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

About the Documentation
• For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal www.paloaltonetworks.com/documentation.
• To search for a specific topic, go to our search page www.paloaltonetworks.com/documentation/document-search.html.
• Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright
Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2017-2019 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised
September 19, 2019
# Table of Contents

## Panorama Overview

- About Panorama................................................................. 11
- Panorama Models............................................................... 12
- Centralized Firewall Configuration and Update Management.................................................. 14
  - Context Switch—Firewall or Panorama........................................ 14
  - Templates and Template Stacks............................................. 14
  - Device Groups.................................................................... 15
- Centralized Logging and Reporting.................................................. 20
  - Managed Collectors and Collector Groups.................................... 20
  - Local and Distributed Log Collection..................................... 21
  - Caveats for a Collector Group with Multiple Log Collectors............ 22
  - Log Forwarding Options..................................................... 24
  - Centralized Reporting......................................................... 25
- User-ID Redistribution Using Panorama............................................ 26
- Role-Based Access Control.......................................................... 27
  - Administrative Roles........................................................ 27
  - Authentication Profiles and Sequences.................................... 28
  - Access Domains.................................................................. 29
  - Administrative Authentication............................................... 29
- Panorama Commit, Validation, and Preview Operations.......................... 31
- Plan Your Panorama Deployment.................................................. 32
- Deploy Panorama: Task Overview................................................ 34

## Set Up Panorama

- Determine Panorama Log Storage Requirements........................................... 37
- Set Up the Panorama Virtual Appliance..................................................... 39
  - Setup Prerequisites for the Panorama Virtual Appliance......................... 39
  - Install the Panorama Virtual Appliance.............................................. 41
  - Perform Initial Configuration of the Panorama Virtual Appliance............... 44
- Set Up the M-Series Appliance............................................................... 57
  - M-Series Appliance Interfaces.................................................... 57
  - M-Series Setup Overview....................................................... 57
- Perform Initial Configuration of the M-Series Appliance........................... 58
- Set Up the M-Series Appliance as a Log Collector...................................... 61
- Increase Storage on the M-Series Appliance............................................. 67
- Configure Panorama to Use Multiple Interfaces....................................... 73
- Register Panorama and Install Licenses................................................... 80
  - Register Panorama.................................................................... 80
  - Activate a Panorama Support License........................................... 83
  - Activate/Retrieve a Firewall Management License on the Panorama Virtual
    Appliance............................................................................... 85
  - Activate/Retrieve a Firewall Management License on the M-Series Appliance... 85
- Install Content and Software Updates for Panorama...................................... 88
  - Panorama, Log Collector, Firewall, and WildFire Version Compatibility........ 88
  - Install Updates for Panorama in an HA Configuration......................... 88
TABLE OF CONTENTS

Manage Log Collection ................................................................................. 169

Use Case: Configure Firewalls Using Panorama .............................................................................162
Transition a Firewall to Panorama Management ............................................................................153
Redistribute User-ID Information to Managed Firewalls ..............................................................150
Manage Templates and Template Stacks .........................................................................................145
Manage Device Groups ........................................................................................................................ 132
Set Up Authentication Using Custom Certificates .........................................................................121
Set Up Administrative Access to Panorama .................................................................................... 109
Set Up Your Centralized Configuration and Policies ........................................................ 164
Templates in this Use Case .....................................................................................................163
Device Groups in this Use Case ............................................................................................ 162
Load a Partial Firewall Configuration into Panorama ....................................................... 159
Migrate a Firewall HA Pair to Panorama Management ....................................................157
Migrate a Firewall to Panorama Management ................................................................... 154
Plan the Transition to Panorama Management ..................................................................153
Transition to a Different Panorama Model.................................................................................. 98
Migrate from a Panorama Virtual Appliance to an M-Series Appliance.................................98
Migrate from an M-Series Appliance to a Panorama Virtual Appliance.................................100
Migrate from an M-100 Appliance to an M-500 Appliance.....................................................102
Access and Navigate Panorama Management Interfaces............................................................106
Log in to the Panorama Web Interface..................................................................................... 106
Navigate the Panorama Web Interface.................................................................................... 106
Log in to the Panorama CLI...................................................................................................... 107
Set Up Administrative Access to Panorama................................................................................ 109
Configure an Admin Role Profile............................................................................................ 109
Configure an Access Domain.................................................................................................. 109
Configure Administrative Accounts and Authentication.............................................................110
Set Up Authentication Using Custom Certificates......................................................................121
How Are SSL/TLS Connections Mutually Authenticated?..................................................121
Configure Authentication Using Custom Certificates on Panorama........................................122
Configure Authentication Using Custom Certificates on Managed Devices..........................123
Add New Client Devices........................................................................................................ 125
Change Certificates................................................................................................................ 125
Manage Firewalls..........................................................................................................................129
Add a Firewall as a Managed Device....................................................................................... 131
Manage Device Groups.............................................................................................................. 132
Add a Device Group................................................................................................................ 132
Create a Device Group Hierarchy............................................................................................ 132
Create Objects for Use in Shared or Device Group Policy..................................................... 134
Revert to Inherited Object Values.............................................................................................135
Manage Unused Shared Objects............................................................................................... 135
Manage Precedence of Inherited Objects................................................................................ 136
Move or Clone a Policy Rule or Object to a Different Device Group......................................... 137
Select a URL Filtering Vendor on Panorama.............................................................................138
Push a Policy Rule to a Subset of Firewalls.............................................................................. 142
Manage the Rule Hierarchy...................................................................................................... 142
Manage Templates and Template Stacks.................................................................................... 145
Template Capabilities and Exceptions..................................................................................... 145
Add a Template....................................................................................................................... 145
Configure a Template Stack..................................................................................................... 146
Override a Template Setting.....................................................................................................148
Disable/Remove Template Settings............................................................................................148
Redistribute User-ID Information to Managed Firewalls..........................................................150
Transition a Firewall to Panorama Management........................................................................ 153
Plan the Transition to Panorama Management........................................................................ 153
Migrate a Firewall to Panorama Management........................................................................ 154
Migrate a Firewall HA Pair to Panorama Management............................................................ 157
Load a Partial Firewall Configuration into Panorama............................................................. 159
Use Case: Configure Firewalls Using Panorama.........................................................................162
Device Groups in this Use Case............................................................................................... 162
Templates in this Use Case....................................................................................................... 163
Set Up Your Centralized Configuration and Policies............................................................... 164

Manage Log Collection.............................................................................................................. 169
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a Managed Collector</td>
<td>171</td>
</tr>
<tr>
<td>Manage Collector Groups</td>
<td>174</td>
</tr>
<tr>
<td>Configure a Collector Group</td>
<td>174</td>
</tr>
<tr>
<td>Move a Log Collector to a Different Collector Group</td>
<td>176</td>
</tr>
<tr>
<td>Remove a Firewall from a Collector Group</td>
<td>177</td>
</tr>
<tr>
<td>Configure Log Forwarding to Panorama</td>
<td>178</td>
</tr>
<tr>
<td>Verify Log Forwarding to Panorama</td>
<td>182</td>
</tr>
<tr>
<td>Modify Log Forwarding and Buffering Defaults</td>
<td>184</td>
</tr>
<tr>
<td>Configure Log Forwarding from Panorama to External Destinations</td>
<td>186</td>
</tr>
<tr>
<td>Log Collection Deployments</td>
<td>188</td>
</tr>
<tr>
<td>Deploy Panorama with Dedicated Log Collectors</td>
<td>188</td>
</tr>
<tr>
<td>Deploy Panorama M-Series Appliances with Local Log Collectors</td>
<td>193</td>
</tr>
<tr>
<td>Deploy Panorama Virtual Appliances with Local Log Collectors</td>
<td>198</td>
</tr>
<tr>
<td>Deploy Panorama Virtual Appliances in Legacy Mode with Local Log Collection</td>
<td>202</td>
</tr>
<tr>
<td>Manage WildFire Appliances</td>
<td>205</td>
</tr>
<tr>
<td>Add Standalone WildFire Appliances to Manage with Panorama</td>
<td>207</td>
</tr>
<tr>
<td>Configure Basic WildFire Appliance Settings on Panorama</td>
<td>210</td>
</tr>
<tr>
<td>Remove a WildFire Appliance from Panorama Management</td>
<td>211</td>
</tr>
<tr>
<td>Manage Licenses and Updates</td>
<td>213</td>
</tr>
<tr>
<td>Manage Licenses on Firewalls Using Panorama</td>
<td>215</td>
</tr>
<tr>
<td>Deploy Updates to Firewalls, Log Collectors, and WildFire Appliances Using Panorama</td>
<td>216</td>
</tr>
<tr>
<td>Supported Updates</td>
<td>216</td>
</tr>
<tr>
<td>Schedule a Content Update Using Panorama</td>
<td>217</td>
</tr>
<tr>
<td>Upgrade Log Collectors When Panorama Is Internet-Connected</td>
<td>218</td>
</tr>
<tr>
<td>Upgrade Log Collectors When Panorama Is Not Internet-Connected</td>
<td>220</td>
</tr>
<tr>
<td>Upgrade Firewalls When Panorama Is Internet-Connected</td>
<td>222</td>
</tr>
<tr>
<td>Upgrade Firewalls When Panorama Is Not Internet-Connected</td>
<td>222</td>
</tr>
<tr>
<td>Monitor Network Activity</td>
<td>227</td>
</tr>
<tr>
<td>Use Panorama for Visibility</td>
<td>229</td>
</tr>
<tr>
<td>Monitor the Network with the ACC and AppScope</td>
<td>229</td>
</tr>
<tr>
<td>Analyze Log Data</td>
<td>231</td>
</tr>
<tr>
<td>Generate, Schedule, and Email Reports</td>
<td>231</td>
</tr>
<tr>
<td>Ingest Traps ESM Logs on Panorama</td>
<td>234</td>
</tr>
<tr>
<td>Use Case: Monitor Applications Using Panorama</td>
<td>236</td>
</tr>
<tr>
<td>Use Case: Respond to an Incident Using Panorama</td>
<td>239</td>
</tr>
<tr>
<td>Incident Notification</td>
<td>239</td>
</tr>
<tr>
<td>Review the Widgets in the ACC</td>
<td>239</td>
</tr>
<tr>
<td>Review Threat Logs</td>
<td>240</td>
</tr>
<tr>
<td>Review WildFire Logs</td>
<td>240</td>
</tr>
<tr>
<td>Review Data Filtering Logs</td>
<td>241</td>
</tr>
<tr>
<td>Update Security Rules</td>
<td>241</td>
</tr>
<tr>
<td>Panorama High Availability</td>
<td>243</td>
</tr>
<tr>
<td>Panorama HA Prerequisites</td>
<td>245</td>
</tr>
<tr>
<td>Priority and Failover on Panorama in HA</td>
<td>247</td>
</tr>
<tr>
<td>Failover Triggers</td>
<td>248</td>
</tr>
<tr>
<td>HA Heartbeat Polling and Hello Messages</td>
<td>248</td>
</tr>
<tr>
<td>HA Path Monitoring</td>
<td>248</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>281</td>
</tr>
<tr>
<td>Troubleshoot Panorama System Issues</td>
<td>283</td>
</tr>
<tr>
<td>Generate Diagnostic Files for Panorama</td>
<td>283</td>
</tr>
<tr>
<td>Diagnose Panorama Suspended State</td>
<td>283</td>
</tr>
<tr>
<td>Monitor the File System Integrity Check</td>
<td>283</td>
</tr>
<tr>
<td>Manage Panorama Storage for Software and Content Updates</td>
<td>283</td>
</tr>
<tr>
<td>Recover from Split Brain in Panorama HA Deployments</td>
<td>284</td>
</tr>
<tr>
<td>Troubleshoot Log Storage and Connection Issues</td>
<td>286</td>
</tr>
<tr>
<td>Verify Panorama Port Usage</td>
<td>286</td>
</tr>
<tr>
<td>Resolve Zero Log Storage for a Collector Group</td>
<td>288</td>
</tr>
<tr>
<td>Replace a Failed Disk on an M-Series Appliance</td>
<td>288</td>
</tr>
<tr>
<td>Replace the Virtual Disk on an ESXi Server</td>
<td>288</td>
</tr>
<tr>
<td>Replace the Virtual Disk on vCloud Air</td>
<td>289</td>
</tr>
<tr>
<td>Migrate Logs to a New M-Series Appliance in Log Collector Mode</td>
<td>290</td>
</tr>
<tr>
<td>Migrate Logs to a New M-Series Appliance in Panorama Mode</td>
<td>294</td>
</tr>
<tr>
<td>Migrate Logs to a New M-Series Appliance Model in Panorama Mode in High Availability</td>
<td>300</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Panorama</td>
<td>275</td>
</tr>
<tr>
<td>Panorama System and Configuration Logs</td>
<td>275</td>
</tr>
<tr>
<td>Monitor Panorama and Log Collector Statistics Using SNMP</td>
<td>275</td>
</tr>
<tr>
<td>Reboot or Shut Down Panorama</td>
<td>278</td>
</tr>
<tr>
<td>Configure Panorama Password Profiles and Complexity</td>
<td>279</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administer Panorama</td>
<td>257</td>
</tr>
<tr>
<td>Preview, Validate, or Commit Configuration Changes</td>
<td>259</td>
</tr>
<tr>
<td>Manage Panorama and Firewall Configuration Backups</td>
<td>262</td>
</tr>
<tr>
<td>Schedule Export of Configuration Files</td>
<td>262</td>
</tr>
<tr>
<td>Save and Export Panorama and Firewall Configurations</td>
<td>263</td>
</tr>
<tr>
<td>Revert Panorama Configuration Changes</td>
<td>264</td>
</tr>
<tr>
<td>Configure the Maximum Number of Configuration Backups on Panorama</td>
<td>266</td>
</tr>
<tr>
<td>Load a Configuration Backup on a Managed Firewall</td>
<td>266</td>
</tr>
<tr>
<td>Compare Changes in Panorama Configurations</td>
<td>267</td>
</tr>
<tr>
<td>Manage Locks for Restricting Configuration Changes</td>
<td>268</td>
</tr>
<tr>
<td>Add Custom Logos to Panorama</td>
<td>270</td>
</tr>
<tr>
<td>Use the Panorama Task Manager</td>
<td>271</td>
</tr>
<tr>
<td>Manage Storage Quotas and Expiration Periods for Logs and Reports</td>
<td>272</td>
</tr>
<tr>
<td>Log and Report Storage</td>
<td>272</td>
</tr>
<tr>
<td>Log and Report Expiration Periods</td>
<td>272</td>
</tr>
<tr>
<td>Configure Storage Quotas and Expiration Periods for Logs and Reports</td>
<td>273</td>
</tr>
<tr>
<td>Configure the Run Time for Panorama Reports</td>
<td>274</td>
</tr>
<tr>
<td>Monitor Panorama</td>
<td>275</td>
</tr>
<tr>
<td>Panorama System and Configuration Logs</td>
<td>275</td>
</tr>
<tr>
<td>Monitor Panorama and Log Collector Statistics Using SNMP</td>
<td>275</td>
</tr>
<tr>
<td>Reboot or Shut Down Panorama</td>
<td>278</td>
</tr>
<tr>
<td>Configure Panorama Password Profiles and Complexity</td>
<td>279</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Migrate Logs to the Same M-Series Appliance Model in Panorama Mode in High Availability</td>
<td>306</td>
</tr>
<tr>
<td>Migrate Log Collectors after Failure/RMA of Non-HA Panorama</td>
<td>311</td>
</tr>
<tr>
<td>Regenerate Metadata for M-Series Appliance RAID Pairs</td>
<td>313</td>
</tr>
<tr>
<td>Replace an RMA Firewall</td>
<td>315</td>
</tr>
<tr>
<td>Partial Device State Generation for Firewalls</td>
<td>315</td>
</tr>
<tr>
<td>Before Starting RMA Firewall Replacement</td>
<td>315</td>
</tr>
<tr>
<td>Restore the Firewall Configuration after Replacement</td>
<td>316</td>
</tr>
<tr>
<td>Troubleshoot Commit Failures</td>
<td>319</td>
</tr>
<tr>
<td>Troubleshoot Registration or Serial Number Errors</td>
<td>320</td>
</tr>
<tr>
<td>Troubleshoot Reporting Errors</td>
<td>321</td>
</tr>
<tr>
<td>View Task Success or Failure Status</td>
<td>322</td>
</tr>
<tr>
<td>Downgrade from Panorama 8.0</td>
<td>323</td>
</tr>
</tbody>
</table>
Panorama Overview

