Aligning the time zones on both Panorama and the managed firewalls ensures that the timestamps are in sync, and the process of querying logs and generating reports on Panorama is harmonious.
3. Enter a **Hostname** for the server and enter the network **Domain** name. The domain name is just a label; it will not be used to join the domain.
4. Enter the **Latitude** and **Longitude** to enable accurate placement of the server on the world map.
5. Enter the **Serial Number**. This was sent to you with the order fulfillment email.
6. Click **OK**.
### Configure the Serial Number and Time Zone of the Panorama Virtual Appliance (Continued)

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Change the default admin password.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To ensure that the management</td>
</tr>
<tr>
<td></td>
<td>interface remains secure, consider</td>
</tr>
<tr>
<td></td>
<td>enforcing **Minimum Password</td>
</tr>
<tr>
<td></td>
<td>Complexity** and defining an</td>
</tr>
<tr>
<td></td>
<td>interval at which administrators</td>
</tr>
<tr>
<td></td>
<td>must change their passwords.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Save your configuration changes.</th>
</tr>
</thead>
<tbody>
<tr>
<td></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>

### Expand Log Storage Capacity on the Panorama Virtual Appliance

By default, the Panorama virtual appliance has a single disk partition for all data, and 10.89GB of this space is allocated for log storage. The following topics describe how to estimate the required log storage capacity based on the log rate and to expand that capacity. If you need another 40GB to 2TB of disk space, add a virtual disk. If you need more than 2TB, use an NFS datastore.

- **Determine the Log Rate on the Firewall**
- **Add a Virtual Disk to the Panorama Virtual Appliance**
- **Mount the Panorama Virtual Appliance to an NFS Datastore**

### Determine the Log Rate on the Firewall

Use these instructions at different times during the day to approximate the normal and peak log generation rate on each firewall. To accurately estimate the amount of storage required for logs on your network, in addition to the log rate on the firewall, you must consider several other factors. For details, refer to the article Panorama Logging Suggestions.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Access the CLI on each Palo Alto Networks firewall.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>See <strong>Log in to the Panorama CLI</strong>; the process of accessing the CLI on the firewall is the same as that on Panorama.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>View the current log generation rate.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enter the following CLI command to gauge the log rate on the firewall: <strong>debug log-receiver statistics</strong></td>
</tr>
<tr>
<td></td>
<td>Logging statistics</td>
</tr>
<tr>
<td></td>
<td>Log incoming rate: 246/sec</td>
</tr>
<tr>
<td></td>
<td>Log written rate: 246/sec</td>
</tr>
</tbody>
</table>
Add a Virtual Disk to the Panorama Virtual Appliance

By default, the Panorama virtual appliance has a virtual disk of size 34GB, of which 10.89GB is used for logging. To enable more log storage, use the following procedure to create a new virtual disk that can support 40GB to 2TB of storage capacity.

The Panorama virtual appliance can only use one virtual disk. When configured to use a virtual disk, the virtual appliance does not use the default 10GB internal storage for logging. Therefore, if it loses connectivity to the virtual disk, logs could be lost 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.

You can also Replace the Virtual Disk on a Panorama Virtual Appliance.

---

Add a Virtual Disk to the Panorama Virtual Appliance

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Power off the Panorama virtual appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>On the ESXi server, add the virtual disk to the Panorama virtual appliance.</td>
</tr>
<tr>
<td></td>
<td>1. Select the Panorama virtual appliance on the ESXi server.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Edit Settings</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add</strong> to launch the Add Hardware wizard, and select the following options when prompted:</td>
</tr>
<tr>
<td></td>
<td>a. Select <strong>Hard Disk</strong> for the hardware type.</td>
</tr>
<tr>
<td></td>
<td>b. Select <strong>Create a new virtual disk</strong>.</td>
</tr>
<tr>
<td></td>
<td>c. Select <strong>SCSI</strong> as the virtual disk type.</td>
</tr>
<tr>
<td></td>
<td>d. Select the <strong>Thick provisioning</strong> disk format.</td>
</tr>
<tr>
<td></td>
<td>e. In the location field, select <strong>Store with the virtual machine option</strong>. The datastore does not have to reside on the ESXi server.</td>
</tr>
<tr>
<td></td>
<td>f. Verify that the settings look correct and click <strong>Finish</strong> to exit the wizard. The new disk is added to the list of devices for the virtual appliance.</td>
</tr>
</tbody>
</table>

Step 3  Power on the Panorama virtual appliance. When powered on, the virtual disk is initialized for first-time use. The time that the initialization process takes to complete varies by the size of the new virtual disk. When the virtual disk is initialized and ready, all existing logs on the internal storage are moved over to the new virtual disk. All new entries will now be written to the virtual disk.

Step 4  Verify the size of the virtual disk. 1. Select **Panorama > Setup > Management**. |
2. In the Logging and Reporting Settings section, verify that the **Log Storage** capacity accurately displays the new disk capacity.
### Mount the Panorama Virtual Appliance to an NFS Datastore

Mounting the Panorama virtual appliance to an NFS datastore provides the ability to write logs to a centralized location and offers the flexibility to expand the log storage capacity beyond 2TB. Before setting up an NFS datastore in a Panorama high availability configuration, see [Logging Considerations in Panorama HA](#).

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select <a href="#">Panorama &gt; Setup &gt; Operations</a>.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <a href="#">Storage Partition Setup</a> link in the Miscellaneous section.</td>
</tr>
<tr>
<td>3.</td>
<td>Select <a href="#">NFS V3</a>.</td>
</tr>
<tr>
<td>4.</td>
<td>Enter the IP address of the NFS <a href="#">Server</a>.</td>
</tr>
<tr>
<td>5.</td>
<td>Enter the location/path for storing the log files in the <a href="#">Log Directory</a> field. For example, export/panorama.</td>
</tr>
<tr>
<td>6.</td>
<td>Select the protocol—<strong>TCP</strong> or <strong>UDP</strong>—and enter the <a href="#">Port</a> for accessing the NFS server.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>7.</td>
<td>For optimal NFS performance, in the <a href="#">Read Size</a> and <a href="#">Write Size</a> 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.</td>
</tr>
<tr>
<td>8.</td>
<td>(Optional) Select the <a href="#">Copy on Setup</a> option. This setting copies the existing logs stored on Panorama to the NFS volume. If you have a lot of existing logs, enabling the <a href="#">Copy on Setup</a> option might initiate the transfer of a large volume of data.</td>
</tr>
<tr>
<td>9.</td>
<td>Click <a href="#">Test Logging Partition</a> to verify that Panorama can access the NFS <a href="#">Server</a> and <a href="#">Log Directory</a>.</td>
</tr>
<tr>
<td>10.</td>
<td>Click <a href="#">OK</a> and <a href="#">Commit</a>, for the <a href="#">Commit Type</a> select <a href="#">Panorama</a>, and click <a href="#">Commit</a> again.</td>
</tr>
<tr>
<td></td>
<td>To begin writing logs to the NFS datastore, reboot the virtual Panorama.</td>
</tr>
<tr>
<td></td>
<td>1. Select <a href="#">Panorama &gt; Setup &gt; Operations</a>.</td>
</tr>
<tr>
<td></td>
<td>2. In the Device Operations section, select <a href="#">Reboot Panorama</a>.</td>
</tr>
</tbody>
</table>

### Complete the Panorama Virtual Appliance Setup

Now that initial configuration is complete, continue with the following sections for additional configuration instructions:

- [Activate a Panorama Support License](#)
- [Activate/Retrieve a Device Management License on the Panorama Virtual Appliance](#)
Set Up Panorama

- 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-100 Appliance

The M-100 management appliance is a high performance hardware platform that you can deploy in two modes:

- **Panorama mode**—The appliance performs both the central management and log collection functions. This is the default mode.

- **Log Collector mode**—The appliance functions as a Dedicated Log Collector. If multiple firewalls forward large volumes of log data, the M-100 appliance in Log Collector mode provides increased scale and performance. In this mode, the appliance does not have a web interface, only a command-line interface (CLI). However, you manage the appliance using the Panorama management server (M-100 appliance in Panorama mode or a Panorama virtual appliance). CLI access to an M-100 appliance in Log Collector mode is only necessary for initial setup and debugging.

The Panorama M-100 appliance supports separate interfaces for configuration (of firewalls, Log Collectors, and Panorama itself), log collection, and communication within Collector Groups. By default, the M-100 appliance uses the MGT (Eth0) interface for all three functions. Only the MGT interface can support the configuration function. For the log collection and Collector Group communication functions, you can assign the Eth1 or Eth2 interface to perform either or both when you Perform Initial Configuration of the M-100 Appliance. You cannot assign multiple interfaces to a single function. The M-100 Hardware Reference Guide explains where to attach cables for the MGT, Eth1, and Eth2 interfaces on the M-100 appliance. To support separate interfaces, the M-100 appliances (in Panorama or Log Collector mode) must have Panorama 6.1 or later installed and the firewalls must have PAN-OS 6.0 or later installed.

Use the following workflows for setting up an M-100 appliance:

<table>
<thead>
<tr>
<th>M-100 Appliance in Panorama Mode</th>
<th>M-100 Appliance in Log Collector Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Rack mount the M-100 appliance. Refer to the M-100 Hardware Reference Guide for instructions.</td>
<td>Step 1 Rack mount the M-100 appliance. Refer to the M-100 Hardware Reference Guide for instructions.</td>
</tr>
<tr>
<td>Step 2 Perform Initial Configuration of the M-100 Appliance</td>
<td>Step 2 Perform Initial Configuration of the M-100 Appliance</td>
</tr>
<tr>
<td>Step 3 Register Panorama and Install Licenses</td>
<td>Step 3 Register Panorama and Install Licenses</td>
</tr>
<tr>
<td>Step 4 Install Content and Software Updates for Panorama</td>
<td>Step 4 Install Content and Software Updates for Panorama</td>
</tr>
<tr>
<td>Step 5 (Optional) Increase Storage on the M-100 Appliance</td>
<td>Step 5 (Optional) Increase Storage on the M-100 Appliance</td>
</tr>
<tr>
<td>Step 6 Set Up Administrative Access to Panorama</td>
<td>Step 6 Switch from Panorama Mode to Log Collector Mode</td>
</tr>
<tr>
<td>Step 7 Manage Firewalls</td>
<td>Step 7 Manage Log Collection</td>
</tr>
<tr>
<td>Step 8 Manage Log Collection</td>
<td></td>
</tr>
</tbody>
</table>
Perform Initial Configuration of the M-100 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 MGT interface or using a direct serial port connection to the console port on the M-100 appliance.

<table>
<thead>
<tr>
<th>Perform Initial Configuration of the M-100 Appliance</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>
</tbody>
</table>
## Perform Initial Configuration of the M-100 Appliance (Continued)

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Configure the network access settings for each interface that Panorama will use for configuration, log collection, and Collector Group communication.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Select <strong>Panorama &gt; Setup &gt; Management</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Edit the Interface Settings of each interface that Panorama will use: Management, Eth1, and/or Eth2. Only the Management interface is mandatory.</td>
</tr>
<tr>
<td></td>
<td>a. Complete one of the following field sets, depending on the IP protocol 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>b. (Optional) Select the check boxes for the management services to allow on the interface. <strong>Ping</strong> is the only option for Eth1 and Eth2. As a best practice, clear the <strong>Telnet</strong> and <strong>HTTP</strong> check boxes for the Management interface: these services use plaintext and so are less secure than others.</td>
</tr>
<tr>
<td></td>
<td>c. Click <strong>OK</strong> to save your changes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Configure the hostname, time zone, and general settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Select <strong>Panorama &gt; Setup &gt; Management</strong> and edit the General Settings.</td>
</tr>
<tr>
<td></td>
<td>2. Align the clock on Panorama and the managed firewalls to use the same <strong>Time Zone</strong>, for example GMT or UTC.</td>
</tr>
<tr>
<td></td>
<td>PAN-OS records timestamps when the firewalls generate logs and when Panorama receives 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.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a <strong>Hostname</strong> 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 <strong>Panorama &gt; Managed Collectors</strong> page.</td>
</tr>
<tr>
<td></td>
<td>4. Enter your network <strong>Domain</strong> name. The domain name is just a label; Panorama does not use it to join the domain.</td>
</tr>
<tr>
<td></td>
<td>5. (Optional) Enter the <strong>Latitude</strong> and <strong>Longitude</strong> to enable accurate placement of the server on the world map. The <strong>App Scope &gt; Traffic Maps</strong> and <strong>App Scope &gt; Threat Maps</strong> use these values.</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>
Set Up Panorama

Set Up the M-100 Appliance

---

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

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Configure the DNS and update servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Select Panorama &gt; Setup &gt; Services and edit the settings.</td>
</tr>
<tr>
<td></td>
<td>2. Enter the IP address of the Primary DNS Server and (optionally) of the Secondary DNS Server.</td>
</tr>
<tr>
<td></td>
<td>3. The default Update Server is updates.paloaltonetworks.com. If you need to specify a particular update resource, refer to Content Delivery Network Infrastructure for Dynamic Updates for a list of URLs and static addresses. Select the Verify Update Server Identity check box if you want Panorama to verify that the 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.</td>
</tr>
<tr>
<td></td>
<td>4. Click OK to save your entries.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Change the default admin password.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To ensure that the management interface remains secure, enforce Minimum Password Complexity and specify the interval at which administrators must change their passwords.</td>
</tr>
<tr>
<td></td>
<td>1. Click the admin link in the lower left part of the management console.</td>
</tr>
<tr>
<td></td>
<td>2. Enter the old administrator password and new password in the appropriate fields, then store the new password in a safe location.</td>
</tr>
<tr>
<td></td>
<td>3. Click OK and Commit, for the Commit Type select Panorama, and click Commit again.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Verify network access to external services required for firewall management, such as the Palo Alto Networks Update Server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To verify that Panorama has external network access, use the ping utility. Verify connectivity to the default gateway, DNS server, and the Palo Alto Networks Update Server as shown in the following example:</td>
</tr>
<tr>
<td></td>
<td>admin@Panorama-Corp&gt; 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.</td>
</tr>
</tbody>
</table>

Continue with Register Panorama and Install Licenses and Install Content and Software Updates for Panorama, regardless of whether you plan on using the M-100 appliance in Panorama mode or in Log Collector mode.

**Switch from Panorama Mode to Log Collector Mode**

Using an M-100 appliance as a Log Collector offloads the task of processing logs from the Panorama management server to a dedicated appliance. Perform the steps below to convert an M-100 appliance from Panorama mode to Log Collector mode. Before starting, ensure that the Panorama management server (virtual appliance or M-100 appliance in Panorama mode) that will manage the firewalls and the Log Collector is already set up.

---

**Palo Alto Networks**

Panorama 7.0 Administrator’s Guide • 45
### Switch From Panorama Mode to Log Collector Mode

| Step  1  | Access the command line interface (CLI) on the M-100 appliance. | Connect to the M-100 appliance in one of the following ways:  
|---|---|---|
|   |   | • Attach a serial cable from a computer to the Console port on the M-100 appliance. Then, connect using a terminal emulation software (9600-8-N-1).  
|   |   | • Use a terminal emulation software such as PuTTY to open a Secure Shell (SSH) session to the IP address assigned to the M-100 appliance during initial configuration.  

| Step 2 | When prompted, log in to the appliance. Use the default admin account and the password assigned during initial configuration. |   |

| Step 3 | Switch from Panorama mode to Log Collector mode. | 1. To switch to Log Collector mode, enter the following command:  
|---|---|---|
|   |   | request system system-mode logger  
|   |   | 2. Enter **Yes** to confirm the change to Log Collector mode. The appliance will reboot. If you see a CMS Login prompt, press Enter without typing a username or password. When the Panorama login prompt appears, enter the default admin account and the password assigned during initial configuration.  

| Step 4 | Verify that the appliance is in Log Collector mode. | 1. Log back in to the CLI on the M-100 appliance.  
|---|---|---|
|   |   | 2. Enter the following command:  
|   |   | show system info | match system-mode  
|   |   | The response printed on screen reads as  
|   |   | system-mode: logger  
|   |   | If the value displays as **False**, the M-100 appliance is still in Panorama mode.  

| Step 5 | Specify the IP address of the Panorama appliance that is managing the Log Collector. | Enter the following commands in the CLI:  
|---|---|---|
|   |   | configure  
|   |   | set deviceconfig system panorama-server <ip_address>  
|   |   | commit  

Now that you have successfully set up your M-100 appliance, for further instructions on assigning a Log Collector to a firewall, defining Collector Groups, and managing the Log Collector using Panorama, see **Manage Log Collection**.
Increase Storage on the M-100 Appliance

The M-100 appliance ships with two disks in a RAID1 configuration. Each M-100 appliance allows for the addition of up to three additional disk pairs in RAID1, each with a storage capacity of 1TB, to reach a maximum capacity of 4 TB RAID storage.

If adding disk pairs to an already deployed M-100 appliance, you do not need to take the system offline to expand the storage capacity. When the additional disk pairs become available, the M-100 appliance redistributes the logs among the disk pairs. This log redistribution process happens in the background and does not impact uptime or the availability of the M-100 appliance.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Install the new disks in the appropriate drive bays.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Make sure to add the drives sequentially in the next open disk bay slot for the disk pair. For example, add B1/B2 before C1/C2. For information on adding the physical drives, refer to the M-100 Hardware Reference Guide.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Access the command line interface (CLI) on the M-100 appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>You can connect to the M-100 appliance in one of the following ways:</td>
</tr>
<tr>
<td></td>
<td>• Connect a serial cable from your computer to the Console port and connect to the M-100 appliance using terminal emulation software (9600-8-N-1).</td>
</tr>
<tr>
<td></td>
<td>• Use a terminal emulation software such as PuTTY to open a Secure Shell (SSH) session to the IP address of the M-100 appliance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>When prompted, log in to the appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Use the default admin account and the password assigned.</td>
</tr>
</tbody>
</table>
Increase Storage on the M-100 Appliance (Continued)

Step 4  Set up each additional disk pair in a RAID configuration.

The time required to mirror the data on the drive may vary from several minutes to a couple hours, depending on the amount of data on the drive.

This example uses the drives in the disk 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:

<table>
<thead>
<tr>
<th>Disk Pair</th>
<th>Status</th>
<th>Disk id</th>
<th>Model</th>
<th>Size</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Available</td>
<td>A1</td>
<td>ST91000640NS</td>
<td>953869 MB</td>
<td>active sync</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A2</td>
<td>ST91000640NS</td>
<td>953869 MB</td>
<td>active sync</td>
</tr>
<tr>
<td>B</td>
<td>Available</td>
<td>B1</td>
<td>ST91000640NS</td>
<td>953869 MB</td>
<td>active sync</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B2</td>
<td>ST91000640NS</td>
<td>953869 MB</td>
<td>active sync</td>
</tr>
</tbody>
</table>

Step 5  Make the disk pair available for logging.

To enable the disk pairs for logging, this appliance must have been added as a managed collector on Panorama. If you have not already added it, see Managed Collector Groups.

1. Access the Panorama management server that is managing this Log Collector (if it is a different appliance).
2. On the Panorama > Managed Collectors tab, select the Log Collector and follow the instructions in Step 10 in Manage Collector Groups.
3. Click Commit, for the Commit Type select Panorama, and click Commit again.

For further instructions on adding a Log Collector as a managed collector on Panorama, defining Collector Groups, or assigning a Log Collector to a firewall, see Manage Log Collection.
Set Up Panorama

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

On a Panorama virtual appliance that manages 10 or more firewalls and has a logging rate of over 10,000 logs per second, migrating to the M-100 appliance will provide improved response time on the web interface and speedier execution of reports. The M-100 appliance also provides up to 4TB of RAID storage. Use the instructions in the following topics to migrate the configuration from the Panorama virtual appliance over to an M-100 appliance.

▲ Prerequisites for Migrating to an M-100 Appliance
▲ Plan to Migrate to an M-100 Appliance
▲ Migrate to an M-100 Appliance
▲ Resume Firewall Management after Migrating to an M-100 Appliance

Prerequisites for Migrating to an M-100 Appliance

The following are prerequisites for migrating your current subscription:

☐ Purchase an M-100 appliance.
☐ Obtain a migration upgrade and purchase a new subscription that includes software and hardware support.
☐ Provide your sales representative the serial number of the Panorama virtual appliance you will phase out, the desired support terms for the M-100 appliance, the auth-code you received when you purchased the appliance, and the effective date for the migration. On the effective date, Palo Alto Networks will automatically apply the associated auth-codes to the serial number of your management appliance, phase out support for the Panorama virtual appliance, and trigger support for the M-100 appliance. Starting at the effective date, you will have a limited time to complete the migration. At the end of the period, Palo Alto Networks terminates the support entitlement on the Panorama virtual appliance and you can no longer receive software or threat updates. For details on the license migration process, refer to the Knowledge Base article Panorama VM License Migration to the M-100 Platform.

Plan to Migrate to an M-100 Appliance

☐ Plan on completing this migration during a maintenance window. Although the firewalls can buffer the logs and forward them to Panorama when the connection is reestablished, completing the migration during a maintenance window minimizes loss of log data during the transition time when the Panorama virtual appliance goes offline and the M-100 appliance comes online.
☐ Consider whether to maintain access to the Panorama virtual appliance after completing the migration. Because the log format on the Panorama virtual appliance is incompatible with that on the M-100 appliance, existing log data cannot migrate over to the M-100 appliance. Therefore, to access the old logs the Panorama virtual appliance must remain accessible.
☐ Decide whether to use the same IP address on the M-100 appliance or to assign a new one. Palo Alto Networks recommends reusing the same management IP address to prevent the need to reconfigure each managed firewall to point to a new IP address.
Keep a new IP address at hand for use in setting up connectivity to the M-100 appliance during initial configuration. If you have decided to transfer the IP address that was assigned to the Panorama virtual appliance, this new IP address will be used temporarily. When you restore the configuration file from the Panorama virtual appliance on the M-100 appliance, this new IP address will be overwritten.

Migrate to an M-100 Appliance

To migrate the configuration from the Panorama virtual appliance to the M-100 appliance, you must perform tasks on the Panorama virtual appliance and on the M-100 appliance.

Complete the following tasks on the Panorama virtual appliance:

### Migrate to an M-100 Appliance: Tasks Performed on the Panorama Virtual Appliance

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Upgrade to the latest Panorama version.</th>
<th>See Install Content and Software Updates for Panorama.</th>
</tr>
</thead>
</table>
| **Step 2** | Export the running configuration on the virtual Panorama. | 1. In the **Panorama > Setup > Operations** tab, **Configuration Management** section, select **Export named Panorama configuration snapshot**.  
2. Select the active configuration (running-config.xml) and click **OK**. The file is downloaded and saved to the local machine.  
3. Rename the file. |
| **Step 3** | Power off the VM or change the IP address. | If you plan on reusing the MGT interface IP address that was configured on the Panorama virtual appliance on the M-100 appliance, you can either power off the virtual appliance or assign a new IP address to the MGT port on the virtual appliance.  
To change the IP address, on the **Panorama > Setup** tab, edit the **Management Interface Settings** section and enter the new IP address. |

Complete the following tasks on the Panorama M-100 appliance:

### Migrate to an M-100 Appliance: Tasks Performed on the M-100 Appliance

| Step 1 | Set up network access. | See Perform Initial Configuration of the M-100 Appliance for instructions.  
Consider assigning a new temporary IP address during initial configuration on the M-100 appliance and reusing the IP address that was assigned to the Panorama virtual appliance. The temporary IP address will be overwritten when you import the configuration later in this process. |
### Migrate to an M-100 Appliance: Tasks Performed on the M-100 Appliance (Continued)

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Install the same Panorama version as that running on the Panorama virtual appliance.</th>
<th>Install the same Panorama version that you selected in Step 1 above. For instructions on performing the upgrade, see Install Content and Software Updates for Panorama.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Register Panorama and retrieve the license.</td>
<td>See Register Panorama and Install Licenses.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Upgrade to the latest Panorama version.</td>
<td>See Install Content and Software Updates for Panorama.</td>
</tr>
</tbody>
</table>
| Step 5 | Import and load the configuration file. | 1. In the **Panorama > Setup > Operations** tab, Configuration Management section, select **Import named Panorama configuration snapshot**.  
2. **Browse** to select the running-config.xml (or the renamed file) and click **OK**.  
3. Select the **Load named Panorama configuration snapshot** link to load the configuration file you just imported. Any errors that occur when loading the configuration file are displayed onscreen.  
4. If errors occurred, save them to a local file. Review and resolve each error to ensure the migration included all configuration components. |
| Step 6 | Review and modify the configuration on Panorama. | 1. If you do not plan to reuse the same network access settings for the MGT interface, modify the values:  
a. Select **Panorama > Setup** and edit the Management Interface Settings.  
b. Enter the **IP Address**, **Netmask**, and **Default Gateway**.  
c. Confirm that the list of IP addresses defined in the Permitted IP Addresses list is accurate.  
2. To change the hostname, edit the General Settings section of the **Panorama > Setup** tab.  
3. Confirm that the administrative access settings (administrators, roles, and access domains) configured on the appliance are accurate on the **Panorama > Administrators** tab, **Panorama > Admin Roles** tab, and **Panorama > Access Domains** tab. |
| Step 7 | Add the default Log Collector back to the M-100 appliance. | When importing the configuration from the Panorama virtual appliance, the default Log Collector is removed from the M-100 appliance. To add the Log Collector back on the M-100 appliance, use the instructions in Manage Collector Groups. |
| Step 8 | Save all your changes to Panorama. | After reviewing the configuration changes, click **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again. |
Resume Firewall Management after Migrating to an M-100 Appliance

To resume central management, you must restore connectivity to the managed firewalls. Complete this task during a maintenance window to minimize network disruption.

### Resume Firewall Management after Migrating to an M-100 Appliance

#### Step 1
Log in to Panorama.

Using a secure connection (HTTPS) from a web browser, log in using the IP address (https://<IP address>), username, and password assigned during initial configuration.

#### Step 2
Synchronize the configuration on Panorama with those of the managed firewalls.

1. Select **Panorama > Managed Devices**, and verify that the **Connected** status of each device displays a check mark.
   
   The status for the templates and device groups will display an **Out of sync** icon.

2. To synchronize the device groups, click **Commit**, for the **Commit Type** select **Device Group**, select every device group, and click **Commit** again.

3. To synchronize the templates:
   a. Click **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.

   b. Click **Commit**, for the **Commit Type** select **Template**, select the firewalls, and click **Commit** again.

#### Step 3
Verify the connection and synchronization status of the managed firewalls.

1. Select **Panorama > Managed Devices**.

2. Verify the Status of the following for each firewall:
   - In the **Connected** column, a check mark indicates the firewall is connected to Panorama.
   - In the **Shared Policy** column, the value **In sync** indicates the firewall configuration is synchronized with the device group in Panorama.
   - In the **Template** column, the value **In sync** indicates the firewall configuration is synchronized with the template in Panorama.
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 devices and obtain support. The device management license enforces the maximum number of devices that Panorama can manage. The support license enables Panorama software updates and dynamic content updates for the latest Applications and Threats signatures, among other updates that Palo Alto Networks publishes. To purchase licenses, contact your Palo Alto Networks Systems Engineer or reseller.

- Register Panorama
- Activate a Panorama Support License
- Activate/Retrieve a Device Management License on the Panorama Virtual Appliance
- Activate/Retrieve a Device Management License on the M-100 Appliance

If you are running an evaluation license for device 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 Device Management License on the Panorama Virtual Appliance.

Register Panorama

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log in to the Panorama web interface. Using a secure connection (https://&lt;IP address&gt;) from a web browser, log in using the IP address and password you assigned during initial configuration.</td>
</tr>
</tbody>
</table>
| 2    | Record the Panorama serial number or auth-code and record your Sales Order Number or Customer ID. 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 platform:  
  - M-100 appliance—See the Dashboard tab, General Information section, Serial # field.  
  - Panorama virtual appliance—See the order fulfillment email. |
| 3    | Go to the Palo Alto Networks Support site. In a new browser tab or window, go to https://support.paloaltonetworks.com. |
Register Panorama (Continued)

Step 4  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 do not yet have a login:
  a. Click Register on the right side of the page, enter your Email Address, enter the code displayed on the page, and click Submit.
  b. Complete the fields in the Create Contact Details section.
  c. Enter a Display Name, Confirm Email Address, and Password/Confirm Password.
  d. Enter the Panorama Device Serial Number or Auth Code.
  e. Enter your Sales Order Number or Customer ID.
  f. Click Submit.

- If you already have a support account:
  a. Log in to the Support site, click the Assets tab, and click Register New Device.
  b. Enter the Panorama Device Serial Number.
  c. Enter your City, Postal Code, and Country.
  d. Click Submit.

Activate a Panorama Support License

Before activating a Panorama support license on a Panorama M-100 appliance or Panorama virtual appliance, you must Register Panorama.

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.
Set Up Panorama

Register Panorama and Install Licenses

Activate/Retrieve a Device Management License on the Panorama Virtual Appliance

Before activating and retrieving a device 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 Device Management License on the Panorama Virtual Appliance

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

**Step 2** Enter the Panorama Serial Number (included in the order fulfillment email) and click OK.

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

To determine how many firewalls a license enables the Panorama virtual appliance to manage, log in to the Palo Alto Support website (https://support.paloaltonetworks.com), select the Assets tab, find the Panorama device, and view the Model Name. For example, a license for the PAN-PRA-25 model can manage 25 devices. This page also displays the Expiration Date and other license information.

---

**Activate/Retrieve a Device Management License on the M-100 Appliance**

Before activating and retrieving a Panorama device management license on the M-100 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 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 devices that the license enables Panorama to manage.

To activate and retrieve the license, the options are:

**Activate/Retrieve a Device Management License on the M-100 Appliance**

- Use the web interface to activate and retrieve the license.
  
  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-100 Appliance) but you have not activated the license on the Palo Alto Networks Support website.

1. Select Panorama > Licenses and click Activate feature using authorization code.
2. Enter the Authorization Code and click OK. Panorama retrieves and activates the license.
Activate/Retrieve a Device Management License on the M-100 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-100 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.

- 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-100 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 the license on the Palo Alto Networks Support website.
   a. On a host with Internet access, access the Palo Alto Support website (https://support.paloaltonetworks.com) in a browser and log in.
   b. In the Assets tab, find your M-100 appliance and, in the Action column, click the icon.
   c. Enter the Authorization Code and click Add to activate the license.

2. Configure Panorama to connect to the update server: see Perform Initial Configuration of the M-100 Appliance.

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

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

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

6. 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 with HA Configuration
- Install Updates for Panorama with Internet Connection
- Install Updates for Panorama without Internet Connection

Panorama, Log Collector, and Firewall Version Compatibility

Palo Alto Networks highly recommends running the same Panorama software version on both the Panorama management server and the Dedicated Log Collectors.

The Panorama software version on the Panorama management server must be the same as or later than the PAN-OS version on the managed firewalls.

⚠️ Panorama 6.1 and later versions can’t push configurations to firewalls running PAN-OS 6.0.3 or earlier versions. Therefore, only upgrade to Panorama to 6.1 or later versions if, before pushing configurations, you will also upgrade all managed firewalls to PAN-OS 6.0.4 or later versions.

The content release versions on the Panorama management server must be the same as or higher than the content release versions on the Dedicated Log Collectors and managed firewalls. Palo Alto Networks recommends that you install the same Applications and Threats database version on Panorama as on the Dedicated Log Collectors and firewalls. Panorama uses the Applications and Threats database to retrieve metadata for processing reports that you initiate from Panorama or managed devices. If a Dedicated Log Collector does not have the database installed, the complete dataset required for the report might not be available and the information displayed might be incomplete or inaccurate. Firewalls use the database to match the identifiers recorded in the logs with the corresponding threat, URL, or application names.

Install Updates for Panorama with HA Configuration

To ensure a seamless failover, the primary and secondary Panorama peers in an HA pair must have the same Panorama version and the same versions of the Applications and Threat databases.

The following example describes how to upgrade an HA pair with an active-primary peer named Primary_A and the passive-secondary peer named Secondary_B.
Install Updates for Panorama with HA Configuration

| Step 1 | Upgrade the Panorama software version on Secondary_B, the passive-secondary peer. | Perform one of the following tasks:  
• Install Updates for Panorama with Internet Connection  
• Install Updates for Panorama without Internet Connection  
After the upgrade, this Panorama will transition to a non-functional state because the OS version does not match that of its peer. |
|---|---|---|
| Step 2 | Suspend Primary_A to trigger a failover. | On Primary_A:  
1. Select **Panorama > High Availability**.  
2. In the **Operational Commands** section, click **Suspend local Panorama** to suspend this peer.  
3. Verify that the state displays as suspended; the state displays in the bottom-right corner of the web interface.  
Placing Primary_A in a suspended mode triggers a failover and Secondary_B transitions to active-secondary state. |
| Step 3 | Upgrade the Panorama software version on Primary_A. | Perform one of the following tasks:  
• Install Updates for Panorama with Internet Connection  
• Install Updates for Panorama without Internet Connection  
After rebooting, Primary_A first transitions to the passive-primary state. Then, because preemption is enabled by default, Primary_A will automatically transition to the active-primary state and Secondary_B will revert to the passive-secondary state.  
If you disabled preemption, see **Restore the Primary Panorama to the Active State**. |
| Step 4 | Verify that the Panorama software version and other content database versions are the same on both peers. | On the **Dashboard** of each Panorama peer, verify that the Panorama Software Version and Application Version match and that the running configuration is synchronized with the peer. |

Install Updates for Panorama with Internet Connection

If Panorama has a direct connection to the Internet, perform the following steps to install content and software updates.

Before deploying updates, see **Panorama, Log Collector, and Firewall Version Compatibility** for critical details about update version compatibility among Palo Alto Networks devices.

Before upgrading a Panorama virtual appliance, ensure the ESXi host meets the minimum resource requirements listed under **Setup Prerequisites for the Panorama Virtual Appliance**.

When upgrading software or content versions, you must upgrade the Panorama management server first, the Dedicated Log Collectors (M-100 appliances in Log Collector mode) second, and the firewalls last.
## Install Updates for Panorama with Internet Connection

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Check for, download, and install the latest content updates.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>You must install the content updates before the software updates. Also, you must install the Applications and Threats updates before the Antivirus and WildFire updates.</td>
</tr>
<tr>
<td></td>
<td>1. Select <strong>Panorama &gt; Dynamic Updates</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Check Now</strong> to check for the latest updates. If the value in the Action column is <strong>Download</strong>, an update is available.</td>
</tr>
<tr>
<td></td>
<td>3. Perform the following steps for each content type:</td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Download</strong> in the Action column to obtain the desired version.</td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>Install</strong> in the Action column. When the installation completes, the Currently Installed column displays a check mark.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Check for, download, and install the latest software update.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Select <strong>Panorama &gt; Software</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Check Now</strong> to check for the latest update. If an update is available, the Action column displays a <strong>Download</strong> link.</td>
</tr>
<tr>
<td></td>
<td>3. Review the Version column to determine the version to which you want to upgrade.</td>
</tr>
<tr>
<td></td>
<td>4. In the Action column of the desired version, click <strong>Download</strong>. When the download completes, the value in the Action column changes to <strong>Install</strong>.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Install</strong>.</td>
</tr>
<tr>
<td></td>
<td>6. Reboot Panorama:</td>
</tr>
<tr>
<td></td>
<td>• If prompted to reboot, click <strong>Yes</strong>. If you see a <strong>CMS Login</strong> prompt, press Enter without typing a username or password. When the Panorama login prompt appears, enter the username/password you set during initial configuration.</td>
</tr>
<tr>
<td></td>
<td>• Otherwise, select <strong>Panorama &gt; Setup &gt; Operations</strong> and, in the Device Operations section, click <strong>Reboot Panorama</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>(Only required if upgrading a Panorama virtual appliance to Panorama 5.1 or later versions) Modify the settings on the Panorama virtual appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Before powering on a Panorama virtual appliance that runs Panorama 5.1 or a later version, ensure that the ESXi host meets the minimum requirements for a 64-bit operating system (OS). For details, see <strong>Setup Prerequisites for the Panorama Virtual Appliance</strong>.</td>
</tr>
<tr>
<td></td>
<td>After Panorama reboots, complete the following tasks on the vSphere web client:</td>
</tr>
<tr>
<td></td>
<td>1. Power off the virtual appliance.</td>
</tr>
<tr>
<td></td>
<td>2. Right-click the Panorama virtual appliance and select <strong>Edit Settings</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Select the <strong>Options</strong> tab and change the <strong>Guest Operating System</strong> from <strong>Other Linux (32-bit)</strong> to <strong>Other Linux (64-bit)</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Select the <strong>Hardware</strong> tab and change:</td>
</tr>
<tr>
<td></td>
<td>• <strong>SCSI Controller</strong> from <strong>BusLogic Parallel</strong> to <strong>LSI Logic Parallel</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Memory allocation to at least 4GB (for less than 10 firewalls) or 16GB (for 10 or more firewalls).</td>
</tr>
<tr>
<td></td>
<td>5. Power on the virtual appliance.</td>
</tr>
</tbody>
</table>
Install Updates for Panorama without Internet Connection

If Panorama does not have a direct connection to the Internet, perform the following steps to install **Install Content and Software Updates for Panorama**.

**Before deploying updates, see Panorama, Log Collector, and Firewall Version Compatibility** for critical details about update version compatibility among Palo Alto Networks devices.

Before upgrading a Panorama virtual appliance, ensure the ESXi host meets the minimum resource requirements listed under Setup Prerequisites for the Panorama Virtual Appliance.

When upgrading software or content versions, you must upgrade the Panorama management server first, the Dedicated Log Collectors (M-100 appliances in Log Collector mode) second, and the firewalls last.

---

### Install Updates for Panorama without Internet Connection

**Step 1**

Download the content and software updates to a host that has Internet access. Panorama must have access to the host.

1. **On a host with Internet access**, access the Palo Alto Support website ([https://support.paloaltonetworks.com](https://support.paloaltonetworks.com)) in a browser and log in.

2. In the Resources section, click **Dynamic Updates**.

3. In the section containing the desired content update, click **Download** and save the file to the host. Perform this step for each content type for which you have a subscription: Applications, Applications and Threats, Antivirus, and/or Wildfire.

4. Return to the main page of the Palo Alto Support website and, in the Resources section, click **Software Updates**.

5. Review the Download column to determine the version to install. The filename of the update package indicates the platform: Panorama-ESX-<release> for the Panorama virtual appliance or Panorama-m-<release> for Panorama M-100 appliance.

6. Click the filename and save the file to the host.

**Step 2**

Upload and install the content updates to Panorama.

You must install the content updates before the software updates. Also, you must install the Application and Threat updates before the Antivirus and WildFire updates.

1. Log in to Panorama and select **Panorama > Dynamic Updates**.

2. Perform the following steps for each content type:

   a. Click **Upload**, select the content **Type**, enter the path to the content update **File** or **Browse** to it, click **OK**, and click **Close** when the Status is Completed.

   b. Click **Install From File**, select the **Package Type**, click **OK**, and click **Close** when the Result is Succeeded.
### Install Updates for Panorama without Internet Connection (Continued)

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Upload and install the software update.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>In the Panorama &gt; Software page, click Upload.</td>
</tr>
<tr>
<td>2.</td>
<td>Enter the path to the software update File or Browse to it, select the Sync To Peer check box if Panorama is in a high availability (HA) configuration (to push the software image to the secondary peer), and click OK.</td>
</tr>
<tr>
<td>3.</td>
<td>Click Install in the Action column.</td>
</tr>
<tr>
<td>4.</td>
<td>Reboot Panorama:</td>
</tr>
<tr>
<td></td>
<td>• 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 set during initial configuration.</td>
</tr>
<tr>
<td></td>
<td>• Otherwise, select Panorama &gt; Setup &gt; Operations and, in the Device Operations section, click Reboot Panorama.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>(Only required if upgrading a Panorama virtual appliance to Panorama 5.1 or later versions) Modify the settings on the Panorama virtual appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Before powering on a Panorama virtual appliance that runs Panorama 5.1 or a later version, ensure that the ESXi host meets the minimum requirements for a 64-bit operating system (OS). For details, see Setup Prerequisites for the Panorama Virtual Appliance.</td>
</tr>
<tr>
<td></td>
<td>After Panorama reboots, complete the following tasks on the vSphere web client:</td>
</tr>
<tr>
<td></td>
<td>1. Power off the virtual appliance.</td>
</tr>
<tr>
<td></td>
<td>2. Right-click the Panorama virtual appliance and select Edit Settings.</td>
</tr>
<tr>
<td></td>
<td>3. Select the Options tab and change the Guest Operating System from Other Linux (32-bit) to Other Linux (64-bit).</td>
</tr>
<tr>
<td></td>
<td>4. Select the Hardware tab and change:</td>
</tr>
<tr>
<td></td>
<td>• SCSI Controller from BusLogic Parallel to LSI Logic Parallel.</td>
</tr>
<tr>
<td></td>
<td>• Memory allocation to at least 4GB (for less than 10 firewalls) or 16GB (for 10 or more firewalls).</td>
</tr>
<tr>
<td></td>
<td>5. Power on the virtual appliance.</td>
</tr>
</tbody>
</table>
Access and Navigate Panorama Management Interfaces

Panorama provides three management interfaces:

- **Web interface**—The Panorama web interface is purposefully designed with a similar look and feel to the firewall web interface. If you are already familiar with the latter, you can navigate, complete administrative tasks, and generate reports from the Panorama web interface with relative ease. This graphical interface allows 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 through the commands in rapid succession to complete a series of tasks. The CLI supports two command modes—operational and configuration—and each mode has its own hierarchy of commands and statements. When you get familiar with the nesting structure and the syntax for the commands, the CLI allows quick response times and offers 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 allows you to streamline your operations and integrate with existing, internally developed applications and repositories. For information on how to use the Panorama API interface, refer to the document PAN-OS and Panorama XML-Based API. To access the online community for developing scripts, visit https://live.paloaltonetworks.com/community/devcenter.

### Log in to the Panorama Web Interface

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in to the Panorama web interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Using a secure connection (https) from a web browser, log in using the IP address and password you assigned during initial configuration (https://&lt;IP address&gt;).</td>
</tr>
</tbody>
</table>

**Step 2** (Optional) Enable HTTP and Secure Shell (SSH) access.

1. Select **Panorama > Setup > Management** and edit the Management Interface Settings.
2. Select which management services to allow on the interface. For example, select **HTTP** and **SSH**.
3. Click **OK**.

### Navigate the Panorama Web Interface

Use the Panorama web interface to configure Panorama, manage and monitor the managed firewalls and Log Collectors, and to access the web interface of each managed firewall using the Device Context. Refer to the online help on Panorama for details on the options in each tab in the web interface.

The Panorama web interface includes the following tabs:
### Set Up Panorama Access and Navigate Panorama Management Interfaces

You can log in to the Panorama CLI using a serial port connection or access remotely using a Secure Shell (SSH) client.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>View general information about the Panorama model 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>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>
<tr>
<td>Device Groups &gt; Policies</td>
<td>Create centralized policies and apply the configuration to multiple firewalls/device groups.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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, that can be applied to the managed firewalls.</td>
</tr>
<tr>
<td></td>
<td>You must Add a Template for this tab to display.</td>
</tr>
<tr>
<td>Templates &gt; Device</td>
<td>Configure device configuration, such as server profiles and admin roles, that can be applied to the managed firewalls.</td>
</tr>
<tr>
<td></td>
<td>You must Add a Template for this tab to display.</td>
</tr>
<tr>
<td><strong>Log in to the Panorama CLI</strong></td>
<td>1. Make sure that you have the following:</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>1. Use SSH to log in to the Panorama CLI.</td>
<td>• A computer with network access to Panorama</td>
</tr>
<tr>
<td>The same instructions apply for an M-100 appliance in Log Collector mode.</td>
<td>• Panorama IP address</td>
</tr>
<tr>
<td>2. To access the CLI using SSH:</td>
<td>• SSH is enabled on the Management interface. See (Optional) Enable HTTP and Secure Shell (SSH) access.</td>
</tr>
<tr>
<td>a. Enter the Panorama IP address in the SSH client and use port 22.</td>
<td></td>
</tr>
<tr>
<td>b. Enter your administrative access credentials when prompted. After successfully logging in, the CLI prompt displays in Operational mode. For example:</td>
<td>See Configure an Administrator with SSH Key-Based Authentication for the CLI.</td>
</tr>
<tr>
<td>admin@ABC_Sydney&gt; configure</td>
<td></td>
</tr>
<tr>
<td>The prompt changes to admin@ABC_Sydney#</td>
<td></td>
</tr>
<tr>
<td>3. Change to Configuration mode.</td>
<td>1. Make sure that you have the following:</td>
</tr>
<tr>
<td>To go into Configuration mode, enter the following command at the prompt:</td>
<td>• A null-modem serial cable that connects Panorama to a computer with a DB-9 serial port</td>
</tr>
<tr>
<td>admin@ABC_Sydney&gt; configure</td>
<td>• A terminal emulation program running on the computer</td>
</tr>
<tr>
<td>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.</td>
<td>3. Enter your administrative access credentials when prompted.</td>
</tr>
<tr>
<td>3. Use a serial port connection to log in to the Panorama CLI.</td>
<td></td>
</tr>
</tbody>
</table>
Set Up Administrative Access to Panorama

Panorama implements Role-Based Access Control (RBAC) to enable you to specify the privileges and responsibilities of administrators.

You can't add an administrator account to a Dedicated Log Collector (M-100 appliance in Log Collector mode). Only the predefined administrator account with the default username (admin) is available on Dedicated Log Collectors.

The following topics describe how to create administrator accounts and configure Administrative Authentication to the Panorama web interface and command line interface (CLI):

- 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 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log in to the KDC and open a command prompt.</td>
</tr>
</tbody>
</table>
| 2.   | Enter the following command, where `<principal_name>`, `<password>`, and `<algorithm>` are variables. The Kerberos principal name and password are for Panorama, not the administrator.  

```
  ktpass /princ <principal_name> /pass <password> /crypto <algorithm> /ptype KRB5_NT_PRINCIPAL /out <file_name>.keytab
```

The algorithm in the keytab must match the algorithm in the service ticket that the TGS issues to clients. Your Kerberos administrator determines which algorithms the service tickets use. The options are:

- `des3-cbc-sha1`
- `arcfour-hmac`
- `aes128-cts-hmac-sha1-96`
- `aes256-cts-hmac-sha1-96`

To use an Advanced Encryption Standard (AES) algorithm, the functional level of the KDC must be Windows Server 2008 or later and you must enable AES encryption for the Panorama account. |
### Configure an Administrator with Kerberos SSO, External, or Local Authentication (Continued)

**Step 2** Configure Access Domains.

Applicable only to Device Group and Template roles.

Panorama supports up to 4,000 access domains.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select <strong>Panorama &gt; Access Domain</strong> and click <strong>Add</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Enter a <strong>Name</strong> to identify the access domain.</td>
</tr>
</tbody>
</table>
| 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 shared objects but cannot perform other operations on them. 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 if your organization requires all objects to be in a single, global repository. |
| 4.   | In the **Device Groups** tab, toggle the icons 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. |
| 5.   | In the **Templates** tab, **Add** each template you want to assign to the access domain. |
| 6.   | In the **Device Context** tab, select check boxes to assign firewalls to the access domain and click **OK**. Administrators can switch context to these firewalls. |
Set Up Panorama

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

Step 3 Configure an Admin Role profile.
Applicable only if you will assign a custom role to the administrator; dynamic roles are predefined.
For details on the role types and the privileges available to each, see Administrative Roles.

1. Select Panorama > Admin Roles and click Add.
2. Enter a Name for the profile and select the Role type: Panorama or Device Group and Template.
3. Configure access to Panorama (Web UI) and firewalls (Context Switch UI) for each functional area by toggling its icon to the desired setting: Enable (read-write), Read Only, or Disable. For details on the options, refer to Reference: Web Interface Administrator Access.

   If administrators with custom roles will commit device group or template changes to managed firewalls, you must give those roles read-write or read-only access to Panorama > Device Groups and/or Panorama > Templates. If you upgrade from an earlier Panorama version, the upgrade process provides read-only access to those nodes.

   No predefined roles restrict access to a firewall CLI or XML API. Therefore, to prevent privilege-level escalation, Panorama doesn’t let you manage access to those interfaces through context-switching privileges.

4. If the Role type is Panorama, configure access to the XML API functional areas by toggling the icons to Enable or Disable.
5. If the Role type is Panorama, select an access level for the Command Line interface: None (default), superuser, superreader, or panorama-admin.
6. Click OK to save the profile.

Step 4 (Optional) Set the password requirements.
Password requirements apply only to local authentication.

- Create Password Profiles—Define how often administrators must change their passwords. You can create multiple password profiles and apply them to administrator accounts as needed to enforce the desired security. To create a password profile, select Panorama > Password Profiles and click Add.

- Configure minimum password complexity settings—Define the rules that govern password complexity. You can define rules that force administrators to create passwords that are harder to guess, crack, or compromise. Unlike password profiles, which apply to individual accounts, these rules are device-wide and apply to all passwords. To configure the settings, select Panorama > Setup and edit the Minimum Password Complexity section.

Step 5 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.
## Configure an Administrator with Kerberos SSO, External, or Local Authentication (Continued)

### Step 6
Configure an authentication profile.

Applicable only if you will use Kerberos SSO or external authentication.

An authentication profile defines how Panorama authenticates an administrator. You can define one or both of the following authentication phases:

- **Kerberos SSO**—Panorama first tries SSO authentication and, if that fails, falls back to username/password authentication of the **Type** specified in the profile.
- **External authentication**—The device prompts the administrator to enter login credentials and uses an external service for 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 (Step 7). Then assign the same authentication sequence to all administrators (Step 8). For details, see [Authentication Profiles and Sequences](#).

1. Select **Panorama > Authentication Profile** and click **Add**.
2. Enter a **Name** to identify the authentication profile.
3. If the authentication **Type** is an external service, select the authentication **Server Profile** you created.
   - If the **Type** is LDAP, define the **Login Attribute**. For Active Directory, enter `sAMAccountName` as the value.
4. (Optional) Specify **User Domain** and **Username Modifier** values to modify the domain/username string that the administrator will enter during login. This is useful when the authentication service requires strings in a particular format and you don’t want to rely on administrators to correctly enter the domain. Select from the following options:
   - To send only the unmodified administrator input, leave the **User Domain** blank (the default) and set the **Username Modifier** to the variable `%USERINPUT%` (the default).
   - To prepend a domain to the administrator input, enter a **User Domain** and set the **Username Modifier** to `%USERDOMAIN%\%USERINPUT%`.
   - To append a domain to the administrator input, enter a **User Domain** and set the **Username Modifier** to `%USERINPUT%@%USERDOMAIN%`.
5. If you want to enable Kerberos SSO, enter the **Kerberos Realm** (usually the DNS domain of the administrators, except that the realm is uppercase) and **Import** the **Kerberos Keytab** that you created for Panorama.
6. Select the **Advanced** tab and add the administrators and groups that can authenticate with this profile. By default, the list is empty, meaning no administrators can authenticate.
7. Enter the number of **Failed Attempts** (0-10) to log in that Panorama allows before locking out the administrator. The default value 0 means there is no limit.
8. Enter the **Lockout Time** (0-60), which is the number of minutes for which Panorama locks out the administrator after reaching the **Failed Attempts** limit. The default value 0 means the lockout applies until you manually unlock the administrator account.
9. Click **OK** to save the authentication profile.
Configure an Administrator with Certificate-Based Authentication for the Web Interface

As a more secure alternative to using a password to authenticate a user, enable certificate-based authentication for securing access to Panorama. With certificate-based authentication, a digital signature is exchanged and verified, in lieu of a password.