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

- About Panorama
- Panorama Models
- Centralized Firewall Configuration and Update Management
- Centralized Logging and Reporting
- User-ID Redistribution Using Panorama
- Role-Based Access Control
- Panorama Commit, Validation, and Preview Operations
- Plan Your Panorama Deployment
- Deploy Panorama: Task Overview
About Panorama

Panorama enables you to effectively configure, manage, and monitor your Palo Alto Networks firewalls with central oversight. The three main areas in which Panorama adds value are:

- **Centralized configuration and deployment**—To simplify central management and rapid deployment of the firewalls and WildFire appliances on your network, use Panorama to pre-stage the firewalls and WildFire appliances 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 Firewall Configuration and Update 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**—Enables 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.

Three Panorama Models are available: the Panorama virtual appliance, M-500 appliance, and M-100 appliance. Figure 1: Panorama Centralized Management illustrates how you can deploy Panorama in a high availability (HA) configuration to manage firewalls.

![Figure 1: Panorama Centralized Management](image-url)
Panorama Models

Panorama is available as one of the following virtual or physical appliances, each of which supports licenses for managing up to 25, 100, or 1,000 firewalls:

- **Panorama virtual appliance**—This model provides simple installation and facilitates server consolidation for sites that need a virtual management appliance. You can install Panorama on a VMware ESXi server, or on VMware vCloud Air. The virtual appliance can collect firewall logs locally at rates of up to 10,000 logs per second and can manage Dedicated Log Collectors for higher logging rates. The virtual appliance can function only as a Panorama management server, not a Dedicated Log Collector. You can deploy the virtual appliance in the following modes:
  - **Panorama mode**—In this mode, the Panorama virtual appliance supports a local Log Collector with 1 to 12 virtual logging disks (see Deploy Panorama Virtual Appliances with Local Log Collectors). Each logging disk has 2TB of storage capacity for a total maximum of 24TB on a single virtual appliance and 48TB on a high availability (HA) pair. Only Panorama mode enables you to add multiple virtual logging disks without losing logs on existing disks. Panorama mode also provides the benefit of faster report generation. In Panorama mode, the virtual appliance does not support NFS storage.
  - **Legacy mode**—In this mode, the Panorama virtual appliance receives and stores firewall logs without using a local Log Collector (see Deploy Panorama Virtual Appliances in Legacy Mode with Local Log Collection). By default, the virtual appliance in Legacy mode has one disk partition for all data. Approximately 11GB of the partition is allocated to log storage. If you need more local log storage, you can add one virtual disk of up to 8TB on ESXi 5.5 and later versions or on vCloud Air. Earlier ESXi versions support one virtual disk of up to 2TB. If you need more than 8TB, you can mount the virtual appliance in Legacy mode to an NFS datastore but only on the ESXi server, not in vCloud Air.

- **M-Series appliance**—The M-100 appliance and M-500 appliance are dedicated hardware appliances intended for large-scale deployments. In environments with high logging rates (over 10,000 logs per second) and log retention requirements, these appliances enable scaling of your log collection infrastructure. Both M-Series models share the following attributes:
  - RAID drives to store firewall logs and RAID 1 mirroring to protect against disk failures
  - SSD to store the logs that Panorama and Log Collectors generate
  - MGT, Eth1, Eth2, and Eth3 interfaces that support 1Gbps throughput

  The M-500 appliance has the following additional attributes, which make it more suitable for data centers:
  - Redundant, hot-swappable power supplies
  - Front-to-back airflow
  - Eth4 and Eth5 interfaces that support 10Gbps throughput

  You can deploy the M-Series appliances in the following modes:
  - **Panorama mode**—The appliance functions as a Panorama management server to manage firewalls and Dedicated Log Collectors. The appliance also supports a local Log Collector to aggregate firewall logs. Panorama mode is the default mode. For configuration details, see Deploy Panorama M-Series Appliances with Local Log Collectors.
  - **Log Collector mode**—The appliance functions as a Dedicated Log Collector. If multiple firewalls forward large volumes of log data, a M-Series appliance in Log Collector mode provides increased scale and performance. In this mode, the appliance does not have a web interface for administrative access; it has only a command line interface (CLI). However, you can manage the appliance using the web interface of the Panorama management server. CLI access to an M-Series appliance in Log Collector mode is available only through the CLI of the Panorama management server.
Collector mode is necessary only for initial setup and debugging. For configuration details, see Deploy Panorama with Dedicated Log Collectors.

The log storage capacity and maximum log collection rate varies by model and mode, as described in Table: Panorama Log Storage and Collection Rates. For more details and specifications, see the M-100 and M-500 Hardware Reference Guides.

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

Panorama 8.0 introduced log query and reporting engine enhancements that have improved the speed when generating reports and executing queries. As a result, log ingestion rates have been affected and are lower than in previous Panorama releases.

**Table 1: Table: Panorama Log Storage and Collection Rates**

<table>
<thead>
<tr>
<th>Model Capacities and Features</th>
<th>M-500 Appliance</th>
<th>M-100 Appliance</th>
<th>Virtual Appliance in Panorama Mode</th>
<th>Virtual Appliance in Legacy Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Logging Rate for Panorama management server</td>
<td>20,000 logs/second</td>
<td>10,000 logs/second</td>
<td>10,000 logs/second</td>
<td></td>
</tr>
<tr>
<td>Maximum Logging Rate for Dedicated Log Collector</td>
<td>30,000 logs/second</td>
<td>18,000 logs/second</td>
<td>Not applicable: the Panorama virtual appliance cannot be a Dedicated Log Collector.</td>
<td></td>
</tr>
<tr>
<td>Maximum Log Storage on Appliance</td>
<td>24TB (24 2TB or 1TB RAID disks)</td>
<td>8TB (8 2TB or 1TB RAID disks)</td>
<td>24TB (12 virtual logging disks)</td>
<td>8TB (2TB for ESXi versions before v5.5)</td>
</tr>
<tr>
<td>Default Log Storage on Appliance</td>
<td>4TB (8 1TB RAID disks)</td>
<td>1TB (2 2TB RAID disks)</td>
<td>2–24TB (set during installation)</td>
<td>~11GB</td>
</tr>
<tr>
<td>SSD Storage on Appliance (for logs that M-Series appliances generate)</td>
<td>240GB</td>
<td>120GB</td>
<td>Not applicable</td>
<td></td>
</tr>
<tr>
<td>NFS Attached Log Storage</td>
<td>Not available</td>
<td>Not available</td>
<td>ESXi server only</td>
<td></td>
</tr>
</tbody>
</table>
Centralized Firewall Configuration and Update Management

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

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

Context Switch—Firewall or Panorama

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

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

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

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

Templates and Template Stacks

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

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

![Template Stacks Diagram]