### Set Up Panorama Set Up Administrative Access to Panorama

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Configure an authentication sequence.</th>
<th>1. Select <strong>Panorama &gt; Authentication Sequence</strong> and click <strong>Add</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Applicable only if you want Panorama to try multiple authentication profiles to authenticate administrators.</td>
<td>2. Enter a <strong>Name</strong> to identify the authentication sequence.</td>
</tr>
<tr>
<td></td>
<td>Panorama tries the profiles sequentially—applying the Kerberos SSO, authentication service, allow list, and account lockout values for each—until one profile successfully authenticates the administrator. Panorama denies access only if all the profiles in the sequence fail to authenticate.</td>
<td><strong>To expedite the authentication process, the best practice is to select the Use domain to determine authentication profile check box:</strong> Panorama will match the domain name that an administrator enters during login with the <strong>User Domain</strong> or <strong>Kerberos Realm</strong> of an authentication profile in the sequence, and then use that profile to authenticate the administrator. If Panorama doesn't find a match, or if you clear the check box, Panorama tries the profiles in the regular top-to-bottom sequence. The check box is selected by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. <strong>Add</strong> the authentication profiles. To change the order in which Panorama tries the profiles, select a profile and click <strong>Move Up</strong> or <strong>Move Down</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>OK</strong> to save the authentication sequence.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Configure an administrator.</th>
<th>1. Select <strong>Panorama &gt; Administrators</strong> and click <strong>Add</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2. Enter a <strong>Name</strong> for the administrator.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. If Panorama will use Kerberos SSO or an external service for authentication, select the <strong>Authentication Profile</strong> you created. If Panorama will use local authentication, set the <strong>Authentication Profile</strong> to <strong>None</strong> and enter the <strong>Password/Confirm Password</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. For the <strong>Administrator Type</strong>, select the role type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Dynamic</strong>—Select a predefined administrator role.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Custom Panorama Admin</strong>—Select the Admin Role Profile you created for this administrator.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Device Group and Template Admin</strong>—In the Access Domain to Administrator Role section, add access domains and map each one to an Admin Role profile: click <strong>Add</strong>, select an Access Domain from the drop-down, click the adjacent Admin Role cell, and select an Admin Role profile.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. (Optional—local authentication only) Select a <strong>Password Profile</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. 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>
To enable certificate-based authentication, you must configure Panorama to use a client certificate profile (as described in the following procedure). When you enable a client certificate profile, each administrator must use a client certificate for access to Panorama.

This example uses a CA certificate generated on Panorama.

### Configure an Administrator with Certificate-Based Authentication for the Web Interface

**Step 1** Generate a CA certificate on Panorama.

To use a certificate from a trusted third-party or enterprise CA, you must import that CA certificate into Panorama.

1. Log in to the Panorama web interface.
2. Select Panorama > Certificate Management > Certificates and click Generate.
3. Enter a **Certificate Name**. Add the IP address or FQDN of Panorama for listing in the **Common Name** field of the certificate. Optionally, you can change the cryptographic settings, and define certificate options such as country, organization, or state.
4. Make sure to leave the **Signed By** option blank and select the **Certificate Authority** option.
5. Click **Generate** to create the certificate using the details you specified above.

**Step 2** Create and export the client certificate that will be used to authenticate an administrator.

1. Use the CA certificate to generate a client certificate for the specified administrative user.
   a. Select Panorama > Certificate Management > Certificates and click Generate.
   b. In the **Common Name** field, enter the name of the administrator for whom you are generating the certificate. The name syntax must match the format used by the local or external authentication mechanism.
   c. In the **Signed by** field, select the CA certificate you just created.
   d. Click **Generate** to create the certificate.
2. Export the client certificate you just generated.
   a. Select the certificate that you just generated and click Export.
   b. To encrypt the private key, select **PKCS12** as the **File Format**.
   c. Enter a passphrase to encrypt the private key and confirm the entry.
   d. Click **OK** to export the certificate.

**Step 3** Add an administrator account or modify an existing one.

Configure an administrator. Select the **Use only client certificate authentication (Web)** check box.
### Configure an Administrator with Certificate-Based Authentication for the Web Interface (Continued)

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Create the client certificate profile that will be used for securing access to the web interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Select <strong>Panorama &gt; Certificate Management &gt; Certificate Profile</strong> and click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Enter a name for the certificate profile and in the <strong>Username Field</strong> select <strong>Subject</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Select <strong>Add</strong> in the CA Certificates section and from the <strong>CA Certificate</strong> drop-down, select the CA certificate you just created.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Configure Panorama to use the client certificate profile for authentication.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. On the <strong>Panorama &gt; Setup</strong> tab, edit the Authentication Settings.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Certificate Profile</strong> field, select the client certificate profile you just created.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>OK</strong> to save your changes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Save the configuration changes. Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Panorama</strong>, and click <strong>Commit</strong> again. You will be logged out of the device.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Import the client certificate of the administrator into the web browser on the client system that the administrator will use to access the Panorama web interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. From a client system that has the client certificate loaded, access the Panorama IP address or hostname.</td>
</tr>
<tr>
<td></td>
<td>2. When prompted, select the client certificate you just imported. A certificate warning will display.</td>
</tr>
<tr>
<td></td>
<td>3. Add the certificate to the exception list and log in to the Panorama web interface.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Verify that certificate-based authentication is configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. For example, in Firefox:</td>
</tr>
<tr>
<td></td>
<td>2. Select <strong>Tools &gt; Options &gt; Advanced</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>View Certificates</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Select the <strong>Your Certificates</strong> tab and click <strong>Import</strong>. Browse to the location where you saved the client certificate.</td>
</tr>
<tr>
<td></td>
<td>5. When prompted, enter the passphrase to decrypt the private key.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Use a Secure Shell (SSH) key generation tool to create an asymmetric keypair on the client machine.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The supported key formats are: IETF SECSH and Open SSH; the supported algorithms are: DSA (1024 bits) and RSA (768-4096 bits).</td>
</tr>
<tr>
<td></td>
<td>For the commands required to generate the keypair, refer to the product documentation for your SSH client.</td>
</tr>
<tr>
<td></td>
<td>The public key and private key are two separate files; save both to a location that can be accessed by Panorama. For added security, enter a passphrase to encrypt the private key. The administrator will be prompted for this passphrase when logging in to Panorama.</td>
</tr>
</tbody>
</table>
### Configure an Administrator with SSH Key-Based Authentication for the CLI (Continued)

<table>
<thead>
<tr>
<th>Step 2 Add an administrator account or modify an existing one.</th>
<th>Configure an administrator.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Select an existing administrator or click Add and enter a user Name for a new administrator.</td>
<td>2. Select an existing administrator or click Add and enter a user Name for a new administrator.</td>
</tr>
<tr>
<td>3. Select the Use Public Key Authentication (SSH) check box.</td>
<td>3. Select the Use Public Key Authentication (SSH) check box.</td>
</tr>
<tr>
<td>4. Click Import Key, click Browse to find the public key you just created, and click OK.</td>
<td>4. Click Import Key, click Browse to find the public key you just created, and click OK.</td>
</tr>
<tr>
<td>5. Click OK and Commit, for the Commit Type select Panorama, and click Commit again.</td>
<td>5. Click OK and Commit, for the Commit Type select Panorama, and click Commit again.</td>
</tr>
</tbody>
</table>

### Step 3 Verify that the SSH client uses the private key to authenticate the public key presented by Panorama.

1. Configure the SSH client to use the private key to authenticate to Panorama.
2. Log in to the CLI on Panorama.
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. For detailed instructions, refer to the following documents:

- 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 VSA**

Before starting this procedure, you must create the administrative accounts in the directory service that your network uses (for example, Active Directory) and set up a RADIUS server that can communicate with that directory service.
## Use RADIUS Vendor-Specific Attributes for Account Authentication

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Configure Panorama.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Configure an Admin Role profile. Select Panorama &gt; Admin Roles. For the Role type, select Device Group and Template.</td>
</tr>
<tr>
<td></td>
<td>3. Configure a RADIUS Server Profile. Select Panorama &gt; Server Profiles &gt; RADIUS.</td>
</tr>
<tr>
<td></td>
<td>4. Configure an authentication profile. Select Panorama &gt; Authentication Profile. For the authentication Type, select RADIUS. Assign the RADIUS Server Profile.</td>
</tr>
<tr>
<td></td>
<td>5. Configure Panorama to use the authentication profile for authentication: select Panorama &gt; Setup &gt; Management, edit the Authentication Settings, and select the Authentication Profile.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Configure the RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Add the Panorama IP address or hostname as the RADIUS client.</td>
</tr>
<tr>
<td></td>
<td>2. Define the VSAs that Panorama supports. To define an attribute, use the vendor code (25461), attribute name (ensure it matches the name of the Admin Role profile/access domain defined on Panorama; it is case sensitive), number, and format (string):</td>
</tr>
<tr>
<td></td>
<td>• PaloAlto-Panorama-Admin-Role, attribute #3</td>
</tr>
<tr>
<td></td>
<td>• PaloAlto-Panorama-Admin-Access-Domain, attribute #4</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:

<table>
<thead>
<tr>
<th>Add a Firewall as a Managed Device</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Add the firewall to Panorama.</td>
<td>1. Select Panorama &gt; Managed Devices and click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. 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 device.</td>
</tr>
<tr>
<td></td>
<td>3. (Optional) Add a <strong>Tag</strong>. Tags make it easier for you to find a device 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 devices across your network.</td>
</tr>
<tr>
<td></td>
<td>a. Select the check box beside the managed device and click <strong>Tag</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>Add</strong>, enter a string of up to 31 characters (no empty spaces), and click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select Panorama, and click <strong>Commit</strong> again.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Verify that the firewall is connected to Panorama.</td>
<td>In the Panorama &gt; Managed Devices page, the Device State column displays whether the firewall is connected or disconnected to Panorama.</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.

**Add a Device Group**

**Step 1** Select Panorama > Device Groups, and click Add.

**Step 2** Enter a unique Name and a Description to identify the device group.

**Step 3** 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.

**Step 4** (Optional) Select the Group HA Peers check box for firewalls that are HA peers.

The firewall name of the passive or active-secondary peer is in parentheses.

**Step 5** Select the Parent Device Group (default is Shared) that will be just above the device group you are creating in the device group hierarchy.

**Step 6** If your policy rules will reference users and groups, assign a Master firewall. This will be the only firewall in the device group from which Panorama gathers username and user group information.

**Step 7** Click OK and Commit, for the Commit Type select Panorama, and click Commit again.

**Step 8** Click Commit, for the Commit Type select Device Group, select the device group you just created, and click Commit again.
## Create a Device Group Hierarchy

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Plan the Device Group Hierarchy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>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 devices to it.</td>
</tr>
</tbody>
</table>
| 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**. |

<table>
<thead>
<tr>
<th>Step 2</th>
<th>For each top-level device group, Add a Device Group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>In the <strong>Panorama &gt; Device Groups</strong> page, click <strong>Add</strong> and enter a <strong>Name</strong> to identify the device group.</td>
</tr>
<tr>
<td>2.</td>
<td>In the Devices section, select check boxes to assign devices and virtual systems to the device group.</td>
</tr>
<tr>
<td>3.</td>
<td>Leave the <strong>Parent Device Group</strong> option at <strong>Shared</strong> (the default) and click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

| Step 3 | For each lower-level device group, Add a Device Group.  
|---|---|
| 1. | 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.  
| 2. | 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**.  
| 3. | If you move a device group to a different parent, all its descendant device groups move with it, along with all devices, 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 Access Domains**. |
Manage Firewalls

Create a Device Group Hierarchy (Continued)

Step 4 Configure, move, and clone objects and policy rules as needed to account for inheritance in the device group hierarchy.

- 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.
- Create or edit policies.
- Move or Clone a Policy Rule or Object to a Different Device Group.

Step 5 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.

1. In the Objects tab, select the object type (for example, Objects > Addresses).
2. Select the Device Group that will have the override instance.
3. Select the object and click Override.
4. Edit the values. You can't edit the Name or Shared settings.
5. Click OK. The Name column displays a yellow-overlapping-green icon for the object to indicate it is overridden.
   If necessary, you can later Revert to Inherited Object Values.

Step 6 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.

1. Click Commit, for the Commit Type select Panorama, and click Commit again.
2. Click Commit, for the Commit Type select Device Group, select all the device groups you added or changed, and click Commit again.

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

- **Create a shared object.**
  
  In this example, we add a shared object for URL Filtering categories for which we want to trigger alerts.
  
  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.

- **Create a device group object.**
  
  In this example, we add an address object for specific web servers on your network.
  
  1. Select **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.

- **View shared objects and device group objects in Panorama.**

  To demonstrate the difference between a shared object and a device group object, the following screenshot includes a shared address object that was created on Panorama.

  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 🟢 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 perform a device group commit, 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.

On lower-end platforms, such as the PA-200, consider pushing only the relevant shared objects to the managed devices. This is because the number of objects that can be stored on the lower-end platforms is considerably lower than that of the mid- to high-end platforms. 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 devices because the configuration pushed to each device 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. |
| Step 2 | Clear the Share Unused Address and Service Objects with Devices check box to push only the shared objects that rules reference, or select the check box to re-enable pushing all shared objects. |
| Step 3 | Click OK and Commit, for the Commit Type select Panorama, and click Commit again. |
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 or the Shared location. 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. 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.]

<table>
<thead>
<tr>
<th>Manage Precedence of Inherited Objects</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>
</tbody>
</table>

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).

<table>
<thead>
<tr>
<th>Move or Clone a Policy Rule or Object to a Device Group</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
</tr>
</tbody>
</table>
Manage Firewalls

Select a URL Filtering Vendor on Panorama

URL Filtering enables you to configure firewalls to monitor and control web access for your users. The policies (Security, QoS, Captive Portal, and Decryption) that enforce web access rules reference URL categories. The URL filtering vendor you select on Panorama determines which URL categories are referenced in the rules that you add to device groups and push to 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 categories that align with those of the vendor enabled on the firewall. For details, refer to the article BrightCloud to PAN-DB Category Mapping.

Move or Clone a Policy Rule or Object to a Device Group (Continued)

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.
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 BrightCloud, and firewalls that run PAN-OS 7.0 use
PAN-DB (or BrightCloud), Panorama must use BrightCloud.

A firewall can have valid licenses for both BrightCloud and PAN-DB, but only one license can be
active. To view the valid URL Filtering licenses on a managed firewall, select Panorama >
Device Deployment > Licenses and check the vendors listed in the URL column for the
corresponding firewall. To determine which license is active (and therefore which URL Filtering
vendor is selected), log in to the firewall and select Device > Licenses. You can change the
active URL Filtering vendor of a firewall.

### Select a URL Filtering Vendor on Panorama

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select a URL filtering vendor for Panorama.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Select Panorama &gt; Setup &gt; Management and edit the General Settings.</td>
</tr>
<tr>
<td></td>
<td>2. Select the vendor in the URL Filtering Database drop-down: brightcloud or paloaltonetworks (PAN-DB).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>(Optional) Verify that the categories are available for referencing in policies.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Unlike firewalls, Panorama does not download the URL database, so you cannot view the database download status.</td>
</tr>
<tr>
<td></td>
<td>2. Click Add and verify that the Categories tab of the URL Filtering profile dialog displays the categories.</td>
</tr>
</tbody>
</table>

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

Step 1 Create a rule.

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.

1. Select the Policies tab and select the Device Group for which you want to define a rule.
2. Select the rulebase. For this example, select Policies > Security > Pre-Rules.
3. Click Add and, in the General tab, enter a descriptive rule Name.
4. In the Source tab, set the Source Zone to Trust.
5. In the Destination tab, set the Destination Zone to DMZ.
6. In the Service/ URL Category tab, set the Service to application-default.
7. In the Actions tab, set the Action to Allow.
8. Leave all the other options at the default values.

Step 2 Target the rule to include or exclude a subset of firewalls.

To apply the rule to a selected set of firewalls:
1. Select the Target tab in the Policy Rule window.
2. Select the firewalls on which you want the rule to apply.
   If you do not select firewalls to target, the rule is added to all of the (unchecked) firewalls in the device group.
   
   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.

3. (Optional) To exclude a subset of firewalls from inheriting the rule, select the check box Install on all but specified devices.
   If you select Install on all but specified devices and do not select any device, the rule is added to none of the firewalls in the device group.

4. Click OK to add the rule.
5. Save the configuration changes.
   a. Click Commit, for the Commit Type select Panorama, and click Commit again.
   b. Click Commit, for the Commit Type select Device Group, select the device group to which you just added the rule, 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.
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 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.
### Manage the Rule Hierarchy (Continued)

<table>
<thead>
<tr>
<th>Step 4</th>
<th>If you modified the rules, save the changes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Panorama</strong>, and click <strong>Commit</strong> again.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Device Group</strong>, select the device group that contains the rules you changed or deleted, and click <strong>Commit</strong> again.</td>
</tr>
</tbody>
</table>
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

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 virtual system (vsys).
- Configure a shared gateway.
- 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).

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.
Manage Firewalls

Manage Templates and Template Stacks

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Add a template.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select <strong>Panorama &gt; Templates</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Add</strong> and enter a unique <strong>Name</strong> to identify the template.</td>
</tr>
<tr>
<td>3.</td>
<td>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 <strong>Default VSYS</strong> drop-down.</td>
</tr>
<tr>
<td></td>
<td>For related information, see <strong>Process by Which a Firewall Receives a Virtual System from a Template</strong>.</td>
</tr>
<tr>
<td>4.</td>
<td>In the Devices section, select check boxes to assign firewalls to the template.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>5.</td>
<td>(Optional) Select <strong>Group HA Peers</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>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 <strong>High Availability Synchronization</strong>.</td>
</tr>
<tr>
<td>6.</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>
<tr>
<td>7.</td>
<td>Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Template</strong>, select the firewalls assigned to the template you just added, and click <strong>Commit</strong> again.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Verify that the template is available.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>After you add the first template, Panorama displays the <strong>Device</strong> and <strong>Network</strong> tabs. These tabs display a <strong>Template</strong> drop-down. Check that the drop-down displays the template you just added.</td>
</tr>
</tbody>
</table>
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. For details and planning, see Templates and Template Stacks.

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.

Add a Template (Continued)

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.

Step 4  Verify that the firewall is configured with the template settings that you pushed from Panorama.

1. In the Context drop-down, select one of the firewalls to which you pushed the template setting.
2. Select Device > Setup > Services > Global. The IP address that you pushed from the template appears. The Services section header displays a template icon to indicate that settings in the section have values pushed from a template.
## Configure a Template Stack (Continued)

**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**.

**Step 3** Edit the **Network** and **Device** settings, if necessary.

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 **Mode** drop-down in the **Network** and **Device** 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**.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Depending on the settings you will configure, select the <strong>Network</strong> or <strong>Device</strong> tab and select the stack in the <strong>Template</strong> drop-down. The tab settings are read-only when you select a stack.</td>
</tr>
<tr>
<td>2.</td>
<td>Filter the tabs to display only the mode-specific settings you want to edit:</td>
</tr>
<tr>
<td></td>
<td>- In the <strong>Mode</strong> drop-down, select or clear the <strong>Multi VSYS</strong>, <strong>Operational Mode</strong>, and <strong>VPN Mode</strong> filter options.</td>
</tr>
<tr>
<td></td>
<td>- Set all the <strong>Mode</strong> options to reflect the mode configuration of a particular firewall by selecting it in the <strong>Device</strong> drop-down.</td>
</tr>
<tr>
<td>3.</td>
<td>You can edit settings only at the template level, not at the stack level. To identify and access the template that contains the setting you want to edit:</td>
</tr>
<tr>
<td></td>
<td>- If the page displays a table, select <strong>Columns &gt; Template</strong> in the drop-down of any column header. The Template column displays the source template for each setting. If multiple templates have the same setting, the Template column displays the higher priority template. Click the template name in this column: the <strong>Template</strong> drop-down changes to that template, at which point you can edit the setting.</td>
</tr>
<tr>
<td></td>
<td>- If the page doesn't display a table, hover over the template icon 📊 for a setting: a tooltip displays the source template. If multiple templates have the same setting, the tooltip displays the higher priority template. In the <strong>Template</strong> drop-down, select the template that the tooltip displays to edit the setting.</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>
<tr>
<td>5.</td>
<td>Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Template</strong>, select the firewalls assigned to the template stack, and click <strong>Commit</strong> again.</td>
</tr>
</tbody>
</table>
### Configure a Template Stack (Continued)

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

### Process by Which a Firewall Receives a Virtual System from a Template

Panorama supports the ability to configure a virtual system (vsys) using a template, and then push the configuration from the template to a multi-vsys firewall. The process by which the firewall receives a template vsys configuration is as follows:

For example, the firewall receives a template-defined vsys named Finance (ID of 3) as follows:

1. If the firewall cannot find a vsys named Finance, the firewall searches for an unnamed vsys with an ID of 3.  
2. If an unnamed vsys with ID 3 does not exist, the firewall creates a new vsys named Finance and assigns the next available ID.

### 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.
Manage Firewalls

How to disable or remove 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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Access the web interface of the firewall.</th>
<th>Directly access the firewall by entering its IP address in the URL field of your browser, or use the Context drop-down in Panorama to switch to the firewall context.</th>
</tr>
</thead>
</table>
| 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. | 1. Select Device > Setup > Services > Global and edit the Services section.  
2. Click the template icon 🛠 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 🛠 to indicate that the value is overridden.  
4. Click OK and Commit. |

### 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.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select Device &gt; Setup &gt; Management and edit the Panorama Settings.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Disable Device and Network Template.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) Select <strong>Import Device and Network Template before disabling</strong>, 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 device.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click OK twice and then click Commit to save the changes.</td>
</tr>
</tbody>
</table>
Transition a Firewall to Panorama Management

If you have already deployed Palo Alto Networks firewalls and configured them locally, but now want to start using 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.

- Plan the Transition to Panorama Management
- Migrate a Firewall to Panorama Management

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. 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), license and update management, high availability (HA), log collection, administrator roles, the device group hierarchy, templates, and template stacks.
- 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 centrally push policy rules that reference those zones without being aware of the variations in port or media type, platform, or logical addressing schema.
- Determine the elements to migrate, including policies, objects, network settings, and device settings. Panorama imports all these elements when you import a firewall configuration, but you can delete unwanted elements after the import.
- Decide how you will manage local rules and firewall-specific exceptions to rules and configuration settings that you will push from Panorama.
- Create a post-migration test plan to verify that the firewalls work as efficiently after the migration as they did before. The test plan might include such tasks 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. The device groups will be one level below the Shared location in the Device Group Hierarchy, though you can reassign them to other parent device groups after the import. Panorama provides the option to import objects from Shared on the firewall into Shared in Panorama.

You can import configurations from firewalls that run PAN-OS 5.0 or later releases. However, Panorama releases that support configuration imports (Panorama 7.0 or later) can’t push or export configurations to firewalls running PAN-OS 6.0.3 or earlier releases.

See Panorama, Log Collector, and Firewall Version Compatibility for important details about software and content version compatibility between Panorama and firewalls.

A firewall doesn’t lose logs when you import its configuration into Panorama.

### Migrate a Firewall 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><strong>Step 2</strong></td>
<td>Add the firewalls as managed devices.</td>
<td>Add a Firewall as a Managed Device:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Log in to Panorama, select Panorama &gt; Managed Devices and click Add.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the serial number of the firewall and click OK.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you will import multiple firewall configurations, enter the serial number of each one on a separate line.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click Commit, for the Commit Type select Panorama, and click Commit again.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Perform steps 3-7 for each firewall configuration you will import.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Set up a connection from the firewall to Panorama.</td>
<td>1. Log in to the firewall, select Device &gt; Setup, and edit the Panorama Settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. In the Panorama Servers fields, enter the IP addresses of the Panorama management server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click OK and Commit.</td>
</tr>
</tbody>
</table>
Transition a Firewall to Panorama Management

Manage Firewalls

Migrate a Firewall to Panorama Management (Continued)

Step 4  Import the firewall configuration into Panorama.

- If you later decide to re-import a firewall configuration, first remove the firewall or its virtual systems from the device groups and template where you originally imported them. (Firewalls don’t lose logs when you remove them from device groups or templates.) Because the imported policies and objects remain in the device groups, you must manually move, edit, or delete them when necessary. When re-importing, use the Device Group Name Prefix fields to define device group names that differ from the ones Panorama created in the original import.

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

2. Enter a Template Name. For a multi-vsys firewall, the field is blank. Otherwise, the default value is the firewall name.

3. For a multi-vsys firewall, in the Device Group Name Prefix field, optionally add a character string to prepend to device group names.

4. (Optional) Edit the Device Group names. For a multi-vsys firewall, each device group has a vsys name by default. Otherwise, the default value is the firewall name.

The Import devices’ shared objects into Panorama’s shared context check box is selected by default, which means Panorama imports objects that belong to Shared in the firewall to Shared in Panorama. If you clear the check box, Panorama copies shared firewall objects into device groups instead of Shared. This could create duplicate objects, so selecting the check box is a best practice in most cases.

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. However, rule names must be unique: delete one of the rules before performing a commit on Panorama.

6. Click OK. Panorama displays the import status, result, details about your selections, details about what was imported, and any warnings. Click Close.
## Migrate a Firewall to Panorama Management (Continued)

### Step 5
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. Based on the config audit and any warnings that Panorama displayed after the import, update the device group and template configurations as needed. For example, you might have to delete redundant objects and policy rules, **Move or Clone a Policy Rule or Object to a Different Device Group**, or move firewalls to different device groups or templates.

3. Move the device groups that Panorama created during the import to different parent device groups, if necessary:
   a. Select **Panorama > Device Groups** and select the device group you want to move.
   b. Select a new **Parent Device Group** and click **OK**.

4. Click **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again. Panorama creates a device configuration bundle named `<firewall_name>_import.tgz`, in which all policies and objects are removed. You will use this bundle in the next step.

### Step 6
Push the device configuration bundle to the firewall to remove all policies and objects from the local configuration.

This step is necessary to prevent device group commit errors.

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

2. 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.

### Step 7
Commit your changes to the device groups and templates.

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.

1. After importing all the firewall configurations, update the device groups and templates as needed to eliminate redundancy and streamline configuration management.

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, as Panorama can’t poll the devices for zone name or configuration. If you will use local firewall rules, ensure their names are unique.

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**.
### Migrate a Firewall to Panorama Management (Continued)

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Perform your post-migration test plan.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Verify that the firewalls work as efficiently with the Panorama-pushed configuration as they did with their original local configuration.</td>
</tr>
</tbody>
</table>
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 devices using Panorama:

- **Device Groups**
- **Templates**
- **Set Up Your Centralized Configuration and Policies**

### Device Groups

In this example, we decide to define two device groups based on the functions the firewalls will perform:

- **DG_BranchAndRegional** for grouping devices 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 devices with similar functions will require similar policy rulebases.

- **DG_DataCenter** for grouping the devices 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.
Use Case: Configure Firewalls Using Panorama

Manage Firewalls

### Templates

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, you 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

<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>Branch</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>Allow access to the Amazon cloud application for the specified hosts/servers in the datacenter.</td>
</tr>
<tr>
<td>Device Group post-rule</td>
<td>Allow Facebook to all users in the marketing group in the regional offices only.</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>
Set Up Your Centralized Configuration and Policies

Using the example described in the preceding topics (starting with Use Case: Configure Firewalls Using Panorama), perform the following tasks to centrally deploy and administer firewalls:

- **TASK 1**—Add the firewalls as managed devices, and deploy content updates and PAN-OS software updates to those firewalls.
- **TASK 2**—Use templates to administer a base configuration.
- **TASK 3**—Use device groups to manage the firewall policies.
- **TASK 4**—Preview your rules and commit your changes to Panorama, device groups, and templates.

### Add the Managed Firewalls and Deploy Updates

<table>
<thead>
<tr>
<th>TASK 1</th>
<th>For each firewall that Panorama will manage, Add a Firewall as a Managed Device.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>In this example, add 12 firewalls.</td>
</tr>
</tbody>
</table>
### Add the Managed Firewalls and Deploy Updates (Continued)

**Step 2**  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 View Panorama Task Completion History.

1.  Select Panorama > Device Deployment > Dynamic Updates.
2.  Click Check Now to check for the latest updates. If the value in the Action column is Download, this indicates an update is available.
3.  Click Download. When the download completes, the value in the Action column changes to Install.
4.  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.
5.  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.

**Step 3**  Deploy the software updates to the firewalls.

1.  Select Panorama > Device Deployment > Software.
2.  Click Check Now to check for the latest updates. If the value in the Action column is Download, this indicates an update is available.
3.  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.
4.  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.
5.  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.

---

### Use Templates to Administer a Base configuration

**TASK 2**  Use templates to administer a base configuration.

**Step 1**  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.
### 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**.
   - 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** and 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 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.

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

**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

**TASK 3**

Use device groups to manage the policy rules on your firewalls.

**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.
### Manage Firewalls Use Case: Configure Firewalls Using Panorama

#### 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.
Manage Firewalls

Use Case: Configure Firewalls Using Panorama

Use Device Groups to Push Policy Rules (Continued)

<table>
<thead>
<tr>
<th>Step 6</th>
<th>To enable logging for all Internet-bound traffic on your network, create a rule that matches trust zone to untrust zone.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Select the Policies tab and, in the Device Group drop-down, select Shared.</td>
</tr>
<tr>
<td></td>
<td>2. Select the Security &gt; Pre-Rules rulebase.</td>
</tr>
<tr>
<td></td>
<td>3. Click Add and enter a Name for the security rule.</td>
</tr>
<tr>
<td></td>
<td>4. In the Source and Destination tabs for the rule, Add trust_zone as the Source Zone and untrust_zone as the Destination Zone.</td>
</tr>
<tr>
<td></td>
<td>5. In the Action tab, set the Action to Deny, set the Log Setting to Log at Session end, and click OK.</td>
</tr>
</tbody>
</table>

Preview the Rules and Commit Changes

**TASK 4**

Preview your rules and commit your changes to Panorama, device groups, and templates.

**Step 1** 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.

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

**Step 3** 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.

**Step 4** In the Context drop-down, select the firewall to access its web interface and confirm that Panorama applied the template and policy configurations.
Use Case: Configure Firewalls Using Panorama

Manage Firewalls
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-100 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.

▲ 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

To manage the System and Config logs that Panorama generates locally, see Monitor Panorama.
Configure a Managed Collector

To enable Panorama (virtual appliance or an M-100 appliance in Panorama mode) to manage Log Collectors, you must add each Log Collector as a managed collector.

If you forward logs to an M-100 appliance in Panorama mode, the default Log Collector that is local to the appliance is added during the manufacturing process. However, if you Migrate from a Panorama Virtual Appliance to an M-100 Appliance, the default Log Collector does not appear; you must re-configure the Log Collector.

To configure a Dedicated Log Collector (M-100 appliance in Log Collector mode), start at Step 1. To configure a local Log Collector (local to the M-100 appliance in Panorama mode), start at Step 4. Skip any steps you have already performed (for example, the initial setup).

### Configure a Managed Collector

<table>
<thead>
<tr>
<th>Step 1</th>
<th>(Dedicated Log Collector only) Perform initial setup of the M-100 appliance in Log Collector mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Rack mount the M-100 appliance. Refer to the M-100 Hardware Reference Guide for instructions.</td>
</tr>
<tr>
<td></td>
<td>2. Perform Initial Configuration of the M-100 Appliance.</td>
</tr>
<tr>
<td></td>
<td>3. Register Panorama and Install Licenses.</td>
</tr>
<tr>
<td></td>
<td>4. Install Content and Software Updates for Panorama.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>(Dedicated Log Collector only) Switch from Panorama Mode to Log Collector Mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Switching the mode of an M-100 appliance deletes any existing log data and deletes all configurations except the management access settings. After the switch, the M-100 appliance retains CLI access but loses web interface access.</td>
</tr>
<tr>
<td></td>
<td>1. Log in to the Panorama CLI of the M-100 appliance.</td>
</tr>
<tr>
<td></td>
<td>2. Enter the <code>request system system-mode logger</code> command, and then enter <code>Yes</code> to confirm the switch to Log Collector mode. The appliance will reboot.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>(Dedicated Log Collector only) For any Dedicated Log Collector that requires more than the default 1TB of storage, add RAID drives. This example uses the drives in disk bays B1 and B2.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>In the Dedicated Log Collector CLI, enter the following commands and confirm the request when prompted:</td>
</tr>
<tr>
<td></td>
<td><code>request system raid add B1</code></td>
</tr>
<tr>
<td></td>
<td><code>request system raid add B2</code></td>
</tr>
<tr>
<td>Step 4</td>
<td>Enable connectivity among the M-100 appliances.</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>The commands you enter depend on the Log Collector type:</td>
</tr>
<tr>
<td></td>
<td>• Dedicated Log Collectors</td>
</tr>
<tr>
<td></td>
<td>a. In the CLI of each Log Collector, enter the following commands, where &lt;IP address1&gt; represents the management interface of the primary (HA) or solitary (non-HA) Panorama.</td>
</tr>
<tr>
<td></td>
<td><code>set deviceconfig system panorama-server &lt;IPaddress1&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>commit</code></td>
</tr>
<tr>
<td></td>
<td>b. In a high availability (HA) deployment, also enter the following commands, where &lt;IP address2&gt; represents the management interface of the secondary Panorama.</td>
</tr>
<tr>
<td></td>
<td><code>set deviceconfig system panorama-server-2 &lt;IPaddress2&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>commit</code></td>
</tr>
<tr>
<td></td>
<td>• Local Log Collectors—Perform the following steps only if Panorama has an HA configuration.</td>
</tr>
<tr>
<td></td>
<td>a. In the CLI of the primary Panorama, enter the following commands, where &lt;IP address2&gt; represents the management interface of the secondary Panorama.</td>
</tr>
<tr>
<td></td>
<td><code>set deviceconfig system panorama-server &lt;IPaddress2&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>commit</code></td>
</tr>
<tr>
<td></td>
<td>b. In the CLI of the secondary Panorama, enter the following commands, where &lt;IP address1&gt; represents the management interface of the primary Panorama.</td>
</tr>
<tr>
<td></td>
<td><code>set deviceconfig system panorama-server &lt;IPaddress1&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>commit</code></td>
</tr>
<tr>
<td>Step 5</td>
<td>Record the serial number of the Log Collector. You will need this when you add the Log Collector as a managed collector.</td>
</tr>
<tr>
<td></td>
<td>The step to display the serial number depends on the Log Collector type:</td>
</tr>
<tr>
<td></td>
<td>• Local—Use the serial number of the M-100 appliance that is in Panorama mode: access the Panorama web interface and record the value on the <strong>Dashboard</strong> tab, General Information section, <strong>Serial #</strong> field.</td>
</tr>
<tr>
<td></td>
<td>In a high availability (HA) deployment, you can configure a local Log Collector on each peer M-100 appliance in Panorama mode. Each peer will have a unique serial number.</td>
</tr>
<tr>
<td></td>
<td>• Dedicated—Use the serial number of the M-100 appliance that is in Log Collector mode: access the Log Collector CLI and enter the <em>show system info</em> command.</td>
</tr>
</tbody>
</table>
### Configure a Managed Collector (Continued)

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Configure the general settings of the Log Collector.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Use the web interface of the Panorama management server to perform the following steps:</td>
</tr>
<tr>
<td></td>
<td>1. Select Panorama &gt; Managed Collectors.</td>
</tr>
<tr>
<td></td>
<td>2. <strong>Add</strong> a new Log Collector or select an existing one to edit it.</td>
</tr>
<tr>
<td></td>
<td>The M-100 appliance in Panorama mode has a predefined Log Collector named <strong>default</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>General</strong> tab, <strong>Collector S/N</strong> field, enter the serial number you recorded in <strong>Step 5</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>The remaining steps depend on your deployment:</strong></td>
</tr>
<tr>
<td></td>
<td>• Proceed to <strong>Step 7</strong> if you are adding a Dedicated Log Collector (M-100 appliance in Log Collector mode) or you are adding a Log Collector that is local on the secondary M-100 appliance in Panorama mode (in an HA deployment).</td>
</tr>
<tr>
<td></td>
<td>• Skip to <strong>Step 10</strong> if the Log Collector you are adding is local on the solitary (non-HA) or primary (HA) M-100 appliance in Panorama mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Configure network access for the Log Collector.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Although you specified the following details during initial configuration of the M-100 appliance, you must re-enter the information on the <strong>General</strong> tab; Panorama does not auto-populate the fields.</td>
</tr>
<tr>
<td></td>
<td>1. In the <strong>Panorama Server IP</strong> field, enter the IP address of the Panorama management server that will manage the Log Collector. If Panorama has an HA configuration, enter the IP address of the secondary peer in the <strong>Panorama Server IP 2</strong> field.</td>
</tr>
<tr>
<td></td>
<td>The preceding fields are required.</td>
</tr>
<tr>
<td></td>
<td>2. Configure the IP addresses of the <strong>Primary DNS Server</strong> and <strong>Secondary DNS Server</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. (Optional) Set the <strong>Timezone</strong> that Panorama will use to record log entries.</td>
</tr>
<tr>
<td></td>
<td><strong>The remaining steps depend on your deployment:</strong></td>
</tr>
<tr>
<td></td>
<td>• Go to <strong>Step 8</strong> if you are adding a Dedicated Log Collector.</td>
</tr>
<tr>
<td></td>
<td>• Skip to <strong>Step 10</strong> if the Log Collector you are adding is local on the secondary M-100 appliance in Panorama mode.</td>
</tr>
</tbody>
</table>

### Step 8 (Dedicated Log Collector only) Configure administrative access to the Log Collector.

The default user is **admin**. You cannot modify this username nor add administrative users on the Log Collector.

|        | 1. In the **Authentication** tab, select the password **Mode**, then enter the **Password** (the default is `admin`). |
|        | 2. Enter the number of **Failed Attempts** to log in that a user can commit before Panorama locks out that user from accessing the Log Collector, and enter the **Lockout Time** interval in minutes. |
### Configure a Managed Collector (Continued)

| Step 9 | (Dedicated Log Collector only) Configure the Log Collector interfaces. | Configure the following settings on each tab associated with an interface the Log Collector will use: Management (MGT), Eth1, and/or Eth2. The Eth1 or Eth2 interfaces are only available if you defined them during the task Perform Initial Configuration of the M-100 Appliance. The MGT interface is required.  
1. Complete one of the following field sets, depending on the IP protocol of your network:  
   - IPv4—IP Address, Netmask, and Default Gateway  
   - IPv6—IPv6 Address/Prefix Length and Default IPv6 Gateway  
   The preceding fields are required.  
2. (Optional) Select the services that the interface supports. By default, Ping is selected for the MGT, Eth1, and Eth2 interfaces. The MGT interface also supports SSH (selected by default) and SNMP (cleared by default).  
3. (Optional) To restrict access to an interface, Add one or more IP addresses in the Permitted IP Addresses list. If you leave the list blank, Panorama does not restrict access.  
   If you add any entries, only the specified IP addresses can access the interface so be sure to add the addresses of the Panorama management server.  
4. Click OK. |

| Step 10 | (Optional) Enable any additional RAID disk pairs for logging. | To enable additional disk pairs, you must have performed Step 3.  
1. In the Disks tab, Add each additional disk pair.  
2. Click OK to make the disk pair available for logging. |

| Step 11 | (Optional) Select the interfaces that the Log Collector will use for Device Log Collection and Collector Group Communication. The M-100 appliance uses the MGT (Management) interface by default. The Eth1 or Eth2 interfaces are only available if you configured them in the corresponding tabs. | Return to the General tab and select the interfaces that the Log Collector will use for Device Log Collection and Collector Group Communication. |
Configure a Managed Collector (Continued)

<table>
<thead>
<tr>
<th>Step 12</th>
<th>Commit and (optionally) verify your changes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Panorama</strong>, and click <strong>Commit</strong> again.</td>
</tr>
<tr>
<td>2.</td>
<td>In the <strong>Panorama &gt; Managed Collectors</strong> page, verify that the grid lists the Log Collector you added. The <strong>Connected</strong> column displays a check mark icon to indicate that the Log Collector is connected to Panorama.</td>
</tr>
<tr>
<td>3.</td>
<td>If you enabled additional disk pairs, click the <strong>Statistics</strong> link in the last column to open a window that displays the status of the disks.</td>
</tr>
</tbody>
</table>

Palo Alto Networks recommends that you install the same Applications and Threats database version on Panorama as on the managed firewalls and Log Collectors. Panorama uses the Applications and Threats database to retrieve metadata for processing reports that you initiate from Panorama or managed devices. If a Log Collector does not have the database installed, the complete dataset required for the report might not be available and the information displayed might be incomplete or inaccurate. For details, see Deploy Updates to Devices Using Panorama.
Manage Collector Groups

After adding Log Collectors as managed collectors, you must assign them to Collector Groups and assign managed firewalls to the Log Collectors. This enables Panorama to access, manage, and update the Log Collectors.

If you forward logs to an M-100 appliance in Panorama mode, Palo Alto Networks predefines a default Collector Group that contains the default local Log Collector. However, if you Migrate from a Panorama Virtual Appliance to an M-100 Appliance, the default Log Collector and Collector Group do not appear; you must manually add the Log Collector and then the Collector Group.

While a Collector Group can have multiple Log Collectors, Palo Alto Networks recommends assigning only one. However, if any firewall generates more than 4TB of logs for the required storage period, you must assign multiple Log Collectors to the Collector Group that receives those logs. To understand the risks and recommended mitigations, see Caveats for a Collector Group with Multiple Log Collectors.

For more information, see Managed Collectors and Collector Groups.

⚠️ If you delete a Collector Group, you will lose logs.

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

## Configure a Collector Group

<table>
<thead>
<tr>
<th>Step 1</th>
<th>(Optional) If you will forward firewall logs from the Collector Group to external services, configure a server profile for each external service.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select Panorama &gt; Server Profiles and select the type of server that will receive the log data: SNMP Trap, Syslog, or Email.</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the server profile. Optionally, you can configure separate profiles for different log types and severity levels or WildFire verdicts.</td>
</tr>
<tr>
<td></td>
<td>• SNMP Trap server profile</td>
</tr>
<tr>
<td></td>
<td>• Syslog server profile</td>
</tr>
<tr>
<td></td>
<td>• Email server profile</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Add a Firewall as a Managed Device. Perform this step for each firewall you will assign to the Collector Group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>In the Panorama web interface, select Panorama &gt; Managed Devices and click Add.</td>
</tr>
<tr>
<td>2.</td>
<td>Enter the serial number of each firewall (one line per serial number) and click OK.</td>
</tr>
</tbody>
</table>
**Configure a Collector Group (Continued)**

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Configure a Managed Collector.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Perform this step for each Log Collector you will assign to a Collector Group.</td>
</tr>
<tr>
<td></td>
<td>If you forward logs to a Dedicated Log Collector (M-100 appliance in Log Collector mode), you must manually add a managed collector before you add a Collector Group.</td>
</tr>
<tr>
<td></td>
<td>If you forward logs to a local Log Collector (local to an M-100 appliance in Panorama mode), Palo Alto Networks predefines a default local Log Collector.</td>
</tr>
<tr>
<td></td>
<td>If you will use SNMP for monitoring, select the <strong>SNMP</strong> service when you configure the <strong>MGT</strong> (Management) interface of each Log Collector.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Add the Collector Group or edit an existing one.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Perform this step for each Log Collector you will assign to a Collector Group.</td>
</tr>
<tr>
<td></td>
<td>If you forward logs to a Dedicated Log Collector (M-100 appliance in Log Collector mode), you must manually add a managed collector before you add a Collector Group.</td>
</tr>
<tr>
<td></td>
<td>If you forward logs to a local Log Collector (local to an M-100 appliance in Panorama mode), Palo Alto Networks predefines a default local Log Collector.</td>
</tr>
<tr>
<td></td>
<td>If you will use SNMP for monitoring, select the <strong>SNMP</strong> service when you configure the <strong>MGT</strong> (Management) interface of each Log Collector.</td>
</tr>
<tr>
<td></td>
<td>1. In the Panorama web interface, select <strong>Panorama &gt; Collector Groups</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. <strong>Add</strong> a new Collector Group or select an existing one to edit it.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>General</strong> tab, if you are adding a new Collector Group, enter a <strong>Name</strong> for it. You cannot edit the name of an existing Collector Group.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Minimum Retention Period</strong> field, enter the number of days (1-2000) for which Panorama will retain the logs of the firewalls you assign to this Collector Group. When the current date minus the oldest log date is less than the defined minimum retention period, Panorama generates a System log. Panorama generates an alert within a day of the logs reaching the retention period.</td>
</tr>
<tr>
<td></td>
<td>5. (Optional) Select the <strong>Enable log redundancy across collectors</strong> check box 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.</td>
</tr>
<tr>
<td></td>
<td>Because enabling redundancy creates more logs, this configuration requires more storage capacity. When a Collector Group runs out of space, it deletes older logs. Enabling redundancy 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.</td>
</tr>
</tbody>
</table>
### Configure a Collector Group (Continued)

**Step 5** (Optional) Configure SNMP monitoring for the Log Collectors.

1. In 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 6** Assign Log Collectors to the Collector Group.

Each Collector Group can have up to eight Log Collectors.

1. In the **Device Log Forwarding** tab, Collector Group Members section, click **Add**.
2. In the drop-down, select the Log Collectors you want to assign to the group.

**Step 7** Assign the firewalls that will forward logs to the Collector Group.

1. In the **Device Log Forwarding** tab, Log Forwarding Preferences section, click **Add**.
2. In the Devices section, click **Modify**, select the firewalls you want to assign to the Collector Group, and click **OK**.
3. 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; only if the primary becomes unavailable will the firewalls send logs to the next Log Collector in the list. To change the priority of a Log Collector, select it and click **Move Up** (higher priority) or **Move Down** (lower priority).
4. When you finish assigning Log Collectors to the firewalls, click **OK**.
### Step 8
Allocate the desired storage capacity (log quotas) and expiration period for each log type.

1. Return to the **General** tab and click the **Log Storage** value. This field does not display a value unless you assigned Log Collectors to the Collector Group. If after assigning Log Collectors the field reads 0MB, verify you enabled the disk pairs for logging and committed the changes (see **Step 10** under **Configure a Managed Collector**).

2. Enter the log 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.

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.

   If you must undo your changes and reset the quotas and expiration periods to the factory defaults, click **Restore Quota Defaults** at the bottom right of the dialog.

### Step 9 (Optional)
Configure log forwarding from the Collector Group to external services.

For a high availability (HA) configuration, you can configure each Panorama HA peer to forward logs to different destinations, if necessary. For details, see Deploy Panorama with Default Log Collectors.

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 you just created.

3. In the **Config**, **HIP Match**, and **Traffic** tabs, select the **SNMP Trap**, **Email**, or **Syslog** server profile you just created.

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 you just created.

5. Click **OK** to save the Collector Group.

### Step 10
Commit the changes and, optionally, 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 **OK**.

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.

   Palo Alto Networks recommends that you install the same Applications and Threats database version on Panorama as on the managed firewalls and Log Collectors. For details, see **Panorama, Log Collector, and Firewall Version Compatibility**.
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-100 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-100 appliance in Panorama mode, move it only if the M-100 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-100 appliance that is the active HA peer.

<p>| Step 11 (Optional) If you will use SNMP to monitor Log Collectors, configure the Simple Network Management Protocol (SNMP) management software. You can use SNMP to collect the following information about the Log Collector: connection status, disk drive statistics, software version, average CPU, average logs/second, and log storage duration for each log type. | Configure the SNMP Manager to get statistics from Panorama and the Log Collectors. Refer to your SNMP manager documentation for the specific steps. |</p>
<table>
<thead>
<tr>
<th>Step 1</th>
<th>Remove the Log Collector from Panorama management.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Select <strong>Panorama &gt; Collector Groups</strong> and select the Collector Group that contains the Log Collector you will move.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Device Log Forwarding</strong> 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:</td>
</tr>
<tr>
<td></td>
<td>a. In the Devices column, click the link for the firewalls assigned to the Log Collector.</td>
</tr>
<tr>
<td></td>
<td>b. In the Collectors column, select the Log Collector and click <strong>Delete</strong>.</td>
</tr>
<tr>
<td></td>
<td>c. Click <strong>OK</strong> twice to save your changes.</td>
</tr>
<tr>
<td></td>
<td>3. Select <strong>Panorama &gt; Managed Collectors</strong>, select the Log Collector you will move, and click <strong>Delete</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Panorama</strong>, and click <strong>Commit</strong> again.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Collector Group</strong>, select the Collector Group from which you deleted the Log Collector, and click <strong>Commit</strong> again.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Reset the Log Collector to its factory default settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Log in to the CLI of the Log Collector.</td>
</tr>
<tr>
<td></td>
<td>2. Enter the following CLI command:</td>
</tr>
<tr>
<td></td>
<td><code>debug system maintenance-mode</code></td>
</tr>
<tr>
<td></td>
<td>The Log Collector will reboot in maintenance mode.</td>
</tr>
<tr>
<td></td>
<td>3. After the Log Collector reboots, press <strong>Enter</strong> to access the maintenance mode menu.</td>
</tr>
<tr>
<td></td>
<td>4. Select <strong>Factory Reset</strong> and press Enter.</td>
</tr>
<tr>
<td></td>
<td>5. Select <strong>Factory Reset</strong> and press Enter again.</td>
</tr>
<tr>
<td></td>
<td>The Log Collector will reboot, after which it won’t have any configuration settings or log data. The default username and password to log in to the Log Collector is admin/admin.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Reconfigure the Log Collector.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Perform Initial Configuration of the M-100 Appliance.</td>
</tr>
<tr>
<td></td>
<td>2. Register Panorama and Install Licenses.</td>
</tr>
<tr>
<td></td>
<td>3. Install Content and Software Updates for Panorama.</td>
</tr>
<tr>
<td></td>
<td>4. Switch from Panorama Mode to Log Collector Mode.</td>
</tr>
<tr>
<td></td>
<td>5. Configure a Managed Collector.</td>
</tr>
</tbody>
</table>
Manage Log Collection

Remove a Firewall from a Collector Group

In a distributed log collection deployment, where you have Dedicated Log Collectors, if you need a device to send logs to Panorama instead of sending logs to the Collector Group, you must remove the device from the Collector group.

When you remove the device from the Collector Group and commit the change, the device will automatically send logs to Panorama instead of sending them to a Log Collector.

Remove a Firewall from a Collector Group

Step 1 Select the Panorama > Collector Groups tab.

Step 2 Click the link for the desired Collector Group, and select the Log Forwarding tab.

Step 3 In the Log Forwarding Preferences section, select the device that you would like to remove from the list, click Delete, and click OK.

Step 4 Click Commit, for the Commit Type select Panorama, and click Commit again.

Step 5 Click Commit, for the Commit Type select Collector Group, select the Collector Group from which you removed the firewall, and click Commit again.

To temporarily remove the log forwarding preference list on the device, you can delete it using the CLI on the device. 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 device will be reconfigured to send logs to the assigned Log Collector.
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. Before starting this procedure, you must Add a Device Group and Add a Template for the firewalls that will forward logs.

To forward firewall logs directly to external services (for example, 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.

<table>
<thead>
<tr>
<th>Configure Log Forwarding to Panorama</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> 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.)</td>
</tr>
</tbody>
</table>
|1. Select **Objects > Log Forwarding** and select the **Device Group** of the firewalls that will forward logs.  
2. Click **Add** and enter a **Name** to identify the profile.  
3. For each log type and each severity level or WildFire verdict, select the **Panorama** check box.|

|Step 2| Assign the log forwarding profile to security rules. To trigger log generation and forwarding, the rules require certain security profiles according to log type:  
- Traffic logs—No security profile is necessary; the traffic only needs to match a specific security rule.  
- Threat logs—The traffic must match any security profile assigned to a security rule.  
- WildFire logs—The traffic must match a File Blocking profile assigned to a security rule.|
|1. In the **Policies** tab, select the **Device Group** of the firewalls that will forward logs.  
2. For each rule that will trigger log forwarding:  
  a. Select the rulebase of the rule that will trigger log forwarding (for example, **Policies > Security > Pre Rules**) and select the rule.  
  b. Select the **Actions** tab, select the **Log Forwarding** profile you just created, and click **OK**.|

|Step 3| Configure the destination of System, Config, HIP Match, and Correlation logs.|
|1. Select **Device > Log Settings** and select the **Template** of the firewalls that will forward logs.  
2. For System and Correlation logs, click each Severity level, select the **Panorama** check box, and click **OK**.  
3. For Config and HIP Match logs, click the icon, select the **Panorama** check box, and click **OK**.  
4. Click **Commit** to complete the log forwarding configuration.|

|Step 4| (M-100 appliances only) Configure Panorama to receive the logs.|
|1. For each Log Collector that will receive logs, **Configure a Managed Collector**.  
2. **Configure a Collector Group**. You assign firewalls to specific Log Collectors for log forwarding.|

---

122  •  Panorama 7.0 Administrator’s Guide  
Palo Alto Networks
### Configure Log Forwarding to Panorama

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Commit the configuration changes.</td>
</tr>
</tbody>
</table>

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 of the firewalls that will forward logs, select the **Include Device and Network Templates** check box, and click **Commit** again.

3. Click **Commit**, for the **Commit Type** select **Collector Group**, select the Collector Group you just configured to receive the logs, and click **Commit** again.
Verify Log Forwarding to Panorama

Now that you have added the Log Collectors as managed collectors, created and configured the Collector Group and assigned the managed firewalls to forward logs to the specified Collector Group, you can test that your configuration was successful.