**Figure 2: Template Stacks**

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

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

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

**Device Groups**

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

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

**Device Group Hierarchy**

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

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

![Figure 3: Device Group Hierarchy](image)

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 Device</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>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></td>
</tr>
<tr>
<td>Local firewall rules</td>
<td>Local rules are specific to a single firewall or virtual system (vsys).</td>
<td>A local firewall administrator, or a Panorama administrator who switches to a local firewall context, can edit local firewall rules.</td>
</tr>
<tr>
<td>Device group post-rules</td>
<td>Panorama pushes shared post-rules to all the firewalls in all device groups. Panorama pushes device group-specific post-rules to all the firewalls in a particular device group and its descendant device groups. If a firewall inherits rules from device groups at multiple levels in the device group hierarchy, it evaluates post-rules in the order of lowest to highest level. This means the firewall first evaluates the rules of device groups with no descendants and last evaluates shared rules. Post-rules typically include rules to deny access to traffic based on the App-ID™ signatures, User-ID™ information (users or user groups), or service.</td>
<td>These rules are visible on firewalls but you can only manage them in Panorama.</td>
</tr>
<tr>
<td>Shared post-rules</td>
<td>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™ signatures, User-ID™ information (users or user groups), or service.</td>
<td>These rules are visible on firewalls but you can only manage them in Panorama.</td>
</tr>
<tr>
<td>intrazone-default</td>
<td>The default rules apply only to the Security rulebase, and are predefined on Panorama (at the Shared level) and the firewall (in each vsys). These rules Default rules are initially read-only, either because they are part of the predefined configuration or because Panorama pushed them to firewalls.</td>
<td></td>
</tr>
<tr>
<td>interzone-default</td>
<td>The default rules apply only to the Security rulebase, and are predefined on Panorama (at the Shared level) and the firewall (in each vsys). These rules Default rules are initially read-only, either because they are part of the predefined configuration or because Panorama pushed them to firewalls.</td>
<td></td>
</tr>
</tbody>
</table>
Evaluation Order | Rule Scope and Description | Administration Device
---|---|---
| 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. | However, you can override the rule settings for tags, action, logging, and security profiles. The context determines the level at which you can override the rules: • Panorama—At the Shared or device group level, you can override default rules that are part of the predefined configuration. • Firewall—You can override default rules that are part of the predefined configuration on the firewall or vsys, or that Panorama pushed from the Shared location or a device group. 

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

![Rule Hierarchy](image)

**Figure 4: Rule Hierarchy**

**Device Group Objects**

Objects are configuration elements that policy rules reference, for example: IP addresses, URL categories, security profiles, users, services, and applications. Rules of any type (pre-rules, post-rules, default rules, and rules locally defined on a firewall) and any rulebase (Security, NAT, QoS, Policy Based Forwarding, Decryption, Application Override, Captive Portal, and DoS Protection) can reference objects. You can reuse an object in any number of rules that have the same scope as that object in the Device Group Hierarchy. For example, if you add an object to the Shared location, all rules in the hierarchy can reference that shared object because all device groups inherit objects from Shared. If you add an object to a particular device group, only the rules in that device group and its descendant device groups can reference that device group object. If object values in a device group must differ from those inherited from an ancestor device group, you can Override inherited object values (see Step 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 logs 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 forward them as SNMP traps, email notifications, syslog messages, and HTTP payloads to an external server.

For centralized logging and reporting, you also have the option to use the cloud-based Logging Service that is architected to work seamlessly with Panorama. The Logging Service allows your managed firewalls to forward logs to the Logging Service infrastructure instead of to Panorama or to the managed Log Collectors, so you can augment your existing distributed log collection setup or to scale your current logging infrastructure without having to invest time and effort yourself.

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 the Logging Service, 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, or on the Logging Service.

If you don’t Configure Log Forwarding to Panorama or the Logging Service, 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 reports don’t provide a granular drill-down on specific information and activities, they still provide a unified monitoring approach.

• Managed Collectors and Collector Groups
• Local and Distributed Log Collection
• Caveats for a Collector Group with Multiple Log Collectors
• Log Forwarding Options
• Centralized Reporting

Managed Collectors and Collector Groups

Panorama uses Log Collectors to aggregate logs from managed firewalls. When generating reports, Panorama queries the Log Collectors for log information, providing you visibility into all the network activity that your firewalls monitor. Because you use Panorama to configure and manage Log Collectors, they are also known as managed collectors. Panorama can manage two types of Log Collectors:

• **Local Log Collector**—This type of Log Collector runs locally on the Panorama management server. Only an M-500 appliance, M-100 appliance, or Panorama virtual appliance in Panorama mode supports a local Log Collector.

  If you forward logs to a Panorama virtual appliance in Legacy mode, it stores the logs locally without a Log Collector.

• **Dedicated Log Collector**—This is an M-500 or M-100 appliance in Log Collector mode. You can use an M-Series appliance in Panorama mode or a Panorama virtual appliance in Panorama or Legacy mode to manage Dedicated Log Collectors. To use the Panorama web interface for managing Dedicated Log Collectors, you must add them as managed collectors. Otherwise, administrative access to a Dedicated Log Collector is only available through its CLI using the predefined administrative user (admin) account. Dedicated Log Collectors don’t support additional administrative user accounts.

You can use either or both types of Log Collectors to achieve the best logging solution for your environment (see Local and Distributed Log Collection).
A Collector Group is 1 to 16 managed collectors that operate as a single logical log collection unit. If the Collector Group contains Dedicated Log Collectors, Panorama uniformly distributes the logs across all the disks in each Log Collector and across all Log Collectors in the group. This distribution optimizes the available storage space. To enable a Log Collector to receive logs, you must add it to a Collector Group. You can enable log redundancy by assigning multiple Log Collectors to a Collector Group (see Caveats for a Collector Group with Multiple Log Collectors). The Collector Group configuration specifies which managed firewalls can send logs to the Log Collectors in the group.

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

Local and Distributed Log Collection

Before you Configure Log Forwarding to Panorama, you must decide whether to use local Log Collectors, Dedicated Log Collectors, or both.

A local Log Collector is easy to deploy because it requires no additional hardware or virtual machine instance. In a high availability (HA) configuration, you can send logs to the local Log Collector on both Panorama peers; the passive Panorama doesn't wait for failover to start collecting logs.

For local log collection, you can also forward logs to a Panorama virtual appliance in Legacy mode, which stores the logs without using a Log Collector as a logical container.

Dedicated Log Collectors are M-500 or M-100 appliances in Log Collector mode. Because they perform only log collection, not firewall management, Dedicated Log Collectors allow for a more robust environment than local Log Collectors. Dedicated Log Collectors provide the following benefits:

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

Distributed Log Collection illustrates a topology in which the Panorama peers in an HA configuration manage the deployment and configuration of firewalls and Dedicated Log Collectors.

You can deploy the Panorama management server in an HA configuration but not the Dedicated Log Collectors.
Caveats for a Collector Group with Multiple Log Collectors

You can **Configure a Collector Group** with multiple Log Collectors (up to 16) to ensure log redundancy, increase the log retention period, and accommodate logging rates that exceed the capacity of a single Log Collector (see Panorama Models for capacity information). In any single Collector Group, all the Log Collectors must run on the same Panorama model: all M-500 appliances, all M-100 appliances, or all Panorama virtual appliances. For example, if a single managed firewall generates 48TB of logs, the Collector Group that receives those logs will require at least six Log Collectors that are M-100 appliances or two Log Collectors that are M-500 appliances or Panorama virtual appliances.

A Collector Group with multiple Log Collectors uses the available storage space as one logical unit and uniformly distributes the logs across all its Log Collectors. The log distribution is based on the disk capacity of the Log Collectors (see Panorama Models) 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 in 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 so long as that primary Log Collector is available. However, based on the hash algorithm, Panorama might choose L2 as the owner that writes the logs to its disks. If L2 becomes inaccessible or has a chassis failure, FW1 will not know because it can still connect to L1.
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 firewall model). As soon as connectivity is restored to the Log Collector, the firewall resumes forwarding logs where it left off before the failure occurred.

In the case of a Collector Group with multiple Log Collectors, the firewall does not buffer logs to its local storage if only one Log Collector is down. In the example scenario where L2 is down, FW1 continues sending logs to L1, and L1 stores the log data that would be sent to L2. Once L2 is back up, L1 no longer stores log data intended for L2 and distribution resumes as expected. If one of the Log Collectors in a Collector Group goes down, there is no risk of losing logs should because the logs that would be written to the down Log Collector are redistributed to the next Log Collector in the preference list.

Palo Alto Networks recommends the following mitigations if using multiple Log Collectors in a Collector Group:

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

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

  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.

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

• In addition to forwarding logs to Panorama, configure forwarding to an external service as backup storage. The external service can be a syslog server, email server, SNMP trap server, or HTTP server.
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 use external services for archiving, notification, or analysis by forwarding logs to the services directly from the firewalls or from Panorama. External services include syslog servers, email servers, SNMP trap servers, or HTTP-based services. In addition to forwarding firewall logs, you can forward the logs that the Panorama management server and Log Collectors generate. The Panorama management server, Log Collector, or firewall that forwards the logs converts them to a format that is appropriate for the destination (syslog message, email notification, SNMP trap, or HTTP payload).

Palo Alto Networks firewalls and Panorama support the following log forwarding options. Before choosing an option, consider the logging capacities of your Panorama Models and Determine Panorama Log Storage Requirements.

- 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.

- 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.
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. 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.
User-ID Redistribution Using Panorama

One of the key benefits of the Palo Alto Networks firewall is that it can enforce policies and generate reports based on usernames instead of IP addresses. The challenge for large-scale networks is ensuring every firewall that enforces policies and generates reports has the IP address-to-username mappings for your entire user base. Additionally, every firewall that enforces Authentication Policy requires a complete, identical set of authentication timestamps for your user base. Whenever users authenticate to access services and applications, individual firewalls record the associated timestamps but don’t automatically share them with other firewalls to ensure consistency. User-ID™ solves these challenges for large-scale networks by enabling you to redistribute information (user mappings and timestamps). However, instead of setting up extra connections to redistribute the User-ID information between firewalls, you can leverage your Panorama and distributed log collection infrastructure to Redistribute User-ID Information to Managed Firewalls. The infrastructure has existing connections that enable you to redistribute User-ID information in layers, from firewalls to Log Collectors to Panorama. Panorama can then redistribute the information to the firewalls that enforce policies and generate reports for all your users.

Each firewall, Log Collector, or Panorama management server can receive User-ID information from up to 100 redistribution points. The redistribution points can be Windows-based User-ID agents or other firewalls, Log Collectors, and Panorama management servers. Panorama and Log Collectors as User-ID Redistribution Points illustrates a redistribution sequence where the firewalls perform user mapping by directly monitoring information sources such as directory servers and syslog senders. However, you can also use Windows-based User-ID agents to perform the mapping and redistribute the information to firewalls. Only the firewalls record authentication timestamps when user traffic matches Authentication policy rules.

You can redistribute user mappings collected through any method except Terminal Services (TS) agents. You cannot redistribute username-to-group mapping or HIP match information.