Verify Log Forwarding to Panorama

<table>
<thead>
<tr>
<th>Step 1</th>
<th>On the managed firewall, check that the firewall has the log forwarding preference list and is forwarding logs to the configured Log Collector. You cannot view this information from the web interface on the firewall.</th>
</tr>
</thead>
</table>
|       | 1. Access the CLI on the firewall.  
|       | 2. Enter the following commands:  
|       | • `show log-collector preference-list`  
|       |     If you have assigned only one Log Collector to the Collector Group, the onscreen output will look something like this:  
|       |     ![Log collector Preference List](image)  
|       | • `show logging-status`  
|       |     The onscreen output will look something like this:  
|       | ![show logging-status](image)  
| Step 2 | On Panorama, verify the log collection rate.  
|       | Click the **Statistics** link in the **Panorama > Managed Collectors** tab to view the average logs/second being received by Panorama. |
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-100 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>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 platform and the volume of logs that are pending roll over. 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>

- 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>Logging Options</td>
<td>Pertains to</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Get Only New Logs on Convert to</td>
<td>Panorama virtual appliance that is mounted to a Network File System (NFS)</td>
<td>With NFS logging, when you have a pair of Panorama servers configured in a high availability configuration, only the primary Panorama peer</td>
</tr>
<tr>
<td>Primary</td>
<td>datastore and is set up in a high availability (HA) configuration</td>
<td>mounts the NFS datastore. Therefore, the firewalls can only send logs to the primary Panorama peer, which can write to the NFS datastore.</td>
</tr>
<tr>
<td>Default: Disabled</td>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to send only newly generated logs to Panorama. This event is triggered when the priority of the active-secondary Panorama is promoted to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>primary and it can begin logging to the NFS. This behavior is typically enabled to prevent the firewalls from sending a large volume of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.

### 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>
</tbody>
</table>
| Step 3 | Configure the destinations for:  
  • Firewall logs that a Panorama virtual appliance collects.  
  • Logs that Panorama (a virtual appliance or M-100 appliance) and managed collectors generate. |

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 for Palo Alto Networks Devices](#).
   - **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.**

3. 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**.

4. For WildFire logs, click each Verdict, select the **SNMP Trap**, **Email**, or **Syslog** server profile you just created, and click **OK**.

5. For Config, HIP Match, and Traffic logs, click the **icon**, 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-100 appliance only) Configure the destinations for firewall logs that an M-100 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-100 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. Select the **Collector Log Forwarding** tab.
3. 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.
4. In the **Config**, **HIP Match**, and **Traffic** tabs, select the **SNMP Trap**, **Email**, or **Syslog** server profile you just created.
5. 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.
6. Click **OK** to save your changes to the Collector Group.

**Step 5**  
(SNMP trap forwarding only) Enable your SNMP manager to interpret traps.

Load the Supported MIBs for Palo Alto Networks devices and, if necessary, compile them. For the specific steps, refer to the documentation of your SNMP manager.

**Step 6**  
(Syslog forwarding only) If the syslog server requires client authentication, and the firewalls forward logs to M-100 appliances in Log Collector mode, assign a certificate that secures syslog communication over SSL.

Perform the following steps for each M-100 appliance in Log Collector mode:

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 7**  
Commit your configuration 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 all the device groups of the firewalls from which Panorama collects logs, select the **Include Device and Network Templates** check box, and click **Commit** again.
3. (M-100 appliance only) Click **Commit**, for the **Commit Type** select **Collector Group**, select the Collector Group you just configured to forward logs, and click **Commit** again.
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 Collector Platforms
- Collector Groups with Single or Multiple Log Collectors
- Log Forwarding Options

Panorama and Log Collector Platforms

Decide which platforms to use for the Panorama management server and Log Collectors based on the number, logging rate, and geographic distribution of managed firewalls. (See Panorama Platforms for more platform specifications and recommendations.)

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-100 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 Panorama management server when considering the number of firewalls.
Log Collection Deployments

The following table summarizes your choice of Log Collector when considering the firewall logging rate.

<table>
<thead>
<tr>
<th>Number of managed firewalls</th>
<th>Panorama Management Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>≤ 10</td>
<td>Panorama virtual appliance or M-100 appliance in Panorama mode</td>
</tr>
<tr>
<td>11–1,000</td>
<td>M-100 appliance in Panorama mode</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Logging Rate</th>
<th>Log Collector</th>
</tr>
</thead>
<tbody>
<tr>
<td>≤ 10,000 logs/second</td>
<td>Depends on the Panorama management server:</td>
</tr>
<tr>
<td></td>
<td>• Virtual appliance—Panorama collects logs without any Log Collector.</td>
</tr>
<tr>
<td></td>
<td>• M-100 appliance—Local default Log Collector</td>
</tr>
<tr>
<td>&gt; 10,000 logs/second</td>
<td>M-100 appliance in Log Collector Mode. Each Dedicated Log Collector can process up to 50,000 logs/second and store 4 TB of log data. Add Dedicated Log Collectors as needed when the logging output exceeds these thresholds.</td>
</tr>
</tbody>
</table>

Collector Groups with Single or Multiple Log Collectors

Palo Alto Networks recommends assigning only one Log Collector to a Collector Group. However, if any single firewall will generate more than 4TB of logs (the maximum an M-100 appliance can store) for the required retention period, you must assign multiple Log Collectors (up to eight) to the Collector Group that receives the logs. To understand how logging works in the latter scenario, as well as the risks and recommended mitigations, see Caveats for a Collector Group with Multiple Log Collectors.

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 device (firewall, Panorama virtual appliance, or M-100 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 devices 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.

**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-100 appliances in Panorama mode, configured for active/passive high availability (HA). Alternatively, you can use a pair of Panorama virtual appliances (if managing 10 or fewer firewalls). The firewalls send logs to Dedicated Log Collectors (M-100 appliances in Log Collector mode). This is the recommended configuration if the firewalls generate logs at a rate exceeding 10,000 logs/second. (For details on deployment options, see Plan a Log Collection Deployment.)

It is a best practice to assign only one Log Collector to each Collector Group (Figure: Single Dedicated Log Collector Per Collector Group). However, if any single firewall generates more than 4 TB of logs for the required log retention period, the Collector Group receiving the logs requires multiple Log Collectors (Figure: Multiple Dedicated Log Collectors Per Collector Group). See Caveats for a Collector Group with Multiple Log Collectors to understand the risks and recommended mitigations associated with the latter configuration.

Figure: Single Dedicated Log Collector Per Collector Group
Perform the following steps to deploy Panorama with Dedicated Log Collectors. Skip any steps you have already performed (for example, the initial setup).

### Deploy Panorama with Dedicated Log Collectors

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Perform the initial setup of the Panorama management server (virtual appliances or M-100 appliances) and the Dedicated Log Collectors.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For each M-100 appliance:</td>
</tr>
<tr>
<td></td>
<td>1. Rack mount the M-100 appliance. Refer to the M-100 Hardware Reference Guide for instructions.</td>
</tr>
<tr>
<td></td>
<td>2. Perform Initial Configuration of the M-100 Appliance.</td>
</tr>
<tr>
<td></td>
<td>For each virtual appliance (if any):</td>
</tr>
<tr>
<td></td>
<td>1. Install Panorama on the ESXi Server.</td>
</tr>
<tr>
<td></td>
<td>2. Perform Initial Configuration of the Panorama Virtual Appliance.</td>
</tr>
<tr>
<td></td>
<td>For each Panorama appliance regardless of type:</td>
</tr>
<tr>
<td></td>
<td>3. Register Panorama and Install Licenses.</td>
</tr>
<tr>
<td></td>
<td>4. Install Content and Software Updates for Panorama.</td>
</tr>
<tr>
<td></td>
<td>For the Panorama management server:</td>
</tr>
<tr>
<td></td>
<td>5. Set Up HA on Panorama.</td>
</tr>
</tbody>
</table>
## Deploy Panorama with Dedicated Log Collectors (Continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 2 | **Switch from Panorama Mode to Log Collector Mode** on each M-100 appliance that will serve as a Dedicated Log Collector.  
Switching the mode of an M-100 appliance deletes any existing log data and delete all configurations except the management access settings. After the switch, the M-100 appliance retains CLI access but loses web interface access. |
| 1. | Log in to the Panorama CLI of the Dedicated Log Collector.  
2. | Enter the command `request system system-mode logger`, then enter **Yes** to confirm the change to Log Collector mode. The appliance will reboot.  |
| Step 3 | **Enable connectivity for distributed log collection on each Dedicated Log Collector.**  
(Optional) for each Dedicated Log Collector that requires more than the default 1TB of storage. This example uses the drives in disk bays B1 and B2. |
| | In the Dedicated Log Collector CLI, enter the following commands and confirm the request when prompted:  
`request system raid add B1`  
`request system raid add B2`  

| Step 4 | **Enable connectivity for distributed log collection on each Dedicated Log Collector.**  
In the Dedicated Log Collector CLI, enter the following commands, where `<IP address1>` and `<IP address2>` represent the management interfaces of the primary and secondary Panorama respectively.  
`set deviceconfig system panorama-server `<IP address1>`  
`set deviceconfig system panorama-server-2 `<IP address2>`  
`commit`  |
| Step 5 | **Record the serial number of each Dedicated Log Collector. You will need this when you add the Log Collectors as Managed Collectors.**  
(Optional) If you will use SNMP to monitor Log Collectors, Configure the SNMP management software. |
| | In the Dedicated Log Collector CLI, enter the following command to display the serial number:  
`show system info`  

| Step 6 | **Add a Firewall as a Managed Device.**  
Perform this step for all the firewalls you will assign to Log Collectors.  
(Optional) If you will use SNMP to monitor Log Collectors, Configure the SNMP management software. |
| | Load all the PAN-OS MIB files into your SNMP management software and, if necessary, compile them. Refer to your SNMP manager documentation for the specific steps.  
1. | If you have not already, perform the initial setup of each firewall that you will assign to a Log Collector.  
2. | In the web interface of the primary Panorama management server peer, select **Panorama > Managed Devices**, click **Add**, enter the serial number of each firewall (one line per serial number), and click **OK**.  |
| Step 7 | **Configure Log Forwarding to Panorama.** By default, firewalls store all log files locally. You must configure the firewalls to forward logs to Panorama. |

---

134 • Panorama 7.0 Administrator’s Guide  
Palo Alto Networks
Step 9 (Optional) If you will forward logs from Panorama to external services, configure a server profile for each service.

Use the web interface of the primary Panorama to perform the following steps:

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:
   - **SNMP Trap** server profile
   - **Syslog** server profile
   - **Email** server profile

   You can configure separate profiles for different log types and severity levels or WildFire verdicts. You can also assign separate profiles to each Collector Group.

   To forward firewall logs, you assign the server profiles when you configure the Collector Groups (Step 12).

3. To forward the System and Config logs that the M-100 appliances generate:
   a. Select **Panorama > Log Settings > System**.
   b. For System logs, click each Severity level, assign a server profile, and click **OK**.
   c. For Config logs, edit the Config settings, assign a server profile, and click **OK**.

Step 10 (Optional) Modify Log Forwarding and Buffering Defaults.

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

1. Select **Panorama > Setup > Management** and edit the Logging and Reporting Settings.

2. Define the **Log Storage** and **Log Export and Reporting** settings as desired.

   It is a best practice to select the **Buffered Log Forwarding from Device** option.

   The **Log Storage** quotas and **Max Days** (expiration periods) you configure here apply only to the System and Config logs that the M-100 appliances generate. You set the storage settings for firewall logs when you configure the Collector Groups.
**Deploy Panorama with Dedicated Log Collectors (Continued)**

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

1. Select **Panorama > Managed Collectors** and click **Add**.
2. In the **General** tab, **Collector S/N** field, enter the serial number you recorded for the Log Collector.
3. Enter the IP address of the primary Panorama management server peer in the **Panorama Server IP** field and the IP address of the secondary Panorama management server peer in the **Panorama Server IP 2** field.
   - The preceding fields are required.
4. In the **Authentication** tab, select the password **Mode** and enter a **Password** (the default is `admin`).
5. In the **Management** tab, complete one of the following field sets for the management interface:
   - **IPv4**—**IP Address**, **Netmask**, and **Default Gateway**
   - **IPv6**—**IPv6 Address/Prefix Length** and **Default IPv6 Gateway**
   - The preceding fields are required.
6. If you configured Eth1 and/or Eth2 interfaces during the task **Perform Initial Configuration of the M-100 Appliance**, configure the settings in the **Eth1** and/or **Eth2** tabs. You must select the **Eth1/Eth2** check box in the corresponding tab before you configure the settings.
7. Return to the **General** tab and select the interfaces to use for **Device Log Collection** and **Collector Group Communication**. Panorama uses the management (mgmt) interface by default. **Eth1** and **Eth2** are only available if you configured them in the corresponding tabs.
8. If you increased storage capacity on the Log Collector, select the **Disks** tab, **Add** each additional disk pair, and click **OK**.
9. Click **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.

---

**Step 11** Configure a Managed Collector for each Dedicated Log Collector.
Deploy Panorama with Dedicated Log Collectors (Continued)

Step 12 Configure a Collector Group.

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

1. Select Panorama > Collector Groups, click Add, and enter a Name for the Collector Group. After you save the Collector Group, you cannot change its name.

2. If you configured the SNMP management software to monitor Log Collectors, select the Monitoring tab and configure the SNMP settings.

3. In the Device Log Forwarding tab, Collector Group Members section, assign one or multiple Log Collectors to the group.

4. In the Device Log Forwarding Preferences section, assign firewalls according to the number of Log Collectors in this Collector Group:
   - Single Log Collector—Assign the firewalls that will forward logs to that Log Collector, as illustrated in Figure: Single Dedicated Log Collector Per Collector Group.
   - Multiple Log Collectors—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. Return to the General tab, click the Log Storage value and allocate the desired Log Storage capacity (log quotas) and Max Days (expiration periods) for each log type (System, Config, HIP Match, Traffic, Threat, and WildFire). This applies to the logs that firewalls and Log Collectors forward to Panorama.

6. If you created server profiles for forwarding firewall logs from Panorama to external destinations, select the Collector Log Forwarding tab and assign the profiles to the desired external services. The profiles can be the same or different for each Collector Group.

7. Click OK to save your changes.

The next step depends on your deployment:

- If each Collector Group has only one Log Collector, repeat Step 12 for each Collector Group before proceeding.
- If you assigned all the Log Collectors to this Collector Group, skip to Step 13.

Step 13 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 added, and click Commit again.
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-100 appliances in Panorama mode, configured for active/passive high availability (HA). The firewalls send logs to the default (predefined) local Log Collector on each Panorama M-100 appliance. This is the recommended deployment if Panorama manages more than 10 firewalls and the firewalls generate up to 10,000 logs/second. (For details on deployment options, see Plan a Log Collection Deployment.)

It is a best practice to assign only one Log Collector to each Collector Group (Figure: Single Default Log Collector Per Collector Group). However, if any single firewall generates more than 4 TB of logs for the required log retention period, the Collector Group receiving the logs requires multiple Log Collectors (Figure: Multiple Default Log Collectors Per Collector Group). See Caveats for a Collector Group with Multiple Log Collectors to understand the risks and recommended mitigations associated with the latter configuration.

After implementing this deployment, if the logging rate increases beyond 10,000 logs per second, it is recommended that you add Dedicated Log Collectors (M-100 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
Perform the following steps to deploy Panorama with default Log Collectors. Skip any steps you have already performed (for example, the initial setup).

### Deploy Panorama with Default Log Collectors

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Perform the initial setup of each M-100 appliance.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>(Optional) for each Panorama appliance (primary and secondary) that requires more than the default 1TB of storage. This example uses the drives in disk bays B1 and B2.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enable connectivity between the M-100 appliances.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Record the serial number of the default Log Collector on the secondary Panorama. This is the serial number of the M-100 appliance. You will need this when you add the Log Collector as a managed collector.</td>
</tr>
</tbody>
</table>

#### Step 2
- In the CLI of the M-100 appliance, enter the following commands and confirm the request when prompted:
  - `request system raid add B1`
  - `request system raid add B2`

#### Step 3
- In the CLI of the primary Panorama, enter the following commands, where `<IP address2>` represents the management interface of the secondary Panorama.
  - `set deviceconfig system panorama-server <IP address2>`
  - `commit`
- In the CLI of the secondary Panorama, enter the following commands, where `<IP address1>` represents the management interface of the primary Panorama.
  - `set deviceconfig system panorama-server <IP address1>`
  - `commit`

#### Step 4
- Log in to the Panorama Web Interface of the secondary Panorama.
- In the Dashboard tab, General Information section, record the Serial # value.
| Step 5 | (Optional) If you will use SNMP to monitor the Log Collectors, configure the SNMP management software. | Load all the PAN-OS MIB files into your SNMP management software and, if necessary, compile them. Refer to your Simple Network Management Protocol (SNMP) manager documentation for the specific steps. |
| Step 6 | Add a Firewall as a Managed Device. Perform this step for all the firewalls you will assign to Log Collectors. | 1. If you have not already, perform the initial setup of each firewall that you will assign to a Log Collector.  
2. In the web interface of the primary M-100 appliance, select Panorama > Managed Devices, click Add, enter the serial number of each firewall (one line per serial number), and click OK. |
| Step 7 | Configure Log Forwarding to Panorama | By default, firewalls store all log files locally. You must configure the firewalls to forward logs to Panorama. |
| Step 8 | (Optional) If you will forward logs from Panorama to external services, configure a server profile for each service. | Use the web interface of the primary Panorama to perform the following steps:  
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 profiles:  
   • SNMP Trap server profile  
   • Syslog server profile  
   • Email server profile  
   You can configure separate profiles for different log types and severity levels or WildFire verdicts. You can also assign separate profiles to each Panorama HA peer when you configure the Collector Groups. For example, you might want each HA peer to forward logs to a different syslog server.  
   To forward firewall logs, you assign the server profiles when you configure the Collector Groups (Step 12).  
3. To forward the System and Config logs that the M-100 appliances generate:  
   a. Select Panorama > Log Settings > System.  
   b. For System logs, click each Severity level, assign the server profiles you just created, and click OK.  
   c. For Config logs, edit the Config settings, assign the server profiles you just created, and click OK. |
## Deploy Panorama with Default Log Collectors (Continued)

### Step 9  Modify Log Forwarding and Buffering Defaults.

- Use the web interface of the primary Panorama to perform the following steps:
  1. Select **Panorama > Setup > Management** and edit the Logging and Reporting Settings.
  2. Define the **Log Storage** and **Log Export and Reporting** settings as desired.

   - It is a best practice to select the **Buffered Log Forwarding from Device** option.
   - The **Log Storage** quotas and **Max Days** (expiration periods) you configure here apply only to the System and Config logs that Panorama generates. You set the storage settings for firewall logs when you configure the Collector Groups.

### Step 10  Configure a Managed Collector that is local to the primary Panorama.

- Because the default Log Collector is predefined on the M-100 appliance, you don’t need to add it, only edit it.

- Use the web interface of the primary Panorama to perform the following steps:
  1. Select **Panorama > Managed Collectors** and select the default Log Collector.
  2. If you configured separate M-100 interfaces during the task **Perform Initial Configuration of the M-100 Appliance**, in the **General** tab select the interfaces to use for **Device Log Collection** and **Collector Group Communication**. Otherwise, Panorama uses the management (mgmt) interface by default.
  3. If you increased storage capacity on the primary M-100 appliance, select the **Disks** tab and **Add** each additional disk pair.
  4. Click **OK** to save your changes.
### Deploy Panorama with Default Log Collectors (Continued)

**Step 11** Configure a Managed Collector that is local to the secondary Panorama.

Even though this Log Collector is local to the secondary Panorama, the Panorama management server treats it as a remote Log Collector because it’s not local to the primary Panorama. Therefore you must manually add it using the web interface of the primary Panorama.

<table>
<thead>
<tr>
<th>Use the web interface of the primary Panorama to perform the following steps:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. In the Panorama web interface, select <strong>Panorama &gt; Managed Collectors</strong> and click <strong>Add</strong>.</td>
</tr>
<tr>
<td>2. In the <strong>General</strong> tab, <strong>Collector S/N</strong> field, enter the serial number you recorded for the default Log Collector on the secondary Panorama.</td>
</tr>
<tr>
<td>3. Enter the IP address of the primary Panorama in the <strong>Panorama Server IP</strong> field and the IP address of the secondary Panorama in the <strong>Panorama Server IP 2</strong> field. <strong>The preceding fields are required.</strong></td>
</tr>
<tr>
<td>4. In the <strong>Authentication</strong> tab, enter a <strong>Password</strong> (the default is <strong>admin</strong>).</td>
</tr>
<tr>
<td>5. In the <strong>Management</strong> tab, complete one of the following field sets with the management interface values of the secondary Panorama:</td>
</tr>
<tr>
<td>• IPv4—<strong>IP Address</strong>, <strong>Netmask</strong>, and <strong>Default Gateway</strong></td>
</tr>
<tr>
<td>• IPv6—<strong>IPv6 Address/Prefix Length</strong> and <strong>Default IPv6 Gateway</strong> <strong>The preceding fields are required.</strong></td>
</tr>
<tr>
<td>6. If you configured Eth1 and/or Eth2 interfaces during the task <strong>Perform Initial Configuration of the M-100 Appliance</strong>, configure the settings in the <strong>Eth1</strong> and/or <strong>Eth2</strong> tabs. You must select the <strong>Eth1/Eth2</strong> check box in the corresponding tab to configure the settings.</td>
</tr>
<tr>
<td>7. Return to the <strong>General</strong> tab and select the interfaces to use for <strong>Device Log Collection</strong> and <strong>Collector Group Communication</strong>. Panorama uses the management (<strong>mgmt</strong>) interface by default. <strong>Eth1</strong> and <strong>Eth2</strong> are only available if you configured them in the corresponding tabs.</td>
</tr>
<tr>
<td>8. If you increased storage capacity on the secondary M-100 appliance, select the <strong>Disks</strong> tab and <strong>Add</strong> each additional disk pair.</td>
</tr>
<tr>
<td>9. Click <strong>OK</strong> and <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Panorama</strong>, and click <strong>Commit</strong> again. Wait until the HA synchronization finishes before proceeding.</td>
</tr>
</tbody>
</table>
Step 12 Configure a Collector Group.

Because the default Collector Group is predefined on the M-100 appliance, you don’t need to add it, only edit it.

Use the web interface of the primary Panorama to perform the following steps:

1. Select Panorama > Collector Groups and select the default Collector Group on the primary Panorama.

2. If you configured the SNMP management software to monitor Log Collectors, select the Monitoring tab and configure the SNMP settings.

3. In the Device Log Forwarding tab, Collector Group Members section, assign Log Collectors according to how many this Collector Group will have:
   - Single Log Collector—By default, the local Log Collector on the primary Panorama is pre-assigned to the default Collector Group so you do not need to assign any member.
   - Multiple Log Collectors—Assign the Log Collector that is local on the secondary Panorama. The local Log Collector on the primary Panorama is pre-assigned.

4. In the Device Log Forwarding Preferences section, assign firewalls according to the number of Log Collectors in this Collector Group:
   - Single Log Collector—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 Log Collectors—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. Return to the General tab, click the Log Storage value and allocate the desired Log Storage capacity (log quotas) and Max Days (expiration periods) for each firewall log type (System, Config, HIP Match, Traffic, Threat, and WildFire).

6. If you created server profiles for forwarding firewall logs from Panorama to external destinations, select the Collector Log Forwarding tab and assign server profiles for the desired external services. The profiles can be the same or different for each Collector Group.

The next step depends on your deployment:

- If you assigned all the Log Collectors to this Collector Group, skip to Step 14.
- If each Collector Group has only one Log Collector, perform Step 13 to add another Collector Group.
<table>
<thead>
<tr>
<th>Step 13</th>
<th>Deploy Panorama with Default Log Collectors (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Only if each Collector Group has one Log Collector) <strong>Configure a Collector Group</strong> for the Log Collector on the secondary Panorama.</td>
<td>Use the web interface of the primary Panorama to perform the following steps:</td>
</tr>
<tr>
<td></td>
<td>1. Select <strong>Panorama &gt; Collector Groups</strong>, click <strong>Add</strong>, and enter a <strong>Name</strong> for the Collector Group on the secondary Panorama. After you save the Collector Group, you cannot change its name.</td>
</tr>
<tr>
<td></td>
<td>2. If you configured the SNMP management software to monitor Log Collectors, select the <strong>Monitoring</strong> tab and configure the SNMP settings.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Device Log Forwarding</strong> tab, Collector Group Members section, assign the default Log Collector of the secondary Panorama.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Device Log Forwarding</strong> tab, 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.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>General</strong> tab, click the <strong>Log Storage</strong> value and allocate the desired <strong>Log Storage</strong> capacity (log quotas) and <strong>Max Days</strong> (expiration periods) for each firewall log type (System, Config, HIP Match, Traffic, Threat, and WildFire).</td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>OK</strong> to save your changes.</td>
</tr>
<tr>
<td></td>
<td>If you want each Panorama HA peer to forward firewall logs to a different destination (for example, different syslog servers), log in to the web interface of the secondary peer, select <strong>Panorama &gt; Collector Groups</strong>, select the Collector Group you just added, select the <strong>Collector Log Forwarding</strong> tab, assign the server profiles, and click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Step 14</td>
<td>Commit your changes.</td>
</tr>
<tr>
<td></td>
<td>Use the web interface of the primary Panorama to perform the following steps:</td>
</tr>
<tr>
<td></td>
<td>1. Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Panorama</strong>, and click <strong>Commit</strong> again.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Collector Group</strong>, select the Collector Groups you added, and click <strong>Commit</strong> again.</td>
</tr>
<tr>
<td>Step 15</td>
<td>Manually fail over so that the secondary Panorama becomes active.</td>
</tr>
<tr>
<td></td>
<td>Use the web interface of the primary Panorama to perform the following steps:</td>
</tr>
<tr>
<td></td>
<td>1. Select <strong>Panorama &gt; High Availability</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the Operational Commands section, click <strong>Suspend local Panorama</strong>.</td>
</tr>
</tbody>
</table>
### Deploy Panorama with Default Log Collectors (Continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 16</td>
<td>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 <strong>Panorama &gt; Managed Collectors</strong> and select the Log Collector that is local to the primary Panorama. 2. In the <strong>General</strong> tab, enter the IP address of the secondary Panorama in the <strong>Panorama Server IP</strong> field and the IP address of the primary Panorama in the <strong>Panorama Server IP 2</strong> field. 3. In the <strong>Management</strong> tab, complete one of the following field sets with the management interface values of the primary Panorama:  - IPv4—<strong>IP Address, Netmask</strong>, and <strong>Default Gateway</strong>  - IPv6—<strong>IPv6 Address/Prefix Length</strong> and <strong>Default IPv6 Gateway</strong>  - The preceding fields are required. 4. Click <strong>OK</strong> and <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Panorama</strong>, and click <strong>Commit</strong> again. Wait until the HA synchronization finishes before proceeding. 5. Click <strong>Commit</strong>, for the <strong>Commit Type</strong> select <strong>Collector Group</strong>, select the Collector Groups you added, and click <strong>Commit</strong> again.</td>
</tr>
</tbody>
</table>

### 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, configured for active/passive high availability (HA). The firewalls send logs to the Panorama management server (to its virtual disk or NFS datastore). By default, both the primary and secondary Panorama receive logs. This configuration suits firewall management within a VMware virtual infrastructure in which Panorama manages up to 10 firewalls and processes up to 10,000 logs/second. (For details on deployment options, see **Plan a Log Collection Deployment**.) By default, the Panorama virtual appliance has a single disk partition for all data, and 10.89GB of this space is allocated for log storage. If you need another 40GB to 2TB of disk space, **Add a Virtual Disk to the Panorama Virtual Appliance**. If you need more than 2TB, **Mount the Panorama Virtual Appliance to an NFS Datastore**.
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).

### Deploy Panorama Virtual Appliances with Local Log Collection

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
</table>
| **Step 1** | Perform the initial setup of each Panorama virtual appliance. | 1. Install Panorama on the ESXi Server.  
2. Perform Initial Configuration of the Panorama Virtual Appliance.  
3. (Optional) Expand Log Storage Capacity on the Panorama Virtual Appliance.  
4. Register Panorama and Install Licenses.  
5. Install Content and Software Updates for Panorama.  
6. Panorama High Availability. |
| **Step 2** | Add a Firewall as a Managed Device. Perform this step for all the firewalls that will forward logs to Panorama. | 1. If you have not already, perform the initial setup of each firewall that you will assign to a Log Collector.  
2. In the Panorama web interface, select Panorama > Managed Devices, click Add, enter the serial number of each firewall (one line per serial number), and click OK. |
| **Step 3** | Configure Log Forwarding to Panorama | By default, firewalls store all log files locally. You must configure the firewalls to forward logs to Panorama. |
Deploy Panorama Virtual Appliances with Local Log Collection  (Continued)

Step 4 (Optional) Configure log forwarding from Panorama to external services.

This step applies to logs that the Panorama virtual appliances generate (System and Config logs) and logs that Panorama collects from the firewalls (System, Config, HIP Match, Traffic, Threat, and/or WildFire logs).

Use the web interface of the primary Panorama to perform the following steps:
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 profiles:
   - SNMP Trap server profile
   - Syslog server profile
   - Email server profile
   If necessary, you can configure a separate profile for each log type and severity level or WildFire verdict.
4. 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.
5. For WildFire logs, click each Verdict, select the SNMP Trap, Email, or Syslog server profile you just created, and click OK.
6. For Config, HIP Match, and Traffic logs, click the icon, select the SNMP Trap, Email, or Syslog server profile you just created, and click OK.

Step 5 (Optional) Modify Log Forwarding and Buffering Defaults.

Use the Panorama web interface to perform the following steps:
1. Select Panorama > Setup > Management and edit the Logging and Reporting Settings.
2. Define the Log Storage and Log Export and Reporting settings as desired.
   If you want only the primary Panorama to receive logs, select the Only Active Primary Logs to Local Disk check box.
   It is a best practice to select the Buffered Log Forwarding from Device option.

Step 6 Commit your changes.

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

Manage Log Collection
Manage Licenses and Updates

As an administrator, you can use Panorama to centrally manage licenses and software/content updates on managed devices (firewalls and Log Collectors). 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/update on the devices. This capability facilitates deployment by eliminating the need to repetitively perform the tasks on each device. It is particularly useful for managing firewalls that do not have direct Internet access or for managing M-100 appliances in Log Collector mode, which do not support a web interface.

- Manage Licenses on Firewalls Using Panorama
- Deploy Updates to Devices Using Panorama

Before deploying updates, see Panorama, Log Collector, and Firewall Version Compatibility for important details about update version compatibility among Palo Alto Networks devices.

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 Panorama itself, see Register Panorama and Install Licenses and Install Content and Software Updates for 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 new licenses.</td>
</tr>
<tr>
<td>1. Select <strong>Panorama &gt; Device Deployment &gt; Licenses</strong> and click <strong>Activate</strong>. This option allows you to activate a newly purchased subscription, for example, a Threat subscription.</td>
</tr>
<tr>
<td>2. Find or filter for the managed firewalls and enter the authentication code(s) that Palo Alto Networks provided for the device in the <strong>Auth Code</strong> column.</td>
</tr>
<tr>
<td>3. Click <strong>Activate</strong>.</td>
</tr>
</tbody>
</table>

150 • Panorama 7.0 Administrator’s Guide  Palo Alto Networks
ManageLicenses on Firewalls Using Panorama (Continued)

- Update the license status of firewalls.

1. Select Panorama > Device Deployment > Licenses. Each entry on the tab indicates whether the license is active or inactive and displays the expiration date for active licenses.

2. If you have previously activated the auth-code for the support subscription directly on the firewall, click Refresh and select one or more firewalls from the list. Panorama retrieves the license(s), deploys it to the managed firewalls and updates the licensing status on the Panorama web interface.
Deploy Updates to Devices Using Panorama

You can use Panorama to qualify software and content updates by deploying them to a subset of the firewalls or Dedicated Log Collectors (M-100 appliances in Log Collector mode) before installing the updates on all managed devices. 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 depending on whether Panorama has an Internet connection.

- Supported Updates by Device Type
- Schedule a Content Update to Devices Using Panorama
- Install a Software Update on Firewall HA Pairs
- Deploy an Update to Devices when Panorama Has an Internet Connection
- Deploy an Update to Devices when Panorama Has No Internet Connection

You do not install SSL VPN client or GlobalProtect agent/app software on firewalls; you activate the software on firewalls so that users can download it onto client systems.

You cannot deploy GlobalProtect data file updates on demand; you can only schedule them

(DEVICE > DYNAMIC UPDATES) using templates or directly through the web interface of a firewall.

Supported Updates by Device Type

The software and content updates you can install depend on which subscriptions are active on each device and the device type:

<table>
<thead>
<tr>
<th>Device</th>
<th>Software Updates</th>
<th>Content Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedicated Log Collectors</td>
<td>Panorama</td>
<td>Applications signatures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Antivirus signatures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WildFire</td>
</tr>
<tr>
<td>Firewalls</td>
<td>PAN-OS</td>
<td>Applications signatures</td>
</tr>
<tr>
<td></td>
<td>SSL VPN client</td>
<td>Applications and Threats signatures</td>
</tr>
<tr>
<td></td>
<td>GlobalProtect agent/app</td>
<td>Antivirus signatures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BrightCloud URL filtering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WildFire</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GlobalProtect data files</td>
</tr>
</tbody>
</table>
Schedule a Content Update to Devices Using Panorama

For a list of content updates you can install on firewalls and Log Collectors, see Supported Updates by Device Type. Panorama requires a direct Internet connection for scheduled updates. Otherwise, you can perform only on-demand updates (see Deploy an Update to Devices when Panorama Has No Internet Connection). On each firewall receiving the update, PAN-OS generates a log to indicate the installation succeeded (Config log) or failed (System log).

Perform the following steps for each update type you want to schedule.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select Panorama &gt; Device Deployment &gt; Dynamic Updates, click Schedules, and click Add.</td>
</tr>
</tbody>
</table>
| 2    | Specify a Name to describe the schedule, the update Type, and the update frequency (Recurrence). The available frequency options depend on the update Type:  
  - **Wildfire**: Select Every 15 Mins, Every 30 Mins, or Every Hour.  
  - **WF-Private**: Select Every 5 Mins, Every 15 Mins, Every 30 Mins, or Every Hour.  
  - **Antivirus**:  
    - **Hourly**—Enter the Minutes Past the Hour when the update will start.  
    - **Daily**—Select the Time of day when the update will start.  
    - **Weekly**—Select the Day of the week and Time of day when the update will start.  
    - Other update types: Select Daily or Weekly.  
  
  PAN-OS uses the Panorama timezone for update scheduling.  
  The WildFire Private (**WF-Private**) option is only available if the WildFire Server field (**Panorama > Setup > WildFire**) is set to a WF-500 Wildfire appliance, not to the WildFire cloud. |
| 3    | Specify the Action to schedule:  
  - **Download And Install** (best practice)—Select the Devices (for firewalls) or Log Collectors option, then select the devices to which the update will apply.  
  - **Download Only**—Panorama downloads the update but does not install it on devices. |
| 4    | Click OK and Commit, for the Commit Type select Panorama, and click Commit again. |

Install a Software Update on Firewall HA Pairs

To avoid downtime when installing software updates on firewall peers in a high availability (HA) configuration, install the updates in the following sequence.
PAN-OS synchronizes the sessions of HA peers even when you upgrade between major releases (for example, from 6.0 to 6.1).

### Install a Software Update on Firewall HA Pairs

| Step 1 | Install the software update on the secondary firewall. | Log in to Panorama and perform one of the following procedures on the secondary firewall:  
- Deploy an Update to Devices when Panorama Has an Internet Connection  
- Deploy an Update to Devices when Panorama Has No Internet Connection  

For either procedure, in the Deploy Software File dialog, you must clear the **Group HA Peers** check box. In the HA Status column, icons indicate the peer state: green for active and yellow for passive. |
|---|---|---|
| Step 2 | Trigger a manual failover on the primary firewall so that it becomes passive and the secondary becomes active. | 1. Log in to the primary firewall, select **Device > High Availability > Operational Commands** and click **Suspend local device**.  
2. Log in to the secondary firewall and, on the **Dashboard, High Availability** widget, verify that the **Local** firewall state is **active** and the **Peer** firewall is **suspended**. |
| Step 3 | Install the software update on the primary firewall. | Repeat **Step 1** for the primary firewall. |
| Step 4 | Restore the primary firewall to the active state. | 1. Log in to the primary firewall, select **Device > High Availability > Operational Commands** and click **Make local device functional**.  
2. Wait two minutes and then, on the primary firewall **Dashboard, High Availability** widget, verify that the **Local** firewall state is **active** and the **Peer** firewall is **passive**. |

### Deploy an Update to Devices when Panorama Has an Internet Connection

For a list of software and content updates you can install on firewalls and Dedicated Log Collectors (M-100 appliances in Log Collector mode), see [Supported Updates by Device Type](https://www.paloaltonetworks.com/support/solutions).
Before deploying updates, see Panorama, Log Collector, and Firewall Version Compatibility for critical details about update version compatibility among Palo Alto Networks devices.

If both Panorama and managed firewalls require updates, upgrade Panorama (see Install Content and Software Updates for Panorama) before upgrading the firewalls.

If you must upgrade firewalls to a PAN-OS maintenance release for which the feature release is higher than the currently installed software, you must upload (without installing) the feature release to the firewalls before uploading and installing the maintenance release. For example, to upgrade firewalls from PAN-OS 5.0.12 to PAN-OS 6.0.3, you must upload PAN-OS 6.0.0 to the firewalls before you upload and install PAN-OS 6.0.3 on the firewalls.

Panorama displays a warning if you manually deploy a content update when an existing schedule has started or is scheduled to start within five minutes. For details, see Schedule a Content Update to Devices Using Panorama.

If you will deploy software updates to firewall pairs in a high availability (HA) configuration, install the updates on one peer at a time as described in Install a Software Update on Firewall HA Pairs.

---

### Deploy an Update to Devices when Panorama Has an Internet Connection

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select Panorama &gt; Device Deployment and select the update type: <strong>Software</strong> (PAN-OS), <strong>SSL VPN Client</strong>, <strong>GlobalProtect Client</strong> (GlobalProtect agent/app), or <strong>Dynamic Updates</strong> (content).</td>
</tr>
<tr>
<td>2</td>
<td>Click <strong>Check Now</strong> to check for the latest updates. If an update is available, the Action column displays <strong>Upgrade</strong> (for BrightCloud URL Filtering) or <strong>Download</strong> (for all other content categories and software).</td>
</tr>
</tbody>
</table>
| 3    | Review the Version, File Name, and Platform columns to determine the update you want to deploy. In the **Software** update page, the Platform values indicate the target platform for each software image:  
  - A number—PAN-OS software for hardware-based firewalls (for example, 5000 indicates the PA-5000 Series firewalls)  
  - vm—PAN-OS software for VM-Series firewalls  
  - m—Panorama software for the M-100 appliance (Dedicated Log Collector)  
  - PanVPN—SSL VPN client software  
  - PanGP—GlobalProtect agent/app software  |
| 4    | In the Action column of the desired update, click **Upgrade** or **Download**. After a successful upgrade/download, the value **Upgrade/Download** changes to **Install** (for content, Panorama, or PAN-OS updates) or **Activate** (for SSL VPN or GlobalProtect agent/app updates). 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. |
| 5    | Click **Install** or **Activate** and select the firewalls or Log Collectors on which to apply the update. You must install content updates before software updates. Also, you must install the Applications and Threats updates before the Antivirus and WildFire updates. URL Filtering updates have no restrictions in terms of installation sequence. |
| 6    | (PAN-OS software updates only) For firewalls that are in a high availability configuration, clear the **Group HA Peers** check box to upgrade one HA peer at a time. In the HA Status column, icons indicate the peer state: green for active and yellow for passive. |
Step 7  Select one of the following check boxes depending on your purpose:

- **Upload only to device (do not install)**—If the file you selected is for a feature release (for example, 6.0.0) and you will install a maintenance release (for example, 6.0.3) immediately after, select this option to create the libraries and directories that are required for the maintenance release.
- **Reboot device after install**—Select this option for all other scenarios. The installation cannot finish until the device reboots.

Step 8  Click **OK** to start the installation or upload. The results of the installation attempt appear on screen.

Step 9  To verify the software and content update versions running on each managed firewall, select **Panorama > Managed Devices**, locate the firewall (Device Name column) and review the values in the Software Version column.

Step 10  To verify the software and content update versions running on a Dedicated Log Collector, **Log in to the Panorama CLI of the M-100 appliance and enter the show system info command**. The output will resemble the following:

```
sw-version: 7.0
app-version: 366-1738
app-release-date: 2014/10/29 15:46:03
av-version: 1168-1550
av-release-date: 2014/10/21 14:31:27
threat-version: 366-1738
threat-release-date: 2014/10/29 15:46:03
```

**Deploy an Update to Devices when Panorama Has No Internet Connection**

For a list of software and content updates you can install on firewalls and Dedicated Log Collectors (M-100 appliances in Log Collector mode), see **Supported Updates by Device Type**.

Before deploying updates, see **Panorama, Log Collector, and Firewall Version Compatibility** for critical details about update version compatibility among Palo Alto Networks devices.

If both Panorama and managed firewalls require updates, upgrade Panorama (see **Install Content and Software Updates for Panorama**) before upgrading the firewalls.

If you need to upgrade firewalls to a PAN-OS maintenance release for which the feature release is higher than the currently installed software, you must upload (without installing) the feature release to the firewalls before uploading and installing the maintenance release. For example, to upgrade firewalls from PAN-OS 5.0.12 to PAN-OS 6.0.3, you must upload PAN-OS 6.0.0 to the firewalls before you upload and install PAN-OS 6.0.3 on the firewalls.

If you will deploy software updates to firewall pairs in high availability (HA) configuration, install the updates on one peer at a time as described in **Install a Software Update on Firewall HA Pairs**.
### Deploy an Update to Devices when Panorama Has No Internet Connection

**Step 1**  Download the update to a host that has Internet access. Panorama must have access to the host.

1. On a host with Internet access, go to the Palo Alto Support website (https://support.paloaltonetworks.com) and log in.
2. In the Resources section, select **Software Updates** or (for content) **Dynamic Updates**. In the **Software Updates** page, the filename of the update package indicates the following:
   - Software type—PanOS, Panorama, PanVPN (SSL VPN client), or PanGP (GlobalProtect agent/app)
   - Device model—A number for hardware-based firewalls, vm for VM-Series firewalls, or m for the M-100 appliance
   - Software release
3. In the Download column, click the **Download** link for the desired software or content update and save the file to the host.

**Step 2**  Upload the update.

By default, you can upload up to two software or content updates of each type to Panorama. When you start any upload 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**.

1. Log in to Panorama, select **Panorama > Device Deployment**, and select the update type: **Software** (PAN-OS), **SSL VPN Client, GlobalProtect Client** (GlobalProtect agent/app), or **Dynamic Updates** (content).
2. Click **Upload**.
3. (Content updates only) Select the update **Type**.
4. Enter the path to the update **File** on the host or click **Browse** to find it, and click **OK**.
## Deploy an Update to Devices when Panorama Has No Internet Connection (Continued)

| Step 3 | Install the update. | 1. Begin the installation according to the update type: |
|        |                    |   • Panorama or PAN-OS software—Click the Install link in the Action column. |
|        |                    |   • Content—Click the Install From File button. |
|        |                    |   • SSL VPN client or GlobalProtect agent/app—Click the Activate From File button. |
|        |                   | 2. (Content updates only) Select the update Type. |
|        |                   | 3. (Content, SSL VPN, or GlobalProtect updates only) In the File Name drop-down, select the file you just uploaded. |
|        |                   | 4. Select the firewalls or Log Collectors on which you want to apply the update. |
|        |                   | 5. If some firewalls are in a high availability (HA) configuration, clear the Group HA Peers check box to upgrade one HA peer at a time. In the HA Status column, icons indicate the peer state: green for active and yellow for passive. |
|        |                   | 6. (PAN-OS update only) Select one of the following check boxes: |
|        |                   |   • Upload only to device (do not install)—If the file you selected is for a feature release (for example, 6.0.0) and you will install a maintenance release (for example, 6.0.3) immediately after, select this option to create the libraries and directories that the maintenance release requires. |
|        |                   |   • Reboot device after install—Select this option for all other scenarios. The installation can't finish until the device reboots. |
|        |                   | 7. Click OK to start the installation. |

| Step 4 | Verify the software or content version running on each managed firewall. | 1. Select Panorama > Managed Devices. |
|        |                        | 2. Locate the firewall (Device Name column) and review the values in the Software Version, Apps and Threat, Antivirus, URL Filtering, and GlobalProtect Client columns. |

| Step 5 | Verify the software or content version running on each Log Collector. | Log in to the Panorama CLI of the M-100 appliance and enter the show system info command. The output will resemble the following: |
|        |                        |   sw-version: 6.1.0  
|        |                        |   app-version: 366-1738  
|        |                        |   app-release-date: 2014/10/29 15:46:03  
|        |                        |   av-version: 1168-1550  
|        |                        |   av-release-date: 2014/10/21 14:31:27  
|        |                        |   threat-version: 366-1738  
|        |                        |   threat-release-date: 2014/10/29 15:46:03  |
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

Use Panorama for Visibility

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 firewall. For details, see Context Switch—Firewall or Panorama.

<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>
Use Panorama for Visibility Monitor Network Activity

• **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 devices are on PAN-OS 7.0. 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.

• **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.

**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.
You can create the following types of reports:

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predefined</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>User-activity</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>Custom</td>
<td>Create and schedule custom reports that display exactly the information you want to see by filtering on conditions and columns to include. You can generate reports to query data from a summary database on Panorama or on the remote devices (that is the managed firewalls), or use the detailed reports on Panorama or on the remote devices. To view the databases available for generating these reports, see the <strong>Monitor &gt; Manage Custom Reports</strong> tab. 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>PDF Summary</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.
  
  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.

**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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select <strong>Monitor &gt; PDF Reports &gt; Report Groups</strong>.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Add</strong> and enter a <strong>Name</strong> for the report group.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>(Optional) Select the <strong>Title Page</strong> check box and add a <strong>Title</strong> for the PDF output.</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Click <strong>Add</strong> to include the selected reports in the report group.</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Click <strong>OK</strong> to save the settings.</td>
<td></td>
</tr>
</tbody>
</table>
### Generate, Schedule, and Email Reports (Continued)

#### Step 3  Configure an Email server profile.

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.

#### Step 4  Schedule the report for email delivery.

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. You can either glance over the list of top applications and mouse over each application block that you want to review the details for, or you can navigate to 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.

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.

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 remote devices 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.

Going back to the list of top applications, we can see that bittorrent is very popular. If you now click into the link for the bittorrent application, bittorrent is applied as a global filter and the display in the ACC pivots to show 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 also see how many users are using BitTorrent and the volume of traffic being generated. If you have enabled User-ID, you will be able to 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. View the **Compromised Hosts** widget in the **Threat Activity** tab 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.
Use Case: Monitor Applications Using Panorama

Monitor Network Activity

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 to 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. Then use Panorama templates to push this rule to one or more firewalls. Refer to Panorama Templates for defining QoS policy using templates.
- 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

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 gent.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.
Monitor Network Activity

Use Case: Respond to an Incident Using Panorama

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.

Look into the matching object and click the match count link to view the match evidence for the incident.
### Use Case: Respond to an Incident Using Panorama

#### Monitor Network Activity

**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, has a green arrow 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.

If you see a DNS-based spyware signature, the IP address of your local DNS server might display as the **Victim IP** address. Often this is because the firewall is located north of the local DNS server, and so DNS queries show the local DNS server as the source IP rather than showing the IP address of the client that originated the request.

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.

### Review WildFire Logs

In addition to the threat logs, use the victim IP address to filter through 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).

If WildFire determines that a file is malicious, a new antivirus signature is created within 24-48 hours and made available to you. If you have a WildFire subscription, the signature is made available within 30-60 minutes as part of the next WildFire signature update. As soon as the Palo Alto Networks next-generation firewall has received a signature for it, if your configuration is configured to block malware, the file will be blocked and the information on the blocked file will be visible in your threat logs. This process is tightly integrated to protect you from this threat and stems the spread of malware on your network.
**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.

**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 device context and configure the firewall for Botnet reports that identify potential botnet-infected hosts on the network.
Use Case: Respond to an Incident Using Panorama Monitor Network Activity
Panorama High Availability

Panorama High Availability (HA) is a configuration in which two Panorama servers are placed in a group (two-device 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-100 appliances) or virtual appliances. For HA, the M-100 appliances must be in Panorama mode; M-100 appliances in Log Collector mode do not support HA.

- **The same Panorama OS version**—Must be running the same version of Panorama in order to synchronize configuration information and maintain parity for a seamless failover.

- **The same set of licenses**—Must purchase and install the same device management capacity license for each Panorama.

- **(Panorama virtual appliance only) Unique serial number**—Must have a unique serial number for each Panorama virtual appliance; if the serial number is duplicated, both instances of Panorama will be placed in a suspended mode until you resolve the issue.

The Panorama servers in the HA configuration are peers and you can use either (active-primary or passive-secondary) to centrally manage the devices 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 devices 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. The maximum latency between the peers is 50ms. 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 device.

When a failover occurs, only the state (active or passive) of the device 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 device deployment functions such as license updates or software upgrades on the managed firewalls.
- 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 passive-secondary</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></td>
</tr>
<tr>
<td>Log to an NFS partition</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 device and the passive device 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 device 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 peer monitors whether the devices are still connected to it 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 device in a suspended state or if **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 device is the preferred active device.

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 devices 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 for network connectivity and link state for a specified IP address. The active peer uses ICMP pings to verify that one or more destination IP addresses can be reached. You can, for example, monitor the availability of an 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 device 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 devices are connected to both Panorama peers over SSL, when a state change occurs, each Panorama sends a message to the managed devices. The devices are notified of the Panorama HA state and can forward logs accordingly.

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-100 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 devices send logs as independent streams to each Panorama HA peer. By default, if a peer becomes unavailable, the managed devices 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 2TB. 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 devices.</td>
</tr>
<tr>
<td>Network File Share (NFS)</td>
<td>When configured to use an NFS, only the active-primary device 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 devices, 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-100 Appliance

If you are using a pair of M-100 appliances (must be in Panorama mode), the managed devices 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 devices to send logs to both peers, however, the RAID-enabled disks on the M-100 appliance protect against disk failure and loss of logs.

If you have a distributed log collection set up where the managed devices 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, 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, and Simple Network Management Protocol (SNMP) system settings
- 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)

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 with HA Configuration.

Set Up HA on Panorama

Review the Panorama HA Prerequisites before performing the following steps:

### Set Up HA on Panorama

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Step 1</strong></td>
<td>Set up connectivity between the MGT ports on the HA peers.</td>
</tr>
<tr>
<td>2. <strong>Step 2</strong></td>
<td>Enable HA and (optionally) enable encryption for the HA connection.</td>
</tr>
</tbody>
</table>

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 Set Up Panorama.

**Pick a device in the pair and complete the remaining tasks.**

1. Select **Panorama > High Availability** and edit the **Setup** section.
2. Select **Enable HA**.
3. In the **Peer HA IP Address** field, enter the IP address assigned to the peer device.
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).
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:
   a. Select **Panorama > Certificate Management > Certificates**.
   b. Select **Export HA key**. Save the HA key to a network location that the peer device can access.
   c. On the peer device, navigate to **Panorama > Certificate Management > Certificates**, select **Import HA key**, browse to the location where you saved the key, and import it.
## Set Up HA on Panorama (Continued)

### Step 3  Set the 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 link monitoring failure if any one of the IP addresses becomes unreachable.
   - **all** triggers a link 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.
Set Up HA on Panorama (Continued)

| 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>Step 1</th>
<th>Log in to the active Panorama peer.</th>
<th>You can verify the state of the Panorama server in the bottom right corner of the web interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Step 2</td>
<td>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></td>
<td>Step 3</td>
<td>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. In the Operational Commands section of the Device > High Availability tab, click the Make local Panorama functional link.  
|                           |        |                                    | 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

Support for a Network File Share (NFS) based logging mechanism is only available on the Panorama virtual appliance.

When a Panorama HA pair is configured to use a Network File Share (NFS) based logging mechanism, 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 is active-secondary. Although a secondary Panorama peer can actively manage the devices, it cannot receive logs or write to the NFS because it does not own the
NFS partition. When the managed device cannot forward logs to the primary Panorama peer, the logs are written to the local disk on each device. The devices maintain a pointer for the last set of log entries that were 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 devices, 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.