Figure 10: Panorama and Log Collectors as User-ID Redistribution Points
Role-Based Access Control

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

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

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

Administrative Roles

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

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

<table>
<thead>
<tr>
<th>Dynamic Role</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Superuser</td>
<td>Full read-write access to Panorama</td>
</tr>
<tr>
<td>Superuser (read-only)</td>
<td>Read-only access to Panorama</td>
</tr>
<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 firewall administrators and roles.</td>
</tr>
<tr>
<td></td>
<td>- Export, validate, revert, save, load, or import a configuration in the Device &gt; Setup &gt; Operations page.</td>
</tr>
</tbody>
</table>

© 2019 Palo Alto Networks, Inc.
• **Admin Role Profiles**—To provide more granular access control over the functional areas of the web interface, CLI, and XML API, you can create custom roles. When new features are added to the product, you must update the roles with corresponding access privileges: Panorama does not automatically add new features to custom role definitions. You select one of the following profile types when you **Configure an Admin Role Profile**.

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

## Authentication Profiles and Sequences

An authentication profile defines the authentication service that validates the login credentials of administrators when they access Panorama. The service can be local authentication or an external authentication service. Some services (SAML, TACACS+, and RADIUS) provide the option to manage both authentication and authorization for administrative accounts on the external server instead of on Panorama. In addition to the authentication service, the authentication profile defines options such as Kerberos single sign-on (SSO) and SAML single logout (SSO).

Some networks have multiple databases (such as TACACS+ and LDAP) for different users and user groups. To authenticate administrators in such cases, **configure an authentication sequence**—a ranked order of authentication profiles that Panorama matches an administrator against during login. Panorama checks
against each profile in sequence until one successfully authenticates the administrator. An administrator is denied access only if authentication fails for all the profiles in the sequence.

Access Domains

Access domains control administrative access to specific Device Groups and templates, and also control the ability to switchcontext to the web interface of managed firewalls. Access domains apply only to administrators with Device Group and Template roles. Mapping Administrative Roles to access domains enables very granular control over the information that administrators access on Panorama. For example, consider a scenario where you configure an access domain that includes all the device groups for firewalls in your data centers and you assign that access domain to an administrator who is allowed to monitor data center traffic but who is not allowed to configure the firewalls. In this case, you would map the access domain to a role that enables all monitoring privileges but disables access to device group settings.

You configure access domains in the local Panorama configuration and then assign them to administrative accounts and roles. You can perform the assignment locally or use an external SAML, TACACS+, or RADIUS server. Using an external server enables you to quickly reassign access domains through your directory service instead of reconfiguring settings on Panorama. To use an external server, you must define a server profile that enables Panorama to access the server. You must also define Vendor-Specific Attributes (VSAs) on the RADIUS or TACACS+ server, or SAML attributes on the SAML IdP server.

For example, if you use a RADIUS server, you would define a VSA number and value for each administrator. The value defined has to match the access domain configured on Panorama. When an administrator tries to log in to Panorama, Panorama queries the RADIUS server for the administrator access domain and attribute number. Based on the response from the RADIUS server, the administrator is authorized for access and is restricted to the firewalls, virtual systems, device groups, and templates that are assigned to the access domain.

For the relevant procedures, see:
- Configure an Access Domain.
- Configure RADIUS Authentication for Panorama Administrators.
- Configure TACACS+ Authentication for Panorama Administrators.
- Configure SAML Authentication for Panorama Administrators.

Administrative Authentication

You can configure the following types of authentication and authorization (Administrative Roles and Access Domains) for Panorama administrators:

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Authorization Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>Local</td>
<td>The administrative account credentials and authentication mechanisms are local to Panorama. You use Panorama to assign administrative roles and access domains to the accounts. To further secure the accounts, you can create a password profile that defines a validity period for passwords and set Panorama-wide password complexity settings. For details, see Configure Local or External Authentication for Panorama Administrators.</td>
</tr>
<tr>
<td>SSH Keys</td>
<td>Local</td>
<td>The administrative accounts are local to Panorama, but authentication to the CLI is based on SSH keys. You use Panorama to assign administrative roles and access domains to the accounts. For details, see</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Authorization Method</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Certificates</strong></td>
<td>Local</td>
<td>The administrative accounts are local to Panorama, but authentication to the web interface is based on client certificates. You use Panorama to assign administrative roles and access domains to the accounts. For details, see Configure a Panorama Administrator with Certificate-Based Authentication for the Web Interface.</td>
</tr>
<tr>
<td><strong>External service</strong></td>
<td>Local</td>
<td>The administrative accounts you define locally on Panorama serve as references to the accounts defined on an external Multi-Factor Authentication, SAML, Kerberos, TACACS+, RADIUS, or LDAP server. The external server performs authentication. You use Panorama to assign administrative roles and access domains to the accounts. For details, see Configure Local or External Authentication for Panorama Administrators.</td>
</tr>
</tbody>
</table>
| **External service**  | External service     | The administrative accounts are defined only on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. Panorama maps the attributes to administrator roles and access domains that you define on Panorama. For details, see:  
  • Configure SAML Authentication for Panorama Administrators  
  • Configure TACACS+ Authentication for Panorama Administrators  
  • Configure RADIUS Authentication for Panorama Administrators |
Panorama Commit, Validation, and Preview Operations

When you are ready to activate changes that you made to the candidate configuration on Panorama or to push changes to the devices that Panorama manages (firewalls, Log Collectors, and WildFire appliances and appliance clusters), you can Preview, Validate, or Commit Configuration Changes. For example, if you add a Log Collector to the Panorama configuration, firewalls cannot send logs to that Log Collector until you commit the change to Panorama and then push the change to the Collector Group that contains the Log Collector.

You can filter changes by administrator or location and then commit, push, validate, or preview only those changes. The location can be specific device groups, templates, Collector Groups, Log Collectors, shared settings, or the Panorama management server.

When you commit changes, they become part of the running configuration. Changes that you haven’t committed are part of the candidate configuration. Panorama queues commit requests so that you can initiate a new commit while a previous commit is in progress. Panorama performs the commits in the order they are initiated but prioritizes auto-commits that are initiated by Panorama (such as FQDN refreshes). However, if the queue already has the maximum number of administrator-initiated commits (10), you must wait for Panorama to finish processing a pending commit before initiating a new one. You can Use the Panorama Task Manager to cancel pending commits or to see details about commits that are pending, in progress, completed, or failed. To check which changes a commit will activate, you can run a commit preview.

When you initiate a commit, Panorama checks the validity of the changes before activating them. The validation output displays conditions that block the commit (errors) or that are important to know (warnings). For example, validation could indicate an invalid route destination that you need to fix for the commit to succeed. The validation process enables you to find and fix errors before you commit (it makes no changes to the running configuration). This is useful if you have a fixed commit window and want to be sure the commit will succeed without errors.

For details on candidate and running configurations, see Manage Panorama and Firewall Configuration Backups.

To prevent multiple administrators from making configuration changes during concurrent sessions, see Manage Locks for Restricting Configuration Changes.

When pushing configurations to managed devices, Panorama pushes the running configuration. Because of this, Panorama does not let you push changes to managed devices until you first commit the changes to Panorama.
Plan Your Panorama Deployment

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

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

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

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

☐ Determine your authentication method between Panorama and its managed devices and high availability peer. By default, Panorama uses predefined certificates to authenticate the SSL connections used for management and inter-device communication. However, you can configure custom certificate-based authentication to enhance the security of the SSL connections between Panorama, firewalls, and log collectors. By using custom certificates, you can establish a unique chain of trust to ensure mutual authentication between Panorama and the devices it manages. You can import the certificates from your enterprise public key infrastructure (PKI) or generate it on Panorama.

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

☐ Plan how to accommodate network segmentation and security requirements in a large-scale deployment. By default, Panorama running on an M-500 or M-100 appliance uses the management (MGT) interface for administrative access to Panorama and for managing devices (firewalls, Log Collectors, and WildFire appliances and appliance clusters), collecting logs, communicating with Collector Groups, and deploying software and content updates to devices. However, to improve security and enable network segmentation, you can reserve the MGT interface for administrative access and use dedicated M-Series Appliance Interfaces (Eth1, Eth2, Eth3, Eth4, and Eth5) for the other services.

☐ For meaningful reports on network activity, plan a logging solution:

- Estimate the log storage capacity your network needs to meet security and compliance requirements. Consider such factors as the logging capacities of your Panorama Models, network topology, number of firewalls sending logs, type of log traffic (for example, URL Filtering and Threat logs versus Traffic logs), the rate at which firewalls generate logs, and the number of days for which you want to store logs on Panorama. For details, see Determine Panorama Log Storage Requirements.
- Do you need to forward logs to external services (such as a syslog server) in addition to Panorama? See Log Forwarding Options.
- If you need a long-term storage solution, do you have a Security Information and Event Management (SIEM) solution, such as Splunk or ArcSight, to which you can forward logs?
- Do you need redundancy in logging?
If you configure a Collector Group with multiple Log Collectors, you can enable redundancy to ensure that no logs are lost if any one Log Collector becomes unavailable (see Caveats for a Collector Group with Multiple Log Collectors).

If you deploy Panorama virtual appliances in Legacy mode in an HA configuration, the managed firewalls can send logs to both HA peers so that a copy of each log resides on each peer. This redundancy option is enabled by default (see Modify Log Forwarding and Buffering Defaults).

- Will you log to a Network File System (NFS)? If the Panorama virtual appliance is in Legacy mode and does not manage Dedicated Log Collectors, NFS storage is the only option for increasing log storage capacity beyond 8TB. NFS storage is available only if Panorama runs on an ESXi server. If you use NFS storage, keep in mind that the firewalls can send logs only to the primary peer in the HA pair; only the primary peer is mounted to the NFS and can write to it.

- Determine which role-based access privileges administrators require to access managed firewalls and Panorama. See Set Up Administrative Access to Panorama.

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

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

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

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

**STEP 1** | **(M-Series appliance only)** Rack mount the appliance.

**STEP 2** | Perform initial configuration to enable network access to Panorama. See Set Up the Panorama Virtual Appliance or Set Up the M-Series Appliance.

**STEP 3** | Register Panorama and Install Licenses.

**STEP 4** | Install Content and Software Updates for Panorama.

**STEP 5** | **(Recommended)** Set up Panorama in a high availability configuration. See Panorama High Availability.

**STEP 6** | Add a Firewall as a Managed Device.

**STEP 7** | Add a Device Group or Create a Device Group Hierarchy, Add a Template, and (if applicable) Configure a Template Stack.

**STEP 8** | **(Optional)** Configure log forwarding to Panorama and/or to external services. See Manage Log Collection.

**STEP 9** | Monitor Network Activity using the visibility and reporting tools on Panorama.
For centralized reporting and cohesive policy management across all the firewalls on your network, you can deploy the Panorama™ management server as a virtual appliance or as a hardware appliance (the M-100 or M-500 appliance).

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

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

When you Plan Your Panorama Deployment, estimate how much log storage capacity Panorama requires to determine which Panorama Models to deploy, whether to expand the storage on those appliances beyond their default capacities, whether to deploy Dedicated Log Collectors, and whether to Configure Log Forwarding from Panorama to External Destinations. When log storage reaches the maximum capacity, Panorama automatically deletes older logs to create space for new ones.

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

STEP 1 | Determine the log retention requirements of your organization.

Factors that affect log retention requirements include:

- IT policy of your organization
- Log redundancy—If you enable log redundancy when you Configure a Collector Group, each log will have two copies, which doubles your required log storage capacity.
- Regulatory requirements, such as those specified by the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act, and Health Insurance Portability and Accountability Act (HIPAA).

If your organization requires the removal of logs after a certain period, you can set the expiration period for each log type. You can also set a storage quota for each log type as a percentage of the total space if you need to prioritize log retention by type. For details, see Manage Storage Quotas and Expiration Periods for Logs and Reports.

STEP 2 | Determine the average daily logging rates.

Do this multiple times each day at peak and non-peak times to estimate the average. The more often you sample the rates, the more accurate your estimate.

1. Display the current log generation rate in logs per second:

   - If Panorama is not yet collecting logs, access the CLI of each firewall, run the following command, and calculate the total rates for all the firewalls. This command displays the number of logs received in the last second.

     ```
     > debug log-receiver statistics
     ```

   - If Panorama is already collecting logs, run the following command at the CLI of each appliance that receives logs (Panorama management server or Dedicated Log Collector) and calculate the total rates. This command gives the average logging rate for the last five minutes.

     ```
     > debug log-collector log-collection-stats show incoming-logs
     ```

   You can also use an SNMP manager to determine the logging rates of Log Collectors (see the panLogCollector MIB, OID 1.3.6.1.4.1.25461.1.1.6) and firewalls (see the panDeviceLogging, OID 1.3.6.1.4.1.25461.2.1.2.7).

2. Calculate the average of the sampled rates.

3. Calculate the daily logging rate by multiplying the average logs-per-second by 86,400.
STEP 3 | Estimate the required storage capacity.

This formula provides only an estimate; the exact amount of required storage will differ from the formula result.

Use the formula:

\(<\text{required_storage_duration}> \times \text{<average_log_size> \times <average_logging_rate>}\)

The average log size varies considerably by log type. However, you can use 500 bytes as an approximate average log size.

For example, if Panorama must store logs for 30 days and the average total logging rate for all firewalls is 21,254,400 logs per day, then the required log storage capacity is: 30 \times 500 \times 21,254,400 = 318,816,000,000 bytes (approximately 318GB).

STEP 4 | Next steps...

If you determine that Panorama requires more log storage capacity:

- Expand Log Storage Capacity on the Panorama Virtual Appliance.
- Increase Storage on the M-Series Appliance.
Set Up the Panorama Virtual Appliance

The Panorama virtual appliance enables you to use your existing VMware virtual infrastructure to centrally manage and monitor Palo Alto Networks firewalls and Dedicated Log Collectors. You can install the virtual appliance on an ESXi server or in vCloud Air. In addition to or instead of deploying Dedicated Log Collectors, you can forward firewall logs directly to the Panorama virtual appliance. For greater log storage capacity and faster reporting, you have the option to switch the virtual appliance from Legacy mode to Panorama mode and configure a local Log Collector. For more details about the Panorama virtual appliance and its modes, see Panorama Models.

You can’t use the Panorama virtual appliance as a Dedicated Log Collector. You must Set Up the M-Series Appliance in Log Collector mode to have dedicated log collection capabilities.

These topics assume you are familiar with the VMware products required to create the virtual appliance and don’t cover VMware concepts or terminology.

- Setup Prerequisites for the Panorama Virtual Appliance
- Install the Panorama Virtual Appliance
- Perform Initial Configuration of the Panorama Virtual Appliance
- Set Up the Panorama Virtual Appliance with Local Log Collector
- Expand Log Storage Capacity on the Panorama Virtual Appliance
- Increase CPUs and Memory on the Panorama Virtual Appliance
- Complete the Panorama Virtual Appliance Setup

Setup Prerequisites for the Panorama Virtual Appliance

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

- Use your browser to access the Palo Alto Networks Customer Support web site and Register Panorama. You will need the Panorama serial number that you received in the order fulfillment email. After registering Panorama, you can access the Panorama software downloads page.
- Review the supported Panorama hypervisors to verify the hypervisor meets the minimum version requirements to deploy Panorama.
- If you will install Panorama on a VMware ESXi server, verify that the server meets the minimum requirements as listed in System Requirements for Panorama Virtual Appliance on an ESXi Server. These requirements apply to Panorama 5.1 and later releases. The requirements vary based on whether you will run the virtual appliance in Panorama mode or Legacy mode. For details on the modes, see Panorama Models.

If you install Panorama on VMware vCloud Air, you set the system settings during installation.

Table 2: System Requirements for Panorama Virtual Appliance on an ESXi Server

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Panorama Virtual Appliance in Panorama Mode</th>
<th>Panorama Virtual Appliance in Legacy Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual hardware version</td>
<td>64-bit kernel-based VMware ESXi 5.1, 5.5, 6.0 or 6.5. The supported version of the virtual hardware family type (also known as the VMware virtual hardware version) on the ESXi server is vmx-09.</td>
<td></td>
</tr>
</tbody>
</table>
### Requirements

<table>
<thead>
<tr>
<th>Panorama Virtual Appliance in Panorama Mode</th>
<th>Panorama Virtual Appliance in Legacy Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>In Panorama mode, the virtual appliance running on any ESXi version supports up to 12 virtual logging disks with 2TB of log storage each, for a total maximum capacity of 24TB.</td>
<td>In Legacy mode, the virtual appliance supports one virtual logging disk. ESXi 5.5 and later versions supports one disk of up to 8TB. Earlier ESXi versions support one disk of up to 2TB.</td>
</tr>
</tbody>
</table>

#### Client computer

To install the Panorama virtual appliance and manage its resources, you must install a VMware vSphere Client or VMware Infrastructure Client that is compatible with your ESXi server.

#### System disk

- **81GB**
  - For log storage, Panorama uses virtual logging disks instead of the system disk or an NFS datastore.
- **52GB**
  - Panorama allocates approximately 11GB on the system disk for log storage. However, you can mount an NFS datastore or add a virtual logging disk to **Expand Log Storage Capacity on the Panorama Virtual Appliance**.

#### CPUs and memory

- **2TB storage** — 8 CPUs and 16GB memory
- **4TB storage** — 8 CPUs and 32GB memory
- **6 to 8TB storage** — 12 CPUs and 32GB memory
- **10 to 16TB storage** — 12 CPUs and 64GB memory
- **18 to 24TB storage** — 16 CPUs and 64GB memory

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

#### Log storage capacity

- **2TB to 24TB**
- **11GB (default log storage on the system disk to 8TB (if you add a virtual logging disk)**

*If you are using the Logging Service, you do not need to allocate a*
Requirements | Panorama Virtual Appliance in Panorama Mode | Panorama Virtual Appliance in Legacy Mode
--- | --- | ---
logging disk. All you need is the system disk for Panorama.

Install the Panorama Virtual Appliance

Before installation, decide whether to run the virtual appliance in Panorama mode or Legacy mode. Each mode has different resource requirements, as described in Setup Prerequisites for the Panorama Virtual Appliance. You must complete the prerequisites before starting the installation.

As a best practice, install the virtual appliance in Panorama mode to optimize log storage and report generation. For details on Panorama and Legacy mode, see Panorama Models.

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

Install Panorama on an ESXi Server

Use these instructions to install a new Panorama virtual appliance on a VMware ESXi server. For upgrades to an existing Panorama virtual appliance, skip to Install Content and Software Updates for Panorama.

STEP 1 | Download the Panorama 8.0.2 base image Open Virtual Appliance (OVA) file.
1. Go to the Palo Alto Networks software downloads site. (If you can’t log in, go to the Palo Alto Networks Customer Support web site for assistance.)
2. In the Download column in the Panorama Base Images section, download the Panorama 8.0.2 release OVA file (Panorama-ESX-8.0.2.ova).

STEP 2 | Install Panorama.
1. Launch the VMware vSphere Client and connect to the VMware server.
2. Select File > Deploy OVF Template.
3. Browse to select the Panorama OVA file and click Next.
4. Confirm that the product name and description match the downloaded version, and click Next.
5. Enter a descriptive name for the Panorama virtual appliance, and click Next.
6. Select a datastore location (system disk) on which to install the Panorama image. The system disk must have exactly 81GB storage for the virtual appliance in Panorama mode and 52GB for the virtual appliance in Legacy mode. After selecting the datastore, click Next.
7. Select Thick Provision Lazy Zeroed as the disk format, and click Next.
8. Specify which networks in the inventory to use for the Panorama virtual appliance, and click Next.
9. Confirm the selected options, click Finish to start the installation process, and click Close when it finishes. Do not power on the Panorama virtual appliance yet.

STEP 3 | Configure resources on the Panorama virtual appliance.

1. Right-click the Panorama virtual appliance and Edit Settings.
2. In the Hardware settings, allocate the CPUs and memory as necessary.

   The virtual appliance boots up in Panorama mode if you allocate sufficient CPUs and Memory and add a virtual logging disk (later in this procedure). Otherwise, the appliance boots up in Legacy mode. For details on the modes, see Panorama Models.

3. Set the SCSI Controller to LSI Logic Parallel.
4. Add a virtual logging disk.

   In Panorama mode, this step is required because the virtual appliance can store logs only on a dedicated logging disk.

   In Legacy mode, the appliance uses approximately 11GB on the system disk for logging by default, so adding a dedicated logging disk to increase storage capacity is optional.

1. Add a disk, select Hard Disk as the hardware type, and click Next.
2. Create a new virtual disk and click Next.
3. Set the Disk Size to exactly 2TB if the virtual appliance is in Panorama mode or up to 8TB if the appliance is in Legacy mode.

   In Panorama mode, you can later add additional logging disks (for a total of 12) with 2TB of storage each. Expanding the size of a logging disk that is already added to Panorama is not supported.

   In Legacy mode, the appliance uses approximately 11GB on the system disk for logging by default, so adding a dedicated logging disk to increase storage capacity is optional.

4. Select your preferred Disk Provisioning disk format.

   Consider your business needs when selecting the disk provisioning format. For more information regarding the disk provisioning performance considerations, refer to the VMware Thick vs Thin Disks and All Flash Arrays document, or additional VMware documentation.

   When adding multiple logging disks, it is a best practice to select the same Disk Provisioning format for all disks to avoid any unexpected performance issues that may arise.

5. Select Specify a datastore or datastore structure as the location, Browse to a datastore that has sufficient storage, click OK, and click Next.
6. Select a SCSI Virtual Device Node (you can use the default selection) and click Next.

   Panorama will fail to boot if you select a format other than SCSI.

7. Verify that the settings are correct and click Finish.
8. Click OK to save your changes.

STEP 4 | Power on the Panorama virtual appliance.

1. In the vSphere Client, right-click the Panorama virtual appliance and select Power > Power On. Wait for Panorama to boot up before continuing.
2. Verify that the virtual appliance is running in the correct mode:

   1. Right-click the Panorama virtual appliance and select Open Console.
2. Enter your username and password to log in (default is admin for both).
3. Display the mode by running the following command:

   ```
   > show system info
   ```

   In the output, the system-mode indicates either panorama or legacy mode.

You are now ready to Perform Initial Configuration of the Panorama Virtual Appliance.

**Install Panorama on vCloud Air**

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

**STEP 1 | Download the Panorama 8.0.2 base image Open Virtual Appliance (OVA) file.**

1. Go to the Palo Alto Networks software downloads site. (If you can't log in, go to the Palo Alto Networks Customer Support web site for assistance.)
2. In the Download column in the Panorama Base Images section, download the Panorama 8.0.2 release OVA file (Panorama-ESX-8.0.2.ova).

**STEP 2 | Import the Panorama image to the vCloud Air catalog.**

For details on these steps, refer to the OVF Tool User's Guide.

1. Install the OVF Tool on your client system.
2. Access the client system CLI.
3. Navigate to the OVF Tool directory (for example, C:\Program Files\VMware\VMware OVF Tool).
4. Convert the OVA file to an OVF package:

   ```
   ovftool.exe <OVA#file#pathname> <OVF#file#pathname>
   ```

5. Use a browser to access the vCloud Air web console, select your Virtual Private Cloud OnDemand location, and record the browser URL. You will use the URL information to complete the next step. The URL format is: https://<virtual#cloud#location>.vchs.vmware.com/compute/cloud/org/<vCloud#account#number>/#/catalogVAppTemplateList?catalog=<catalog#ID>.
6. Import the OVF package, using the information from the vCloud Air URL to complete the <virtual#cloud#location>, <vCloud#account#number>, and <catalog#ID> variables. The other variables are your vCloud Air username and domain <user>@<domain>, a virtual data center <datacenter>, and a vCloud Air template <template>.