### Switch Priority after Panorama Failover to Resume NFS Logging

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log in to the currently passive-primary Panorama, select <strong>Panorama &gt; Setup &gt; Operations</strong> and, in the Device Operations section, click <strong>Shutdown Panorama</strong>.</td>
</tr>
<tr>
<td>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>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>4</td>
<td>Log in to the Panorama CLI 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>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>6</td>
<td>Power on the Panorama peer that you powered off in Step 1. 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 device so that all your uncommitted configuration changes are saved and can be accessed on the other peer.
## Suspend the Secondary Panorama

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Suspend Panorama.</th>
</tr>
</thead>
</table>
|        | 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. |

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Verify that the status displays that the device was suspended at user request.</th>
</tr>
</thead>
</table>
|        | 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. |

## Restore the Primary Panorama to a Functional State

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Restore the suspended Panorama to a functional state.</th>
</tr>
</thead>
</table>
|        | 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 device 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:

- Manage Configuration Backups
- Compare Changes in Panorama Configurations
- Validate a Panorama Configuration
- Restrict Access to Configuration Changes
- Add Custom Logos to Panorama
- View Panorama Task Completion History
- 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.
Manage Configuration Backups

A configuration backup is a snapshot of the system configuration. In case of a system failure or a misconfiguration, a configuration backup allows you to restore Panorama to a previously saved version of the configuration. On Panorama, you can manage configuration backups of the managed firewalls and that of Panorama:

- **Manage configuration backups of the managed devices**—Panorama automatically saves every configuration change that is committed to a managed firewall running PAN-OS version 5.0 or later. By default, Panorama stores up to 100 versions for each firewall. This value is configurable.

- **Manage Panorama configuration backups**—You can manually export the running configuration of Panorama, as required.

- **Export a configuration file package**—In addition to its own running configuration, Panorama saves a backup of the running configuration from all managed firewalls. You can generate a gzip package of the latest version of the configuration backup of Panorama and that of each managed firewall either on-demand or schedule an export using the **Scheduled Config Export** capability. The package can be scheduled for daily delivery to an FTP server or a Secure Copy (SCP) server; the files in the package are in an XML format, and each file name references the firewall serial number for easy identification.

You can perform the following tasks to manage configuration backups:

- **Schedule Export of Configuration Files**
- **Manage Panorama and Firewall Configuration Backups**
- **Configure the Number of Configuration Backups Panorama Stores**
- **Load a Configuration Backup on a Managed Firewall**
Schedule Export of Configuration Files

Use these instructions to schedule daily exports of the configuration file package that contains the backup of the running configuration of Panorama and the managed firewalls. You require superuser privileges to configure the export.

If Panorama has a high availability (HA) configuration, you must perform these instructions on each peer to ensure the scheduled exports continue after a failover. Panorama does not synchronize scheduled configuration exports between HA peers.

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select Panorama &gt; Scheduled Configuration Export.</td>
</tr>
<tr>
<td>2</td>
<td>Click Add, and enter a Name and Description for the file export process.</td>
</tr>
<tr>
<td>3</td>
<td>Select Enable to allow the configuration file export.</td>
</tr>
<tr>
<td>4</td>
<td>Using the 24-hour clock format, enter a daily Scheduled Export Start Time or select one from the drop-down.</td>
</tr>
<tr>
<td>5</td>
<td>For the export Protocol, select Secure Copy (SCP) or File Transfer Protocol (FTP).</td>
</tr>
<tr>
<td>6</td>
<td>Enter the details for accessing the server, including: Hostname or IP address, Port, Path for uploading the file, Username, and Password.</td>
</tr>
<tr>
<td>7</td>
<td>(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.</td>
</tr>
<tr>
<td>8</td>
<td>Click OK and Commit, for the Commit Type select Panorama, and click Commit again.</td>
</tr>
</tbody>
</table>
Manage Panorama and Firewall Configuration Backups

Step 1  Select Panorama > Setup > Operations.

Step 2  In the Configuration Management section, select from the following options:

- **Revert to last saved Panorama configuration**—Overwrites the current candidate configuration and restores the last saved candidate configuration from disk.

- **Revert to running Panorama configuration**—Reverts all changes saved to the candidate configuration; it effectively allows you to undo all configuration changes that were made since the last commit operation.

- **Save named Panorama configuration snapshot**—Saves the candidate configuration to a file. Enter a file name or select an existing file to overwrite. Note that the current active configuration file (running-config.xml) cannot be overwritten.

- **Save candidate Panorama configuration**—Saves the candidate configuration to disk; it is the same as using the Save link at the top of the page to save the changes to the candidate configuration file.

- **Load Panorama configuration version**—Loads a configuration file from a list of previously committed versions.

- **Load named Panorama configuration snapshot**—Loads a selected candidate configuration; you can select a previously imported or saved configuration. The current candidate configuration is overwritten.

- **Export named Panorama configuration snapshot**—Exports the active configuration (running-config.xml) or a previously saved or imported configuration. Select the configuration file to be exported. You can open the file and/or save it in any network location.

- **Export Panorama configuration version**—Exports a previously committed version of the configuration file. Select the version to export.

- **Export Panorama and devices config bundle**—This option is used to manually generate and export the latest version of the configuration backup of Panorama and that of each managed firewall. To automate the process of creating and exporting the configuration bundle daily to a Secure Copy (SCP) or FTP server, see Schedule Export of Configuration Files.

- **Export or push device config bundle**—After you import a firewall configuration into Panorama, Panorama creates a firewall configuration bundle named `<firewall_name>_import.tgz`, in which all local policies and objects are removed. You can then click Export or push device config bundle to perform one of the following actions:
  - **Push & Commit** the configuration bundle to the firewall. This action cleans the firewall (removes any local configuration from it), enabling you to manage the firewall from Panorama.
  - **Export** the configuration to the firewall without loading it. When you are ready to load the configuration, log in to the firewall CLI and run the configuration mode command `load device-state`. This command cleans the firewall in the same way as the Push & Commit option.

- **Import device configuration into Panorama**—Enables you to Import the firewall configuration into Panorama.

- **Import named Panorama configuration snapshot**—Imports a previously exported configuration file. Click Browse to locate the saved file and click OK to import.
Administer Panorama

Manage Configuration Backups

Configure the Number of Configuration Backups Panorama Stores

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Select <strong>Panorama &gt; Setup &gt; Management</strong> and edit the Logging and Reporting Settings.</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>For the <strong>Number of Versions for Config Backups</strong>, enter a value between 1 and 1048576. The default is 100.</td>
</tr>
<tr>
<td><strong>3</strong></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>

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, and the current candidate configuration on the firewall is overwritten.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Select <strong>Panorama &gt; Managed Devices</strong>.</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Select the <strong>Manage...</strong> link in the <strong>Backups</strong> column.</td>
</tr>
</tbody>
</table>
| **3** | Select from the **Saved Configurations** or the **Committed Configurations**.  
  • Click the link in the **Version** column to view the contents of the selected version.  
  • Click **Load** to load a chosen configuration version. |
| **4** | Click **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again. |
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 allows you to:

- Preview the changes in configuration 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.

### Compare Changes in Panorama Configurations

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select <strong>Panorama &gt; Config Audit</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>For each drop-down, select a configuration for the comparison.</td>
</tr>
</tbody>
</table>
| 3    | Select the number of lines that you want to include for **Context**, and click **Go**.  
To easily compare versions, the changes have color highlighting. |

### Configure the Number of Versions Panorama Stores for Configuration Audits

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select <strong>Panorama &gt; Setup &gt; Management</strong> and edit the Logging and Reporting Settings.</td>
</tr>
<tr>
<td>2</td>
<td>For the <strong>Number of Versions for Config Audit</strong>, enter a value between 1 and 1048576. The default is 100.</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

### View and Compare Panorama Configuration Files Before Committing

Click **Commit**, select **Preview Changes**, select the number of lines of context you want to see, and click **OK**.
Validate a Panorama Configuration

You can perform a syntactic validation (of configuration syntax) and semantic validation (whether the configuration is complete and makes sense) of a Panorama candidate configuration before committing it. The results display all the errors and warnings of a commit, including rule shadowing and application dependency warnings. For example, the validation could indicate an invalid route destination or a missing account and password that are required to query a server. This gives you the chance to fix errors before committing. You can independently validate the configurations of Panorama, device groups, and templates.

**Validate a Panorama Configuration**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>After modifying the Panorama configuration, click <strong>Commit</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>For the <strong>Commit Type</strong>, select <strong>Panorama</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>Click <strong>Validate Changes</strong>.</td>
</tr>
<tr>
<td></td>
<td>If the validation succeeds, the <strong>Result</strong> field displays <strong>OK</strong>. The <strong>Details</strong> field displays any errors or warnings.</td>
</tr>
</tbody>
</table>

**Validate a candidate configuration for a device group or template.**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Click <strong>Commit</strong>, for <strong>Commit Type</strong>, select <strong>Template</strong> or <strong>Device Group</strong>, and select a template or device group.</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional) Select the <strong>Merge with Device Candidate Config</strong> check box.</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional—device groups only) Select the <strong>Include Device and Network Templates</strong> check box.</td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>Validate Changes</strong>.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Status</strong> column displays any errors or warnings, and clicking the text displays details about them.</td>
</tr>
</tbody>
</table>
Restrict Access to Configuration Changes

Use locks to prevent multiple administrative users from making configuration changes or committing changes on Panorama, shared policy rules, or to selected templates and/or device groups.

- **Types of Locks**
- **Locations for Taking a Lock**
- **Take a Lock**
- **View Lock Holders**
- **Enable Automatic Acquisition of the Commit Lock**
- **Remove a Lock**

### Types of Locks

The available lock types are:

- **Config Lock**—Blocks other administrators from making changes to the configuration. This type of lock can be set globally or for a virtual system. It can be removed only by the administrator who set it or by a superuser. The configuration lock is not released automatically.

- **Commit Lock**—Blocks other administrators from committing changes until all of the locks have been released. The commit lock ensures that partial configuration changes are not inadvertently committed to the firewall or to Panorama when two administrators are making changes at the same time and the first administrator finishes and commits changes before the second administrator has finished. The lock is released automatically when the administrator who applied the lock commits the changes; the lock can be removed manually by the administrator who took the lock or by the superuser.

If a commit lock is held on a firewall, and an administrator commits configuration changes or shared policy rules to a template or device group that includes that firewall, the commit will fail with an error message indicating that there is an outstanding lock on a firewall.

---

**Read-only administrators who cannot make configuration changes to the firewall or Panorama will not be able to take either lock.**

Role-based administrators who cannot commit changes can take the config lock and save the changes to the candidate configuration. They cannot, however, commit the changes themselves. Because they cannot commit the changes, the lock is not automatically released on commit; the administrator must manually remove the config lock after making the required changes.

---

### Locations for Taking a Lock

The administrator can take a lock for any of the following:

- **Device group**—Restricts changes to the selected device group but not its descendant device groups.

- **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.)
Administer Panorama

Restrict Access to Configuration Changes

- **Shared**—Restricts changes to the centrally administered rules—pre-rules and post-rules—that are shared across all device groups. For more information on shared rules, see Device Group Policies.

- **Panorama**—Restricts access to changes on Panorama.

## Take a Lock

**Step 1**  Click the lock icon at the top right of the web interface.

**Step 2**  Select **Take Lock**.

**Step 3**  For the **Type**, based on your role/permissions, select **Commit** or **Config**.

**Step 4**  As a best practice, add a **Comment** to describe the reasons for taking the lock.

**Step 5**  Click **OK** and **Close**.

## View Lock Holders

Before changing a particular area of the configuration, check whether another administrator has taken the lock for the area.

Click the lock icon on the top right corner of the web interface and review the details.

The lock icon displays the total number of locks taken. It also includes information on the username of the lock holder, type of lock, the category in which the lock is held, when it was taken, the last activity by the administrator, and whether or not the administrator is still logged in.

## Enable Automatic Acquisition of the Commit Lock

By default, you must manually take a lock before you start making changes on Panorama. If you would like to enable automatic acquisition of the commit lock, use the following procedure.

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

**Step 2**  Select the **Automatically Acquire Commit Lock** check box.

**Step 3**  Click **OK** and **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.
### Remove a Lock

**Step 1** Click the lock icon at the top right of the web interface.

**Step 2** Select the lock that you want to release, click *Remove Lock*, and click **OK**.

Unless you are a superuser, you can remove only the lock that you previously took.
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.

Add Custom Logos to Panorama

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select <strong>Panorama &gt; Setup &gt; Operations.</strong></td>
</tr>
<tr>
<td>2</td>
<td>In the Miscellaneous section, click <strong>Custom Logos.</strong></td>
</tr>
<tr>
<td>3</td>
<td>Click the Upload logo icon and select an image for any of the following options: the login screen, the left corner of the main user interface, the PDF report title page and the PDF report footer.</td>
</tr>
<tr>
<td>4</td>
<td>Click <strong>Open</strong> to add the image. To preview the image, click the preview logo icon.</td>
</tr>
<tr>
<td>5</td>
<td>(Optional) To clear the green background header on the Panorama web interface, select the check box for <strong>Remove Panorama background header.</strong></td>
</tr>
<tr>
<td>6</td>
<td>Click <strong>Close</strong> to save your changes.</td>
</tr>
<tr>
<td>7</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>
View Panorama Task Completion History

Use the Task Manager to view currently-running tasks, historical task data, event success or failure information, and related errors.

**View Panorama Task Completion History**

**Step 1** Click the **Tasks** icon on the bottom right corner of the web interface.

**Step 2** Select the list of tasks to review. By default **All Tasks** are displayed.

![Task Manager Interface]

**Step 3** You can filter by **All** or **Running** tasks and select **Jobs**, **Reports**, or **Log Requests**:

- **Jobs**—Lists commits, auto commits, downloads and installs for software and dynamic updates performed on locally on Panorama or centrally pushed to the managed firewalls from Panorama. Each job is a link; click the link in the Type column to view details on the firewalls, status, and review errors, if any.

- **Reports**—Displays the status and start time for scheduled reports.

- **Log Requests**—Lists the log queries triggered from the **Monitor >Log Viewer** tab or the **Dashboard**. For example, to display the logs in the URL Filtering widget or the Data Filtering widget on the Dashboard, log requests are generated on Panorama.
Manage 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-100 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 the default 10GB disk created during installation, a virtual disk (see Add a Virtual Disk to the Panorama Virtual Appliance), or an NFS partition (see Mount the Panorama Virtual Appliance to an NFS Datastore). The storage space for reports is 200MB.

- **M-100 appliance**—Panorama saves logs to its internal SSD and RAID-enabled disks. The M-100 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 Config logs, System logs, and 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-100 appliance in Panorama mode or are in a Dedicated Log Collector (M-100 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.

- **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 the device deletes expired logs, the device doesn’t delete that log. The next time the device 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**

**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-100 appliance) receives from firewalls.
- System and Config logs that Panorama (a virtual appliance or M-100 appliance) and its Log Collectors generate locally.

If you reduce a log quota size, Panorama removes the oldest logs when you commit the changes.

- Select **Panorama > Setup > Management** and edit the **Logging and Reporting Settings**.
- 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.
- 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 undo your changes and reset the quotas and expiration periods to the factory defaults, click **Restore Quota Defaults** at the bottom right of the dialog.

**Step 2** Configure the expiration period for reports that Panorama (a virtual appliance or M-100 appliance) generates.

- Select the **Log Export and Reporting** tab.
- Enter the **Report Expiration Period** in days (range is 1-2,000). By default, the field is blank, which means reports never expire.
- Click **OK** to save your changes.
## Configure 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-100 appliance receives from firewalls. |

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 after assigning Log Collectors the field displays 0MB, verify you enabled the disk pairs for logging and committed the changes (see Step 10 under Configure a Managed Collector).
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.

   If you must undo your changes and reset the quotas and expiration periods to the factory defaults, click **Restore Quota Defaults** at the bottom right of the dialog.

| Step 4 | Commit your changes. |

1. Click **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.
2. (M-100 appliance only) Click **Commit**, for the **Commit Type** select **Collector Group**, select the Collector Group you modified, and click **OK**.
Monitor Panorama

To monitor Panorama and its managed collectors, you can periodically view their System and Config logs (filter the log data by device), 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-100 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 statistics 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-100 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-100 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 Palo Alto Networks devices implement SNMP, see SNMP for Palo Alto Networks Devices.

Monitor Panorama and Log Collector Statistics Using SNMP

<table>
<thead>
<tr>
<th>Step</th>
<th>Configure the SNMP Manager to get statistics from Panorama and the Log Collectors.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>To enable the SNMP manager to interpret device statistics, load the Supported MIBs for Palo Alto Networks devices and, if necessary, compile them.</td>
</tr>
<tr>
<td>2.</td>
<td>For each Panorama M-100 or virtual appliance that the SNMP manager will monitor, define the connection settings (IP address and port) and authentication settings (SNMPv2c community string or SNMPv3 username and password) for the device. All Palo Alto Networks devices use port 161. The SNMP manager can use the same or different connection and authentication settings for multiple devices. The settings must match those you define when you configure SNMP on the device (see Step 4). For example, if you use SNMPv2c, the community string you define when configuring the device must match the community string you define in the SNMP manager for that device.</td>
</tr>
<tr>
<td>3.</td>
<td>Determine the object identifiers (OIDs) of the statistics you will monitor. For example, to monitor the logging rate, a MIB browser shows that this statistic corresponds to OID 1.3.6.1.4.1.25461.2.3.30.1.1 in PAN-PRODUCT-MIB.my. For details, see Use an SNMP Manager to Explore MIBs and Objects.</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the SNMP manager to monitor the desired OIDs.</td>
</tr>
</tbody>
</table>
Monitor Panorama and Log Collector Statistics Using SNMP (Continued)

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Enable SNMP traffic on the management (MGT) interface of the Panorama management server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Select Panorama &gt; Setup &gt; Management and edit the Management Interface Settings.</td>
</tr>
<tr>
<td></td>
<td>2. In the Services section, select the SNMP check box and click OK.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enable SNMP traffic on the management (MGT) interface of any M-100 appliances in Log Collector mode:</td>
</tr>
<tr>
<td></td>
<td>1. Select Panorama &gt; Managed Collectors and select the Log Collector.</td>
</tr>
<tr>
<td></td>
<td>2. Select the Management tab, select the SNMP check box, and click OK.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure the Panorama management server to respond to statistics requests from an SNMP manager.</td>
</tr>
<tr>
<td></td>
<td>1. Select Panorama &gt; Setup &gt; Operations and, in the Miscellaneous section, click SNMP Setup.</td>
</tr>
<tr>
<td></td>
<td>2. Select the SNMP Version and configure the authentication values as follows. For version details, see SNMP for Palo Alto Networks Devices.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>Don’t use the default community string public; it is well known and therefore not secure.</td>
</tr>
<tr>
<td></td>
<td>• 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 device statistics.</td>
</tr>
<tr>
<td></td>
<td>– 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.</td>
</tr>
<tr>
<td></td>
<td>– 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.</td>
</tr>
<tr>
<td></td>
<td>3. Click OK to save the settings.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure the Dedicated Log Collectors (if any) to respond to SNMP requests.</td>
</tr>
<tr>
<td></td>
<td>For each Collector Group:</td>
</tr>
<tr>
<td></td>
<td>1. Select Panorama &gt; Collector Groups and select the Collector Group.</td>
</tr>
<tr>
<td></td>
<td>2. Select the Monitoring tab, configure the same settings as in Step 4, and click OK.</td>
</tr>
</tbody>
</table>

Monitor Panorama and Log Collector Statistics Using SNMP (Continued)
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| **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.

### Reboot or Shut Down Panorama

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select <strong>Panorama &gt; Setup &gt; Operations</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Device Operations section, select <strong>Reboot Panorama</strong> or <strong>Shutdown Panorama</strong>.</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.

### Configure Panorama Password Profiles and Complexity

**Step 1** Configure minimum password complexity settings.

1. Select **Panorama > Setup > Management** and edit the Minimum Password Complexity section.
2. Select **Enabled**.
3. Define the **Password Format Requirements**. You can enforce the requirements for uppercase, lowercase, numeric, and special characters that a password must contain.
4. To prevent the account username (or reversed version of the name) from being used in the password, select **Block Username Inclusion (including reversed)**.
5. Define the password **Functionality Requirements**. 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.
Configure Panorama Password Profiles and Complexity (Continued)

Step 2 Create password profiles.

You can create multiple password profiles and apply them to administrator accounts as required to enforce security.

1. Select Panorama > Password Profiles and click Add.
2. Enter a Name for the password profile and define the following:
   a. **Required Password Change Period**: Frequency, in days, at which the passwords must be changed.
   b. **Expiration Warning Period**: Number of days before expiration that the administrator will receive a password reminder.
   c. **Post Expiration Grace Period**: Number of days that the administrator can still log in to the system after the password expires.
   d. **Post Expiration Admin Login Count**: Number of times that the administrator can log in to the system after the password has expired.
Troubleshooting

The following topics address Panorama issues:

- Troubleshoot Panorama System Issues
- Troubleshoot Log Storage and Connection Issues
- Replace an RMA Firewall
- Diagnose Template Commit Failures
- 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. In order to assist Palo Alto Networks Technical Support in troubleshooting an issue, the support representative might request diagnostic files—tech support file or a stats dump file. The following procedure describes how to download a diagnostic file and upload it to your support case.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select Panorama &gt; Support.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Click Generate Tech Support File.</td>
</tr>
<tr>
<td></td>
<td>Click Generate Stats Dump File.</td>
</tr>
</tbody>
</table>

| Step 2 | Download and save the file(s) to your computer. |

| Step 3 | Upload the file(s) to your case on the Support Portal. |

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 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

On Panorama, you can download (or manually upload) software images and content updates to centrally manage them on firewalls and M-100 appliances in Log Collector mode. Supported Updates by Device Type lists which updates these devices support. For Panorama itself, you can also manage updates for Applications, Applications and Threats, Antivirus, and Wildfire.

The amount of space available on Panorama to store these images and updates is not user configurable. When the used capacity of the allotted storage reaches 90%, Panorama alerts you to free up space (delete stored images) for new downloads/uploads.

The maximum number of images is a global setting that applies to all the images and updates that Panorama stores. You can use only the CLI to configure this setting. The default value is two images or 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 images or updates of each type.</td>
</tr>
<tr>
<td>• View the number of images that Panorama currently stores.</td>
</tr>
</tbody>
</table>
Troubleshoot Panorama System Issues

Manage Panorama Storage for Software and Content Updates (Continued)

- Delete images and updates to free up space on Panorama.

<table>
<thead>
<tr>
<th>To delete images and updates using the CLI:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Delete software images by filename:</td>
</tr>
<tr>
<td>delete software image &lt;filename&gt;</td>
</tr>
<tr>
<td>• Delete software images by version:</td>
</tr>
<tr>
<td>delete software version &lt;version_number&gt;</td>
</tr>
<tr>
<td>• Delete content updates:</td>
</tr>
<tr>
<td>delete content update &lt;filename&gt;</td>
</tr>
</tbody>
</table>

To delete images and updates using the web interface:

- Delete firewall or Log Collector software images or updates that were downloaded or uploaded to Panorama for deployment:
  a. Select **Panorama > Device Deployment** and select the image or update type: **Software**, **SSL VPN Client**, **GlobalProtect Client**, or **Dynamic Updates**.
  b. Click the icon in the far right column for the image or update.

- Delete Panorama software images:
  a. Select **Panorama > Software**.
  b. Click the icon in the far right column for the image or update.

- Delete Panorama content updates:
  a. Select **Panorama > Dynamic Updates**.
  b. Click the icon in the far right column for the image or update.

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 re-established the configuration is synchronized.

- If you need to add/change the configuration at only one Panorama location, make the changes and sync the configuration (make sure that you initiate the sync from the peer on which you made the changes) when the link between the Panorama peers is re-established.

- 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-100 Appliance
- Replace the Virtual Disk on a Panorama Virtual Appliance
- Recover Logs after Failure/RMA of M-100 Appliance in Log Collector Mode
- Recover Logs after Failure/RMA of M-100 Appliance in Panorama Mode
- Recover Logs after Panorama Failure/RMA in Non-HA Deployments
- Regenerate Metadata for M-100 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.

On an M-100 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 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.)

<table>
<thead>
<tr>
<th>Communicating Devices &amp; Direction of Connection Establishment</th>
<th>Ports Used: 5.0 and 5.1</th>
<th>Ports Used: 6.0 and 6.1</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panorama and Panorama (HA)</td>
<td>28</td>
<td>28</td>
<td>For HA connectivity and synchronization if encryption is enabled.</td>
</tr>
<tr>
<td>Direction: Each peer initiates its own connection to the other</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Panorama and Panorama (HA)</td>
<td>28769 and 28260 (5.1)</td>
<td>28260 and 28769</td>
<td>For HA connectivity and synchronization if encryption is not enabled.</td>
</tr>
<tr>
<td>Direction: Each peer initiates its own connection to the other</td>
<td>28769 and 49160 (5.0)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Panorama and managed firewalls</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>
<tr>
<td>Direction: Initiated by the firewall</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting

Troubleshoot Log Storage and Connection Issues

<table>
<thead>
<tr>
<th>Communicating Devices &amp; Direction of Connection Establishment</th>
<th>Ports Used: 5.0 and 5.1</th>
<th>Ports Used: 6.0 and 6.1</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**

The log storage capacity for the Collector Group might display as 0MB if the disk pairs are not enabled for logging. You must select the Log Collector and enable the disk pairs for logging in the Panorama > Managed Collectors tab; for instructions, see Step 10 in the Manage Collector Groups topic.

To verify that the disks are enabled and available for log storage, select Panorama > Managed Collectors tab and verify that the Log Collector displays as Connected and that the Configuration Status displays as In sync.