   ```
   ovftool.exe -st="OVF" "<OVF#file#pathname>"
   "vcloud://<user>@<domain>:password@<virtual-cloud-location>.vchs.vmware.com?vdc=<datacenter>&org=<vCloud-account-number>&vappTemplate=<template>.ovf&catalog=default-catalog"
   ```

**STEP 3 | Install Panorama.**

1. Access the vCloud Air web console and select your Virtual Private Cloud OnDemand region.
2. Create a Panorama virtual machine. For the steps, refer to Add a Virtual Machine from a Template in the vCloud Air Documentation Center. Configure the CPU, Memory and Storage as follows:
   - Set the CPU and Memory based on whether the virtual appliance will be in Panorama mode or Legacy mode: see CPUs and memory.
• Set the **Storage** to exactly 81GB for the virtual appliance in Panorama mode and 52GB for the virtual appliance in Legacy mode. For better logging and reporting performance, select the **SSD-Accelerated** option.

The Panorama virtual appliance in Legacy mode uses approximately 11GB for log storage. To increase the log storage capacity, you must **Add a Virtual Disk to Panorama on vCloud Air**. In Panorama mode, the virtual appliance does not use the system disk for log storage; you must add a virtual logging disk.

**STEP 4 |** Create vCloud Air NAT rules on the gateway to allow inbound and outbound traffic for the Panorama virtual appliance.

Refer to **Add a NAT Rule** in the vCloud Air Documentation Center for the detailed instructions:

1. Add a NAT rule that allows Panorama to receive traffic from the firewalls and allows administrators to access Panorama.
2. Add a NAT rule that allows Panorama to retrieve updates from the Palo Alto Networks update server and to access the firewalls.

**STEP 5 |** Create a vCloud Air firewall rule to allow inbound traffic on the Panorama virtual appliance.

Outbound traffic is allowed by default.

Refer to **Add a Firewall Rule** in the vCloud Air Documentation Center for the detailed instructions.

**STEP 6 |** Power on the Panorama virtual appliance if it isn’t already on.

In the vCloud Air web console, select the **Virtual Machines** tab, select the Panorama virtual machine, and click **Power On**.

You are now ready to **Perform Initial Configuration of the Panorama Virtual Appliance**.

---

**Support for VMware Tools on the Panorama Virtual Appliance**

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

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

---

**Perform Initial Configuration of the Panorama Virtual Appliance**

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

**STEP 1 |** Gather the required information from your network administrator.
Collect the following information for the management (MGT) interface:

- IP address for the management (MGT) interface
- Netmask
- Default gateway
- DNS server IP address

To complete the configuration of the MGT interface, you must specify the IP address, netmask (for IPv4) or prefix length (for IPv6), and default gateway. If you omit settings (such as the default gateway), you can access Panorama only through the console port for future configuration changes. As a best practice, always commit a complete MGT interface configuration.

STEP 2 | Access the console of the Panorama virtual appliance.

1. Access the console.
   
   On an ESXi server:
   1. Launch the VMware vSphere Client.
   2. Select the Console tab for the Panorama virtual appliance and press enter to access the login screen.

   On vCloud Air:
   1. Access the vCloud Air web console and select your Virtual Private Cloud OnDemand region.
   2. Select the Virtual Machines tab, right-click the Panorama virtual machine, and select Open In Console.

2. Enter your username and password to log in (default is admin for both).

STEP 3 | Configure the network access settings for the MGT interface.

Panorama uses the MGT interface for management traffic, high availability synchronization, log collection, and communication within Collector Groups.

1. Enter the following commands, 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:

```
> configure
# set deviceconfig system ip-address <Panorama-IP> netmask <netmask> default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
# commit
# exit
```

2. Use the ping utility to verify network access to external services required for firewall management, such as the default gateway, DNS server, and the Palo Alto Networks Update Server, as shown in the following example:

```
admin@Panorama-Corp> ping host updates.paloaltonetworks.com
PING updates.paloaltonetworks.com (67.192.236.252) 56(84) bytes of data.
64 bytes from 67.192.236.252: icmp_seq=1 ttl=243 time=40.5 ms
64 bytes from 67.192.236.252: icmp_seq=1 ttl=243 time=53.6 ms
64 bytes from 67.192.236.252: icmp_seq=1 ttl=243 time=79.5 ms
```

After verifying connectivity, press Ctrl+C to stop the pings.

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

STEP 5 | Change the default administrator password.

To ensure that the management interface remains secure, configure the Minimum Password Complexity (Panorama > Setup > Management).

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

STEP 6 | (Optional) Modify the management interface settings.

1. Select Panorama > Setup > Interfaces and click Management.
2. Select which Network Connectivity Services to allow on the interface (such as SSH access).
   Don't select Telnet or HTTP. These services use plaintext and are less secure than the other services.
3. Click OK to save your changes to the interface.

STEP 7 | Commit your configuration changes.

Select Commit > Commit to Panorama and Commit your changes.

STEP 8 | Next steps...

1. If necessary, Expand Log Storage Capacity on the Panorama Virtual Appliance.
2. (Best Practice) Replace the default certificate that Panorama uses to secure HTTPS traffic over the management (MGT) interface.
3. Activate a Panorama Support License
4. Activate/Retrieve a Firewall Management License on the Panorama Virtual Appliance
5. Install Content and Software Updates for Panorama.

Set Up the Panorama Virtual Appliance with Local Log Collector

After you upgrade from a Panorama 7.1 or earlier release to a Panorama 8.0 (or later) release, the Panorama virtual appliance is in Legacy mode by default and is limited to 8TB of local log storage. By switching to
Panorama mode, you can create a local Log Collector, add multiple logging disks without losing existing logs, increase log storage to up to 24TB, and enable faster report generation.

The Panorama virtual appliance cannot function as a Dedicated Log Collector but can manage Dedicated Log Collectors.

The virtual appliance supports NFS log storage only in Legacy mode, not in Panorama mode. After switching to Panorama mode, you must migrate the logs that are in the NFS storage to the virtual disks on the local Log Collector.

For a new Panorama installation, you can ensure the virtual appliance starts in Panorama mode automatically by specifying sufficient resources when you Install the Panorama Virtual Appliance.

After upgrading to Panorama 8.0, the first step is to increase the system resources on the virtual appliance to the minimum required for Panorama mode. Panorama reboots when you increase resources, so perform this procedure during a maintenance window. You must install a larger system disk (81GB), increase CPUs and memory based on the log storage capacity, and add a virtual logging disk. The new logging disk must have at least as much capacity as the appliance currently uses in Legacy mode and cannot be less than 2TB. Adding a virtual disk enables you to migrate existing logs to the Log Collector and enables the Log Collector to store new logs.

If Panorama is deployed in an HA configuration, perform the following steps on the secondary peer first and then on the primary peer.

STEP 1 | Determine which system resources you need to increase before the virtual appliance can operate in Panorama mode.

You must run the command specified in this step even if you have determined that Panorama already has adequate resources.

1. Access the Panorama CLI:
   1. Use terminal emulation software such as PuTTY to open an SSH session to the IP address that you specified for the Panorama MGT interface.
   2. Log in to the CLI when prompted.
2. Check the resources you must increase by running the following command:

   ```
   > request system system-mode panorama
   ```

   Enter y when prompted to continue. The output specifies the resources you must increase. For example:

   ```
   Panorama mode not supported on current system disk of size 52.0 GB.
   Please attach a disk of size 81.0 GB, then use 'request system clone-system-disk' to migrate the current system disk
   Please add a new virtual logging disk with more than 50.00 GB of storage capacity.
   Not enough CPU cores: Found 4 cores, need 8 cores
   ```

STEP 2 | Increase the CPUs and memory, and replace the system disk with a larger disk.

1. Access the VMware ESXi vSphere Client, select Virtual Machines, right-click the Panorama virtual appliance, and select Power > Power Off.
2. Right-click the Panorama virtual appliance and Edit Settings.
3. Select Memory and enter the new Memory Size.
4. Select CPUs and specify the number of CPUs (the Number of virtual sockets multiplied by the Number of cores per socket).
5. Add a virtual disk.
   You will use this disk to replace the existing system disk.
   1. In the Hardware settings, Add a disk, select Hard Disk as the hardware type, and click Next.
   2. Create a new virtual disk and click Next.
   3. Set the Disk Size to exactly 81GB and select the Thick Provision Lazy Zeroed disk format.
   4. Select Specify a datastore or datastore structure as the location, Browse to a datastore of at least 81GB, click OK, and click Next.
   5. Select a SCSI Virtual Device Node (you can use the default selection) and click Next.

   Panorama will fail to boot if you select a format other than SCSI.

6. Verify that the settings are correct and then click Finish and OK.
6. Right-click the Panorama virtual appliance and select Power > Power On. Wait for Panorama to reboot before continuing.
7. Return to the Panorama CLI and copy the data from the original system disk to the new system disk:

   > request system clone-system-disk target sdb

   Enter y when prompted to continue.

   The copying process takes around 20 to 25 minutes, during which Panorama reboots. When the process finishes, the output tells you to shut down Panorama.
8. Return to the vSphere Client console, right-click the Panorama virtual appliance, and select Power > Power Off.
9. Right-click the Panorama virtual appliance and Edit Settings.
10. Select the original system disk, click Remove, select Remove from virtual machine, and click OK.
11. Right-click the Panorama virtual appliance and Edit Settings.
12. Select the new system disk, set the Virtual Device Node to SCSI (0:0), and click OK.
13. Right-click the Panorama virtual appliance and select Power > Power On. Before proceeding, wait for Panorama to reboot on the new system disk (around 15 minutes).

STEP 3 | Add a virtual logging disk.

This is the disk to which you will migrate existing logs.

1. In the VMware ESXi vSphere Client, right-click the Panorama virtual appliance and select Power > Power Off.
2. Right-click the Panorama virtual appliance and Edit Settings.
3. Repeat the steps to Add a virtual disk. Set the Disk Size to a multiple of 2TB based on the amount of log storage you need. The capacity must be at least as large as the existing virtual disk or NFS storage that Panorama currently uses for logs. The disk capacity must be a multiple of 2TB and can be up to 24TB. For example, if the existing disk has 5TB of log storage, you must add a new disk of at least 6TB.

   After you switch to Panorama mode, Panorama will automatically divide the new disk into 2TB partitions, each of which will function as a separate virtual disk.
4. Right-click the Panorama virtual appliance and select Power > Power On. Wait for Panorama to reboot before continuing.

STEP 4 | Switch from Legacy mode to Panorama mode.
After switching the mode, the appliance reboots again and then automatically creates a local Log Collector and Collector Group. The existing logs won't be available for querying or reporting until you migrate them later in this procedure.

1. Return to the Panorama CLI and run the following command.

   ```plaintext
   > request system system-mode panorama
   ```

   Enter y when prompted to continue. After rebooting, Panorama automatically creates a local Log Collector (named Panorama) and creates a Collector Group (named default) to contain it. Panorama also configures the virtual logging disk you added and divides it into separate 2TB disks. Wait for the process to finish and for Panorama to reboot (around five minutes) before continuing.

2. Log in to the Panorama web interface.

3. In the Dashboard, General Information settings, verify that the Mode is now panorama.

   In an HA deployment, the secondary peer is in a suspended state at this point because its mode (Panorama) does not match the mode on the primary peer (Legacy). You will un-suspend the secondary peer after switching the primary peer to Panorama mode later in this procedure.

4. Select Panorama > Collector Groups to verify that the default collector group has been created, and that the local Log Collector is part of the default collector group.

5. Push the configuration to the managed devices.

   - If there are no pending changes:
     1. Select Commit > Push to Devices and Edit Selections.
     2. Select Collector Group and make sure the default collector group is selected.
     3. Click OK and Push.
   - If you have pending changes:
     1. Select Commit > Commit and Push and Edit Selections.
     2. Verify that your Device Group devices and Templates are included.
     3. Select Collector Group and make sure the default collector group is selected.
     4. Click OK and Commit and Push.

6. Select Panorama > Managed Collectors and verify that the columns display the following information for the local Log Collector:
   - Collector Name—This defaults to the Panorama hostname. It should be listed under the default Collector Group.
   - Connected—Check mark
   - Configuration Status—In sync
   - Run Time Status—connected

**STEP 5 | (HA only)** Switch the primary Panorama from Legacy mode to Panorama mode.

This step triggers failover.

1. Repeat steps 1 through 4 on the primary Panorama.

   Wait for the primary Panorama to reboot and return to an active HA state. If preemption is not enabled, you must manually fail back: select Panorama > High Availability and, in the Operational Commands section, Make local Panorama functional.

2. On the primary Panorama, select Dashboard and, in the High Availability section, Sync to peer, click Yes, and wait for the Running Config to display Synchronized status.

This step is necessary to bring the secondary Panorama out of its suspended HA state.

STEP 6 | Migrate existing logs to the new virtual logging disks.

If you deployed Panorama in an HA configuration, perform this only on the primary peer.

1. Return to the Panorama CLI.
2. Start the log migration:

   ```bash
   > request logdb migrate vm start
   ```

   The process duration varies by the volume of log data you are migrating. To check the status of the migration, run the following command:

   ```bash
   > request logdb migrate vm status
   ```

   When the migration finishes, the output displays: migration has been done.
3. Verify that the existing logs are available.

   1. Log in to the Panorama web interface.
   2. Select Panorama > Monitor, select a log type that you know matches some existing logs (for example, Panorama > Monitor > System), and verify that the logs display.

STEP 7 | Next steps...

Configure log forwarding to Panorama so that the Log Collector receives new logs from firewalls.

Expand Log Storage Capacity on the Panorama Virtual Appliance

After you Perform Initial Configuration of the Panorama Virtual Appliance, the available log storage capacity and the options for expanding it depend on the virtual platform (VMware ESXi server or vCloud Air) and mode (Legacy or Panorama mode): see Panorama Models for details.

To expand the log storage capacity on the Panorama virtual appliance, you must add additional logging disks. Expanding the log storage capacity of an existing logging disk is not supported, and Panorama does not recognize the additional storage capacity. For example, if you added a 2TB logging disk, and then expanded that existing logging disk to 4TB, Panorama continues to recognize the logging disk as having 2TB of storage capacity and ignores the additional 2TB of storage capacity.

For additional log storage, you can also forward firewall logs to Dedicated Log Collectors (see Configure a Managed Collector) or Configure Log Forwarding from Panorama to External Destinations.

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

- Preserve Existing Logs When Adding Storage on Panorama Virtual Appliance in Legacy Mode
- Add a Virtual Disk to Panorama on an ESXi Server
- Add a Virtual Disk to Panorama on vCloud Air
- Mount the Panorama ESXi Server to an NFS Datastore
Preserve Existing Logs When Adding Storage on Panorama Virtual Appliance in Legacy Mode

The Panorama virtual appliance in Legacy mode can use only one virtual disk for logging. Therefore, if you add a virtual disk that is dedicated for logging, Panorama stops using the default 11GB log storage on the system disk and automatically copies any existing logs to the new logging disk. (Panorama continues using the system disk for data other than logs.)

If you replace an existing dedicated logging disk of up to 2TB storage capacity with a disk of up to 8TB, you will lose the logs on the existing disk. To preserve the logs, your choices are:

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

Contact Palo Alto Networks Customer Support for instructions.

Add a Virtual Disk to Panorama on an ESXi Server

To expand log storage capacity on the Panorama virtual appliance, you can add virtual logging disks. If the appliance is in Panorama mode, you can add 1 to 12 virtual logging disks of 2TB each, for a maximum total of 24TB. If the appliance is in Legacy mode, you can add one virtual logging disk of up to 8TB on ESXi 5.5 and later versions or one disk of up to 2TB on earlier ESXi versions. Additionally, it is recommended to add logging disks with the same disk provisioning format to avoid any unexpected performance that may arise from having multiple disk with different provisioning formats.

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

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

If necessary, you can Replace the Virtual Disk on an ESXi Server.

STEP 1 | Add additional disks to Panorama

In all modes, the first logging disk on the Panorama VM must be at least 2TB in order to add additional disks. If the first logging disk is smaller than 2TB, you will be unable to add additional disk space.

1. Access the VMware vSphere Client and select Virtual Machines.
2. Right-click the Panorama virtual appliance and select Power > Power off.
3. Right-click the Panorama virtual appliance and select Edit Settings.
4. Click **Add** in the **Hardware** tab to launch the Add Hardware wizard.
5. Select **Hard Disk** as the hardware type and click **Next**.
6. **Create a new virtual disk** and click **Next**.
7. Set the **Disk Size**. If the Panorama virtual appliance is in Panorama mode, set the size to at least 2TB. If the appliance is in Legacy mode, you can set the size to as much as 8TB.
   
   *In Panorama mode, you can add disk sizes larger than 2TB and Panorama will automatically create as many 2TB partitions as possible. For example, if disk sdc was 24TB, it will create 12 2TB partitions. These disks will be named sdc1-12.*
8. Select the **Disk Provisioning** format and click **Next**.
9. Specify a datastore or datastore structure. **Browse** to a datastore with enough space for the specified **Disk Size**, click **OK**, and click **Next**.
10. Select a **SCSI Virtual Device Node** (you can use the default selection) and click **Next**.
   
   *The selected node must be in SCSI format; Panorama will fail to boot if you select another format.*
11. Verify that the settings are correct and then click **Finish** and **OK**.

   The new disk appears in the list of devices for the virtual appliance.
12. Repeat Step 4 through Step 11 to add additional disks to the Panorama virtual appliance if necessary.
13. Right click the Panorama virtual appliance and select **Power > Power On**. The virtual disk initializes for first-time use. The size of the new disk determines how long initialization takes.

### STEP 2 | Configure each disk.

The following example uses the sdc virtual disk.

1. Log in to the Panorama CLI.
2. Enter the following command to view the disks on the Panorama virtual appliance:
   
   ```
   show system disk details
   ```

   The user will see the following response:

   ```
   Name : sdb
   State : Present
   Size : 2048 MB
   Status : Available
   Reason : Admin enabled
   Name : sdc
   State : Present
   Size : 2048 MB
   Status : Available
   Reason : Admin disabled
   ```
3. Enter the following command and confirm the request when prompted for all disks with the **Reason : Admin disabled** response:
   
   ```
   request system disk add sdc
   ```
4. Enter the **show system disk details** command to monitor the status of the disk addition. Continue to Step 3 when all newly added disk responses display **Reason : Admin enabled**.

### STEP 3 | Make disks available for logging.

1. Log in to the Panorama web interface.
2. Select **Panorama > Managed Collectors** and edit the Log Collector.
3. Select **Disks** and Add each newly added disk.
4. Click **OK**.
5. Select **Commit > Commit and Push** and **Commit and Push** your changes.

**STEP 4 |** Configure Panorama to receive logs.

This step is intended for new Panorama deployments in Panorama mode. If you are adding logging disks to an existing Panorama virtual appliance, continue to Step 5.

1. Configure a Managed Collector.
2. Configure a Collector Group.
3. Configure Log Forwarding to Panorama.

**STEP 5 |** Verify that the Panorama Log Storage capacity has been increased.

1. Log in to the Panorama web interface.
2. Select **Panorama > Collector Groups** and select the Collector Group that the Panorama virtual appliance belongs to.
3. Verify that the **Log Storage** capacity accurately displays the disk capacity.

Add a Virtual Disk to Panorama on vCloud Air

To expand log storage capacity on the Panorama virtual appliance, you can add virtual logging disks. If the appliance is in Panorama mode, you can add 1 to 12 virtual logging disks of 2TB each, for a maximum total of 24TB. If the appliance is in Legacy mode, you can add one virtual logging disk of up to 8TB.

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

*If necessary, you can Replace the Virtual Disk on vCloud Air.*

**STEP 1 |** Add additional disks to Panorama.

*In all modes, the first logging disk on the Panorama VM must be at least 2TB in order to add additional disks. If the first logging disk is less than 2TB, you will be unable to add additional disk space.*

1. Access the vCloud Air web console and select your **Virtual Private Cloud On Demand** region.
2. Select the Panorama virtual appliance in the **Virtual Machines** tab.
3. Select **Actions > Edit Resources** and **Add another disk**.
4. Set the **Storage** size. If the Panorama virtual appliance is in Panorama mode, set the size to at least 2TB. If the appliance is in Legacy mode, you can set the size to as much as 8TB.

*In Panorama mode, you can add disk sizes larger than 2TB and Panorama will automatically create as many 2TB partitions as possible. For example, if disk sdc was 24TB, it will create 12 2TB partitions. These disks will be named sdc1-12.*

5. Set the storage tier to **Standard** or **SSD-Accelerated**.
6. Repeat Step c and Step d to add additional disks to the Panorama virtual appliance if necessary.
7. Save your changes.

**STEP 2 |** Configure each disk.

The following example uses the sdc virtual disk.

1. Log in to the Panorama CLI.
2. Enter the following command to view the disks on the Panorama virtual appliance:

   ```
   show system disk details
   ```
The user will see the following response:

<table>
<thead>
<tr>
<th>Name</th>
<th>sdb</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Present</td>
</tr>
<tr>
<td>Size</td>
<td>2048 MB</td>
</tr>
<tr>
<td>Status</td>
<td>Available</td>
</tr>
<tr>
<td>Reason</td>
<td>Admin enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>sdc</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Present</td>
</tr>
<tr>
<td>Size</td>
<td>2048 MB</td>
</tr>
<tr>
<td>Status</td>
<td>Available</td>
</tr>
<tr>
<td>Reason</td>
<td>Admin disabled</td>
</tr>
</tbody>
</table>

3. Enter the following command and confirm the request when prompted for all disks with the reason: ```Admin disabled``` response:

   ```bash
   request system disk add sdc
   ```

4. Enter the `show system disk details` command to monitor the status of the disk addition. Continue to next step when all newly added disk responses display ```Admin enabled```.

**STEP 3** | Make disks available for logging.

1. Log in to the Panorama web interface.
2. Select Panorama > Managed Collectors and edit the Log Collector.
3. Select Disks and Add each newly added disk.
4. Click OK.
5. Select Commit > Commit and Push and Commit and Push your changes.

**STEP 4** | Configure Panorama to receive logs.

This step is intended for new Panorama deployments in Panorama mode. If you are adding logging disks to an existing virtual Panorama appliance, continue to the next step.

1. Configure a Managed Collector.
2. Configure a Collector Group.
3. Configure Log Forwarding to Panorama.

**STEP 5** | Verify that the Panorama Log Storage capacity has been increased.

1. Log in to the Panorama web interface.
2. Select Panorama > Collector Groups and select the Collector Group that the virtual Panorama appliance belongs to.
3. Verify that the Log Storage capacity accurately displays the disk capacity.