**Replace a Failed Disk on an M-100 Appliance**

If a disk fails on the M-100 appliance, you must replace the disk and reconfigure it in a RAID pair. This allows the data to be mirrored and synchronized between the disks in the RAID pair.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Install the new disk in the appropriate drive bay. Refer to the M-100 Hardware Reference Guide for instructions to replace the failed with the new disk.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Set up the disk in a RAID pair. The time required to mirror the data on the drive may vary from several minutes to a couple hours, depending on the amount of data on the drive. This example uses the drives in the disk bays B1.</td>
</tr>
<tr>
<td></td>
<td>1. Enter the following commands to add the disk to the RAID pair and confirm the request when prompted: <strong>request system raid add B1</strong></td>
</tr>
<tr>
<td></td>
<td>2. To monitor the progress of the RAID configuration and verify that the disk is RAID enabled, enter the following command: <strong>show system raid detail</strong></td>
</tr>
</tbody>
</table>
Replace the Virtual Disk on a Panorama Virtual Appliance

You cannot resize a virtual disk after adding it to a Panorama virtual appliance. Because the Panorama virtual appliance allows only one log storage location, if you need to increase or decrease disk space for logging, you must replace the virtual disk on the ESXi server to adjust the log storage capacity.

### Replace the Virtual Disk on a Panorama Virtual Appliance

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Export the logs before detaching the virtual disk from the Panorama virtual appliance. The logs on the disk will no longer be accessible after the disk is detached.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Access the CLI on the Panorama virtual appliance.</td>
</tr>
<tr>
<td></td>
<td>2. Check the current disk usage:</td>
</tr>
<tr>
<td></td>
<td>admin@Panorama&gt; show system logdb-quota</td>
</tr>
<tr>
<td></td>
<td>3. Export the logs. The command has the following syntax:</td>
</tr>
<tr>
<td></td>
<td>admin@Panorama&gt; scp export logdb to &lt;user account&gt;@&lt;IP of SCP server&gt;: &lt;directory path with destination filename&gt;</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>admin@Panorama&gt; scp export logdb to sabel@10.236.10.30:/Panorama/log_file_exportMay2013</td>
</tr>
<tr>
<td></td>
<td>You must specify a filename. The command saves a .tar file with that filename to the Secure Copy (SCP) server.</td>
</tr>
<tr>
<td></td>
<td>Because the export process compresses the files, the size of the exported file will be smaller than the size on disk.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Replace the virtual disk.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Power off the Panorama virtual appliance.</td>
</tr>
<tr>
<td></td>
<td>2. Edit the settings on the Panorama virtual appliance to add a new virtual disk with the desired capacity. The virtual disk type must be IDE and the maximum capacity is 2TB.</td>
</tr>
<tr>
<td></td>
<td>3. Remove the virtual disk you want to replace.</td>
</tr>
</tbody>
</table>
Replace the Virtual Disk on a Panorama Virtual Appliance  (Continued)

Step 3  Import the logs into the new virtual disk.

1. Power on the Panorama virtual appliance. The reboot process might take several minutes and the message cache data unavailable will appear.
2. Log in to the Panorama virtual appliance.
3. Select Panorama > Setup > Management and verify that the Logging and Reporting Settings section displays the modified log storage capacity accurately.
4. Use the Panorama CLI to import the logs into the new virtual disk:

   admin@Panorama> scp import logdb from <user account>@<IP of SCP server>: <directory path with destination filename>

Recover Logs after Failure/RMA of M-100 Appliance in Log Collector Mode

If a system failure occurs on an M-100 appliance in Log Collector mode (Dedicated Log Collector), use the following procedure to recover the logs on the replacement M-100 appliance. This procedure applies whether the Panorama management server that manages the Log Collector is a Panorama virtual appliance or an M-100 appliance in Panorama mode.

**Replace the Virtual Disk on a Panorama Virtual Appliance  (Continued)**

Step 1  Perform the following tasks on the new/replacement M-100 appliance in Log Collector mode.

1. Set Up the M-100 Appliance.
2. Register Panorama.
3. Switch from Panorama Mode to Log Collector Mode.
4. Transfer licenses as necessary: refer to How to Transfer Licenses from RMA Device.
Troubleshoot Log Storage and Connection Issues

Recover Logs after Failure/RMA of M-100 Appliance in Log Collector Mode (Continued)

Step 2  On the Panorama management server that is managing the M-100 appliance in Log Collector mode, add the new Log Collector as a managed collector.

1. See Manage Collector Groups or use the following CLI commands:
   
   \texttt{configure set log-collector <log-collector_SN> deviceconfig system hostname <log-collector-hostname> exit}

2. Verify that the Log Collector has been added and is connected to Panorama.
   
   \texttt{show log-collector serial-number <log-collector_SN>}
   
   The disk pairs will display as disabled at this stage of the restoration process. Verify that the status is present/available.

3. Commit your changes to Panorama. Do not commit the changes to the Collector Group just yet.
   
   \texttt{configure commit exit}

Step 3  Remove the RAID disks from the failed M-100 appliance.

1. Power off the M-100 appliance.

2. Make sure to maintain the disk pair association as you remove them from the appliance.

   Although a disk in slot A can be placed in Slot B on the replacement device, the pair has to kept together in the same slot; if the pair is separated the data might not be successfully restored.

Step 4  Prepare the disks for migration.

   Generating the metadata for each disk pair rebuilds the indexes. Therefore, depending on the data size, this process can take a long time to complete. If you are replacing 4 RAID pairs, you can launch 4 CLI sessions and issue the command independently in each session to complete the metadata regeneration process simultaneously for all the pairs. To understand more, see Regenerate Metadata for M-100 Appliance RAID Pairs.

1. Insert the disks in the new M-100 appliance in Log Collector mode.

2. For each disk pair that you need to migrate, issue the following command to enable the disk pair(s) on the new Log Collector.

   \texttt{request system raid add <slot> force no-format}

   For example:

   \texttt{request system raid add A1 force no-format request system raid add A2 force no-format}

   The \texttt{force} and \texttt{no-format} options in this command are required. The \texttt{force} option associates the disk pair with this replacement appliance; the \texttt{no-format} option prevents reformatting the drives and retains the logs stored on the disks.

3. Generate the metadata for each disk pair.

   \texttt{request metadata-regenerate slot <slot_number>}

   For example:

   \texttt{request metadata-regenerate slot 1}
### Troubleshooting Troubleshoot Log Storage and Connection Issues

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Migrate the logs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>For each disk pair complete the migration of the logs from the old Log Collector to the new Log Collector. The following command attaches the disk pair to the new appliance.</td>
<td></td>
</tr>
</tbody>
</table>
| \[
| \text{request log-migration from} \\
| \quad \text{<SN_of_old_log_collector> old-disk-pair} \\
| \quad \text{<log_disk_pair> to <SN_of_new_log_collector>} \\
| \quad \text{new-disk-pair <log_disk_pair>} \\
| \]
| For example: |
| \[
| \text{request log-migration from 003001000010} \\
| \quad \text{old-disk-pair A to 003001000038 new-disk-pair A} \\
| \]

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Reconfigure the Collector Group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Add the new Log Collector as a member of the Collector Group.</td>
<td></td>
</tr>
<tr>
<td>configure</td>
<td></td>
</tr>
</tbody>
</table>
| \text{set log-collector-group <collector_group_name>} \\
| \text{logfwd-setting collectors <SNManaged_collector>} \\
| For example: |
| \[
| \text{set log collector-group DC-Collector-Group} \\
| \text{logfwd-setting devices 0030010110010} \\
| \]
| 2. Redefine the preference list used by the managed firewalls. Repeat the command for each managed firewall. |
| configure |
| \text{set log collector-group <group_name> logfwd-setting devices <device_serial_number>} \\
| For example: |
| \[
| \text{set log collector-group DC-Collector-Group logfwd-setting devices 0030010110010} \\
| \]
| 3. Delete the failed Log Collector from the Panorama configuration and commit your changes to Panorama. |
| configure |
| \text{delete log-collector <old_serial>} \\
| \text{commit} \\
| For example: |
| \[
| \text{delete log-collector 003001000010} \\
| \text{commit} \\
| \]
| 4. Commit the Collector Group changes so that the managed firewalls can send logs to the new Log Collector. |
| configure |
| \text{commit-all log-collector-config} \\
| \text{log-collector-group <collector_group_name>} \\
| For example: |
| \[
| \text{commit-all log-collector-config} \\
| \text{log-collector-group DC-Collector-Group} \\
| \]

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Synchronize the configuration between the Panorama HA peers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>To synchronize the running configuration with the Panorama HA peer, click the <strong>Sync to peer</strong> link in the High Availability widget on the Dashboard or use the following CLI command.</td>
<td></td>
</tr>
</tbody>
</table>
| \[
| \text{request high-availability sync-to-remote running-config} \\
| \]

---

Recover Logs after Failure/RMA of M-100 Appliance in Log Collector Mode (Continued)
Recover Logs after Failure/RMA of M-100 Appliance in Panorama Mode

You can recover logs from a RAID disk on an M-100 appliance in Panorama mode only if the Panorama is configured in a High Availability (HA) pair. In the event of an M-100 appliance system failure, you can transfer the RAID disks in to a replacement M-100 appliance and recover the logs stored on the disks of the failed appliance. The ability to migrate the disks to another appliance allows you to regain access to the log data and to resume log queries and generate reports.

This workflow covers the following scenarios where the M-100 appliances are deployed in Panorama mode and are configured in an HA configuration:

- One Panorama in the pair is configured as a managed Log Collector and is receiving logs from the managed firewalls.

- Both Panorama peers are managed Log Collectors that belong to one Collector Group (Note that this is not a recommended deployment).

- Each Panorama is configured as a managed collector and assigned to separate Collector Groups (Log Collector Group1 and Log Collector Group2).

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Power off the M-100 appliance.</td>
</tr>
<tr>
<td>2.</td>
<td>Make sure to mark the disk pairs as you remove them from the appliance. Although a disk in slot A can be placed in Slot B on the replacement device, the pair has to kept together in the same slot; if the pair is separated the data might not be successfully restored.</td>
</tr>
</tbody>
</table>
Troubleshooting

Troubleshoot Log Storage and Connection Issues

Recover Logs after Failure/RMA of M-100 Appliance in Panorama Mode (Continued)

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Perform the following tasks on the new/replacement M-100 appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Set Up the M-100 Appliance.</td>
</tr>
<tr>
<td></td>
<td>2. Register Panorama.</td>
</tr>
<tr>
<td></td>
<td>3. Transfer licenses as necessary: refer to How to Transfer Licenses from RMA Device.</td>
</tr>
<tr>
<td></td>
<td>4. Set the HA priority value to match that of the peer you are replacing. See Manage a Panorama HA Pair for more information.</td>
</tr>
<tr>
<td></td>
<td>5. Verify that HA is functional.</td>
</tr>
</tbody>
</table>

Step 3 Prepare the disks for migration.

- Generating the metadata for each disk pair rebuilds the indexes. Therefore, depending on the data size, this process can take a long time to complete. If you are replacing 4 RAID pairs, you can launch 4 CLI sessions and issue the command independently in each session to complete the metadata regeneration process simultaneously for all the pairs. To understand more, see Regenerate Metadata for M-100 Appliance RAID Pairs.

- Insert the disks in to the new M-100 appliance.
- For each disk pair that you need to migrate, issue the following command to enable the disk pair(s) on the new Log Collector. 
  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 options in this command are required. The force option associates the disk pair with this replacement appliance; the no-format option prevents reformatting the drives and retains the logs stored on the disks.
- Generate the metadata for each disk pair.
  request metadata-regenerate slot <slot_number>
  For example:
  request metadata-regenerate slot 1

Step 4 Synchronize the configuration from the other Panorama peer to this replacement Panorama.

To synchronize the running configuration with the Panorama HA peer, click the Sync to peer link in the High Availability widget on the Dashboard or use the following CLI command.
request high-availability sync-to-remote running-config

Step 5 Add the new Log Collector as a managed collector.

- Do not enable the disks on the managed collector, yet. This disks will be enabled automatically when the logs are successfully migrated.
- Generating the metadata for each disk pair, rebuilds the indexes. Therefore, depending on the data size, this process can take a long time to complete. See Diagnose Template Commit Failures.

- See Manage Collector Groups or use the following CLI commands:
  configure
  set log-collector <log-collector_SN> deviceconfig
  system hostname <log-collector-hostname>
  exit
- Verify that the Log Collector has been added and is connected to Panorama.
  show log-collector serial-number <log-collector_SN>
  The disk pairs will display as disabled at this stage of the restoration process. Verify that the status is present/available.
- Commit your changes to Panorama. Do not commit the changes to the Collector Group just yet.
  configure
  commit
  exit
### Troubleshoot Log Storage and Connection Issues

#### Troubleshooting

**Step 6** Migrate the logs.

1. For each disk pair, issue the command to complete the migration of the logs to the new appliance.
   
   ```
   request log-migration from <SN_of_old_log_collector> old-disk-pair <log_disk_pair> to <SN_of_new_log_collector> new-disk-pair <log_disk_pair>
   ```
   
   For example:
   ```
   request log-migration from 003001000010 old-disk-pair A to 003001000038 new-disk-pair A
   ```

2. Commit the changes to Panorama.
   ```
   configure
   commit
   exit
   ```

**Step 7** Reconfigure the Collector Group.

1. Add the managed collector as a member of the Collector Group.
   ```
   set log-collector-group <collector_group_name> logfwd-setting collectors <SN_managed_collector>
   ```
   
   The old Log Collector still appears in the list of members, because you did not yet delete it from the configuration.

2. Redefine the preference list that the managed firewalls use for forwarding logs.
   ```
   set log collector-group <group_name> logfwd-setting devices <device_serial_number>
   ```

3. Delete the failed Log Collector from the Collector Group.
   ```
   delete log collector-group <group_name> logfwd-setting collectors <old_serial>
   ```
   
   For example:
   ```
   delete log collector-group DC-Collector-Group logfwd-setting collectors 003001000010
   ```

4. Commit the changes to Panorama.

5. 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
   ```
Troubleshoot Log Storage and Connection Issues

Recover Logs after Failure/RMA of M-100 Appliance in Panorama Mode (Continued)

Step 8  Synchronize the running configuration between the Panorama HA peers.

1. In order to make sure that the running configuration is synchronized with the Panorama HA peer, click the Sync to peer link in the High Availability widget on the Dashboard to initiate a manual synchronization.

2. On the active-primary Panorama peer, confirm that the configuration is synchronized.

Recover Logs after Panorama Failure/RMA in Non-HA Deployments

If a system failure occurs on a Panorama server that is managing one or more Dedicated Log Collectors and the Panorama server is not deployed in an HA configuration, use this procedure to restore the configuration on the replacement Panorama and regain access to the logs on the Log Collectors.

To manage data, Panorama maintains a ring file that maps the segments and partitions used for storing logs on the Log Collector. This ring file is stored to the internal SSD on an M-100 appliance or on the internal disk of the Panorama virtual appliance that manages the Log Collector(s). When Panorama is not configured in HA and a system failure occurs, the ring file cannot be automatically recovered. Therefore, when you replace Panorama, in order to access the logs on the managed Collectors, you must restore the ring file.

As a best practice, Palo Alto Networks recommends deploying Panorama in an HA configuration. When deployed in HA, the primary Panorama peer that manages the Log Collectors stores the ring file to its internal storage (SSD of an M-100 appliance or the internal disk of the Panorama VM). Panorama then automatically synchronizes this ring file to the secondary/passive peer, thereby maintaining access to logs on the managed Log Collectors.

Use the following workflow after you have registered the new appliance and transferred licenses on the Support Portal as needed (refer to How to Transfer Licenses from RMA Device), performed initial configuration and retrieved the license on the replacement Panorama.
### Recover Logs after Panorama Failure/RMA in Non-HA Deployments

| Step 1 | **Restore the configuration from the old Panorama to the replacement Panorama.**  
This task assumes that you have followed the recommendation to back up and export your Panorama configuration in order to recover from a system failure.  
|---|---|
| **Step 2** | **Verify that connections to the managed collectors are restored.**  
Select **Panorama > Managed Collectors** and check that the managed collectors are connected.  
If the managed collector does not display, it indicates that you do not have the most recent Panorama configuration. Your configuration snapshot was taken before the managed Log Collector/Collector Group configuration was implemented on Panorama. For reconfiguring the managed Log Collector/Collector Group configuration, see **Step 4**.  
| **Step 3** | **Fetch the ring file to restore access to the logs stored on the managed collector.**  
1. Access the CLI on Panorama.  
2. Enter the following command to fetch the ring file:  
   ```
   request fetch ring from log-collector <serial_number>
   ```  
   For example:  
   ```
   request fetch ring from log-collector 009201000343
   ```  
   3. Commit your changes to the Collector Group.  

| Step 1 | Restore the configuration from the old Panorama server to the new server.  
1. Select **Panorama > Setup > Operations.**  
2. Select **Import named Panorama configuration snapshot**, **Browse** to locate the saved file and click **OK** to import.  
3. Select **Load named Panorama configuration snapshot** and select the version you just imported.  
4. Click **Commit**, for the **Commit Type** select **Panorama**, and click **Commit** again.  

| Step 2 | Select **Panorama > Managed Collectors** and check that the managed collectors are connected.  
If the managed collector does not display, it indicates that you do not have the most recent Panorama configuration. Your configuration snapshot was taken before the managed Log Collector/Collector Group configuration was implemented on Panorama. For reconfiguring the managed Log Collector/Collector Group configuration, see **Step 4**.  
|---|---|
| Step 3 | Fetch the ring file to restore access to the logs stored on the managed collector.  
1. Access the CLI on Panorama.  
2. Enter the following command to fetch the ring file:  
   ```
   request fetch ring from log-collector <serial_number>
   ```  
   For example:  
   ```
   request fetch ring from log-collector 009201000343
   ```  
   3. Commit your changes to the Collector Group.  

---
Regenerate Metadata for M-100 Appliance RAID Pairs

When a system failure occurs on the M-100 appliance and you need to physically replace 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.

You need to issue this command for every RAID disk pair configured in your M-100 appliance. The length of time required to regenerate the metadata depends on the size of the RAID disks; on average, it takes an hour to regenerate metadata for every 100 GB. When you run the command the current CLI session is locked-up till

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | Access the CLI on the managed collector and enter the following commands to view the last entries in the log. These command allow you to verify the name of the managed collector that you must define on Panorama.  
   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_convertResp_ring_to_file(pan_ops_cms.c: 3719): Current configuration does not contain group CA-Collector-Group
      ```  
      The error message indicates that the missing Collector Group has the name CA-Collector-Group.  
| 2.   | Create the Collector Group on Panorama, and add the managed collector as a member of this Collector Group.  
      ```
      set log-collector-group CA-Collector-Group
      set log-collector-group CA-Collector-Group
      logfwd-setting collector 009201000343
      ```  
| 3.   | Commit the changes to Panorama. Do not commit to Collector group at this point.  
| 4.   | Fetch the fetch the ring file from the Log Collector using the command:  
      ```
      request fetch ring from log-collector <serial_number>
      ```  
| 5.   | Commit the changes to the Collector Group.  
      ```
      commit-all log-collector-config
      log-collector-group <log_collector_group_name>
      ```
the command is fully executed. Therefore, if you are replacing 4 RAID pairs, you can launch 4 CLI sessions and issue the command independently in each session to complete the metadata regeneration process simultaneously for all the pairs/slots in about 10 hours for 4TB of log data.

When the metadata is being regenerated, the Collector Group to which these disks belong is not available yet and the disk pair is not available for any logging and reporting operations (writes/queries). You can, however, perform other tasks such as handling new firewall connections or managing configuration changes on the managed firewalls. All other Collector Groups managed by this Panorama, which are not a part of this RMA process, can perform the assigned logging and reporting functionality as normal.
Troubleshooting

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/replacement 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 device 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 configuration on a managed firewall:

- Centralized configuration managed by Panorama—Panorama maintains a snapshot of the shared policy rules and templates that it pushes to firewalls.
- Local configuration on the firewall—When a configuration change is committed, each firewall sends a copy of its local configuration file to Panorama. Panorama stores this file and uses it to compile the partial device state bundle.

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 managed firewall (that was replaced) must have been on PAN-OS 5.0.4 and later version. Panorama cannot generate the device state for firewalls running older PAN-OS versions. If you need to restore the configuration for a firewall running a version earlier than PAN-OS 5.0.4, refer to the article Configuration Recovery with Panorama.
- Record the following details about the old firewall:
Replace an RMA Firewall Troubleshooting

– **Serial number**—You must enter the serial number on the Support portal to transfer the licenses from the old firewall to your replacement firewall. You will also enter this information on Panorama, to replace all references to the older serial number with the 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 allows you to create the same state on the replacement firewall. If you decide to install the latest version of the content database, you may notice differences because of updates and additions to the database. To verify 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 of the same model and is enabled for similar operational capability. Consider the following operational features: does it need to be enabled for multi-virtual systems, support jumbo frames, or be enabled to operate in CC or FIPS mode?

  – Configure network access, transfer the licenses, and install the appropriate PAN-OS version and the content database version.

• You must use the Panorama CLI to complete this firewall replacement process. This CLI-based workflow is available for the *superuser* and *panorama-admin* user roles.

• If you have an LSVPN configuration, and are replacing a Palo Alto Networks firewall deployed as a satellite device 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 have been following the recommendation to frequently generate and export the device state for firewalls in an LSVPN configuration, use the device state that you have 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 portal device** that is explicitly configured with the serial number of the satellite devices (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 satellite devices successfully. The successful authentication will populate the dynamic configuration information and LSVPN connectivity will be reinstated.

  – **If you are replacing a satellite firewall**, the satellite firewall will not be able to connect and authenticate to the portal. This connection failure occurs either because the serial number was not explicitly configured on the firewall (Network > GlobalProtect > Portals > Satellite Configuration) or because although the serial number was explicitly configured, 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. When this authentication occurs, 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.
## Troubleshooting Replace an RMA Firewall

### Restore the Firewall Configuration after Replacement

<table>
<thead>
<tr>
<th>Tasks on the new firewall:</th>
<th>Use the CLI for a more streamlined workflow.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Perform initial configuration 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 firewall can access the Palo Alto Networks updates server.</td>
</tr>
<tr>
<td><strong>Step 2</strong> (Optional) Set the Operational mode to match that on the old firewall. A serial port connection is required for this task.</td>
<td>1. Enter the following CLI command to access maintenance mode on the firewall: <code>debug system maintenance-mode</code> 2. To boot into the maintenance partition, enter <code>maint</code> during the boot sequence. 3. Select the Operational mode as Set FIPS Mode or Set CCEAL 4 Mode from the main menu.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Retrieve the license(s).</td>
<td>Enter the following command to retrieve your licenses: <code>request license fetch</code></td>
</tr>
<tr>
<td><strong>Step 4</strong> (Optional) Match the operational state of the new firewall with that of the old firewall. For example, enable multi-virtual system (multi-vsys) capability for a firewall that was enabled for multi-vsys capability.</td>
<td>Enter the commands that pertain to your firewall settings: <code>set system setting multi-vsxs on</code> <code>set system setting jumbo-frame on</code></td>
</tr>
<tr>
<td><strong>Step 5</strong> Upgrade the PAN-OS version on the firewall. You must upgrade to the same OS and content database version that is installed on the old firewall.</td>
<td>Enter the following commands: 1. To upgrade the content database version: <code>request content upgrade download &lt;xxx-xxxx&gt;</code> 2. To install the content database version that you downloaded: <code>request content upgrade install version &lt;xxx-xxxx&gt;</code> 3. To upgrade the PAN-OS software version: <code>request system software download version 5.x.x</code> 4. To install the content database version that you downloaded: <code>request system software install version 5.x.x</code></td>
</tr>
</tbody>
</table>

### Tasks on the Panorama CLI: You cannot perform these tasks on the Panorama web interface.

(Skip this step if you have manually exported the device state from your firewall.)

**Step 6** Export the device state bundle to a computer using Secure Copy (SCP) or TFTP.  
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 <new serial#> to <login> @ <serverIP>: <path>
```

or,
```
tftp export device-state device <new serial#> to <login> @ <serverIP>: <path>
```
Replace an RMA Firewall

Troubleshooting

## Restore the Firewall Configuration after Replacement (Continued)

<table>
<thead>
<tr>
<th>Step 7</th>
<th>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.</th>
</tr>
</thead>
</table>
| 1. Enter the following command in Operational mode: `replace device old <old SN#> new <new SN#>`  
2. Enter Configuration mode and commit your changes.  
3. Exit Configuration mode. |

### Tasks on the new firewall:

**You can use the firewall web interface to perform these tasks.**

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Import the device state and commit the changes on the firewall.</th>
</tr>
</thead>
</table>
| 1. Access the web interface of the 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 your changes to the running configuration on the firewall.  
5. To confirm that the device state restored includes the references to Panorama pushed policies and objects, verify that a little green icon appears beside the device name. |

### Tasks on Panorama:

**You can now use the Panorama web interface to access and manage the replaced firewall.**

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Verify that the firewall configuration was successfully restored.</th>
</tr>
</thead>
</table>
| 1. Access the Panorama web interface and select **Panorama > Managed Devices**.  
2. Verify that the Connected column for the replaced firewall has a check mark icon.  
3. To synchronize the firewall with Panorama, click **Commit**, for the **Commit Type** select **Device Group**, select the device group that contains the firewall, select the **Include Device and Network Template** check box, and click **Commit** again. |

---

After replacing the firewall, if you need to generate reports for a period that spans the duration when the old firewall was functional and after you installed the replacement firewall, you must generate a separate query for the serial number of each firewall because replacing the serial number on Panorama does not overwrite the information in the logs.
Diagnose Template Commit Failures

A template commit could fail because of the following reasons:

- Capability mismatch: When configuring a template, the following options are available: multiple virtual systems capability, VPN mode, and Operational mode.
  - If the multiple virtual systems capability is enabled (the Virtual systems check box is selected), a template commit failure will occur when you push the template to firewalls that are not capable of, or enabled for, multiple virtual systems functionality. To resolve the error, select Panorama > Templates, click the template name to edit it, and clear the Virtual systems check box.
  - If you push VPN-related configuration options to firewalls that are hard-coded to disallow VPN configuration. To resolve the error, select Panorama > Templates, click the template name to edit it, and select the VPN Disable Mode check box.
  - If the Operational mode on the firewall differs from that on the template. For example, the managed firewall might be enabled for FIPS mode while the template is enabled for normal mode. To resolve the error, select Panorama > Templates, click the template name to edit it, and verify that the Operational mode selection is correct.

- The managed firewall is not enabled for receiving template and device group changes from Panorama. This happens when the ability to receive template and device groups configuration changes has been disabled on the firewall.
  
  To resolve the error, access the web interface of the firewall, select Device > Setup, edit the Panorama Settings section, and then click Enable Device and Network Template and Enable Panorama Policy and Objects.
View Task Success or Failure Status

Use 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 View Panorama Task Completion History.