*Mount the Panorama ESXi Server to an NFS Datastore*

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

*The Panorama virtual appliance in Panorama mode does not support NFS.*

**STEP 1** | Select Panorama > Setup > Operations and, in the Miscellaneous section, click Storage Partition Setup.
STEP 2 | Set the **Storage Partition** type to **NFS V3**.

STEP 3 | Enter the IP address of the **NFS Server**.

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

STEP 5 | For the **Protocol**, select **TCP** or **UDP**, and enter the **Port** for accessing the NFS server.

To use NFS over TCP, the NFS server must support it. Common NFS ports are UDP/TCP 111 for RPC and UDP/TCP 2049 for NFS.

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

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

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

STEP 9 | Click **OK** to save your changes.

STEP 10 | Select **Commit > Commit to Panorama** and **Commit** your changes. Until you reboot, the Panorama virtual appliance writes logs to the local storage disk.

STEP 11 | Select **Panorama > Setup > Operations** and select **Reboot Panorama** in the Device Operations section. After rebooting, Panorama starts writing logs to the NFS datastore.

### Increase CPUs and Memory on the Panorama Virtual Appliance

When you **Perform Initial Configuration of the Panorama Virtual Appliance**, you specify the memory and number of CPUs based on whether the appliance is in Panorama mode or Legacy mode and based on the log storage capacity or number of managed firewalls. If you later add storage capacity or managed firewalls, you must also increase the memory and CPUs.

<table>
<thead>
<tr>
<th>Panorama Virtual Appliance in Panorama Mode</th>
<th>Panorama Virtual Appliance in Legacy Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the memory and the number of CPUs based on the log storage capacity of Panorama:</td>
<td>Set the memory and the number of CPUs based on the number of firewalls that Panorama will manage:</td>
</tr>
<tr>
<td>• 2TB storage — 8 CPUs and 16GB memory</td>
<td>• 1 to 10 firewalls — 4 CPUs and 4GB memory</td>
</tr>
<tr>
<td>• 4TB storage — 8 CPUs and 32GB memory</td>
<td>• 11 to 50 firewalls — 8 CPUs and 8GB memory</td>
</tr>
<tr>
<td>• 6 to 8TB storage — 12 CPUs and 32GB memory</td>
<td>• 51 to 1,000 firewalls — 8 CPUs and 16GB memory</td>
</tr>
<tr>
<td>• 10 to 16TB storage — 12 CPUs and 64GB memory</td>
<td></td>
</tr>
<tr>
<td>• 18 to 24TB storage — 16 CPUs and 64GB memory</td>
<td></td>
</tr>
</tbody>
</table>
• Increase CPUs and Memory for Panorama on an ESXi Server
• Increase CPUs and Memory for Panorama on vCloud Air

Increase CPUs and Memory for Panorama on an ESXi Server
For the minimum CPUs and memory that Panorama requires, see Increase CPUs and Memory on the Panorama Virtual Appliance.

STEP 1 | Access the VMware vSphere Client and select Virtual Machines.
STEP 2 | Right-click the Panorama virtual appliance and select Power > Power Off.
STEP 3 | Right-click the Panorama virtual appliance and select Edit Settings.
STEP 4 | Select Memory and enter the new Memory Size.
STEP 5 | Select CPUs and specify the number of CPUs (the Number of virtual sockets multiplied by the Number of cores per socket).
STEP 6 | Click OK to save your changes.
STEP 7 | Right-click the Panorama virtual appliance and select Power > Power On.

Increase CPUs and Memory for Panorama on vCloud Air
For the minimum CPUs and memory that Panorama requires, see Increase CPUs and Memory on the Panorama Virtual Appliance.

STEP 1 | Access the vCloud Air web console and select your Virtual Private Cloud OnDemand region.
STEP 2 | In the Virtual Machines tab, select the Panorama virtual machine and Power Off.
STEP 3 | Select Actions > Edit Resources.
STEP 4 | Set the CPU and Memory.
STEP 5 | Save your changes.
STEP 6 | Select the Panorama virtual machine and Power On.

Complete the Panorama Virtual Appliance Setup
After you Perform Initial Configuration of the Panorama Virtual Appliance, continue with the following tasks for additional configuration:
• Activate a Panorama Support License
• Activate/Retrieve a Firewall Management License on the Panorama Virtual Appliance
• Install Content and Software Updates for Panorama
• Access and Navigate Panorama Management Interfaces
• Set Up Administrative Access to Panorama
• Manage Firewalls
Set Up the M-Series Appliance

The M-500 and M-100 appliances are high performance hardware appliances that you can deploy in Panorama mode (as Panorama management servers) or in Log Collector mode (as Dedicated Log Collectors). The appliances provide multiple interfaces that you can assign to various Panorama services such as firewall management and log collection. Before setting up the appliance, consider how you can configure the interfaces to optimize security, enable network segmentation (in large-scale deployments), and load balance the traffic for Panorama services.

- M-Series Appliance Interfaces
- M-Series Setup Overview
- Perform Initial Configuration of the M-Series Appliance
- Set Up the M-Series Appliance as a Log Collector
- Increase Storage on the M-Series Appliance
- Configure Panorama to Use Multiple Interfaces

M-Series Appliance Interfaces

The Panorama M-500 and M-100 appliances have several interfaces for communicating with other systems such as managed firewalls and the client systems of Panorama administrators. Panorama communicates with these systems to perform various services, including managing devices (firewalls, Log Collectors, and WildFire appliances and appliance clusters), collecting logs, communicating with Collector Groups, deploying software and content updates to devices, and providing administrative access to Panorama. By default, Panorama uses its management (MGT) interface for all these services. However, you can improve security by reserving the MGT interface for administrative access and dedicating separate interfaces for the other services. In a large-scale network with multiple subnetworks and heavy log traffic, using multiple interfaces for device management and log collection also enables network segmentation and load balancing (see Configure Panorama to Use Multiple Interfaces).

When assigning Panorama services to various interfaces, keep in mind that only the MGT interface allows administrative access to Panorama for configuration and monitoring tasks. You can assign any interface to the other services when you Perform Initial Configuration of the M-Series Appliance. The M-100 and M-500 Appliance Hardware Reference Guides explain where to attach cables for the interfaces. The M-100 appliance support 1Gbps throughput on all its interfaces: MGT, Eth1, Eth2, and Eth3. In addition to these interfaces, the M-500 appliance supports 10Gbps throughput on its Eth4 and Eth5 interfaces.

The M-Series appliances do not support Link Aggregation Control Protocol (LACP) for aggregating interfaces.

M-Series Setup Overview

Use the following procedures to set up an M-Series appliance:

- Set Up an M-Series Appliance in Panorama Mode
- Set Up an M-Series Appliance in Log Collector Mode

Set Up an M-Series Appliance in Panorama Mode

STEP 1 | Rack mount the M-Series appliance. Refer to the M-100 or M-500 Appliance Hardware Reference Guide for instructions.

STEP 2 | Perform Initial Configuration of the M-Series Appliance
Perform Initial Configuration of the M-Series Appliance

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

STEP 1 | Gather the required interface and server information from your network administrator.

- Gather the IP address, netmask (for IPv4) or prefix length (for IPv6), and default gateway for each interface that you plan to configure (MGT, Eth1, Eth2, Eth3, Eth4, Eth5). Only the MGT interface is mandatory.

Palo Alto Networks recommends that you specify all these settings for the MGT interface. If you omit values for some of these settings (such as the default gateway), you can access Panorama only through the console port for future configuration changes. You cannot commit the configurations for other interfaces unless you specify all these settings.

If you plan to use the appliance as a Panorama management server, Palo Alto Networks recommends using the MGT interface only for managing Panorama and using other interfaces for managing devices, collecting logs, communicating with Collector Groups, and deploying updates to devices (see M-Series Appliance Interfaces).
• Gather the IP addresses of the DNS servers.

**STEP 2 |** Access the M-Series appliance from your computer.

1. Connect to the M-Series appliance in one of the following ways:
   • Attach a serial cable from a computer to the Console port on the M-Series appliance and connect using terminal emulation software (9600-8-N-1).
   • Attach an RJ-45 Ethernet cable from a computer to the MGT port on the M-Series appliance. From a browser, go to https://192.168.1.1. Enabling access to this URL might require changing the IP address on the computer to an address in the 192.168.1.0 network (for example, 192.168.1.2).

2. When prompted, log in to the appliance using the default username and password (admin/admin). The appliance starts initializing.

**STEP 3 |** Configure the network access settings for each interface that you will use to manage Panorama, manage devices, collect logs, communicate with Collector Groups, and deploy updates to devices.

1. Select **Panorama > Setup > Interfaces** and click the Interface Name.

2. **(Non-MGT interfaces only)** Enable the interface.

3. Edit the network access settings of each interface that Panorama will use. Only the MGT interface is required. The Eth1, Eth2, Eth3, Eth4, and Eth5 interfaces are optional and apply only if you plan to use the M-Series appliance as a Panorama management server.

1. Complete one or both of the following field sets based on the IP protocols of your network:
   - **IPv4**—IP Address, Netmask, and Default Gateway
   - **IPv6**—IPv6 Address/Prefix Length and Default IPv6 Gateway

2. Select the Device Management Services that the interface supports:
   - **Device Management and Device Log Collection**—You can assign one or more interfaces.
   - **Collector Group Communication**—You can assign only one interface.
   - **Device Deployment** (software and content updates)—You can assign only one interface.

3. **(Optional)** Select the Network Connectivity Services that the interface supports.

   - **(MGT interface only)** Disable Telnet and HTTP; these services use plaintext and so are less secure than other services.

4. Click **OK** to save your changes.

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

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

2. Align the clock on Panorama and the managed firewalls to use the same **Time Zone**, for example GMT or UTC. If you plan to use the Logging service, you must configure NTP so that Panorama can stay in sync with the Logging Service.

   The firewall records timestamps when it generate logs and Panorama records timestamps upon receiving the logs. Aligning the time zones ensures that the timestamps are synchronized and that the process of querying logs and generating reports on Panorama is harmonious.

3. Enter a **Hostname** for the server. Panorama uses this as the display name/label for the appliance. For example, this is the name that appears at the CLI prompt. It also appears in the Collector Name field if you add the appliance as a managed collector on the **Panorama > Managed Collectors** page.

4. **(Optional)** Enter the **Latitude** and **Longitude** to enable accurate placement of the M-Series appliance on the world map. The **App Scope > Traffic Maps** and **App Scope > Threat Maps** use these values.

5. Click **OK** to save your entries.
Configure the DNS servers and Palo Alto Networks Update Server.

1. Select Panorama > Setup > Services and edit the settings.
2. Enter the IP address of the Primary DNS Server and (optionally) of the Secondary DNS Server.
3. Enter the URL or static address of the Update Server (default updates.paloaltonetworks.com).

   Select Verify Update Server Identity if you want Panorama to verify that the Update Server from which it downloads software or content packages has an SSL certificate that a trusted authority signed. This option adds an additional level of security for communication between the Panorama management server and Update Server.

4. Click OK to save your entries.

Change the default admin password.

1. Click the admin link in the lower left of the web interface.
2. Enter the Old Password, New Password, and Confirm New Password, and then click OK. Store the new password in a safe location.

   To ensure that the MGT interface remains secure, configure Minimum Password Complexity settings (select Panorama > Setup > Management) and specify the interval at which administrators must change their passwords.

Commit your configuration changes.

Select Commit > Commit to Panorama and Commit your changes.

If you plan to use the M-Series appliance as a Panorama management server and you configured interfaces other than MGT, you must assign those interfaces to the Device Log Collection or Collector Group Communication functions when you Configure a Managed Collector. To make the interfaces operational, you must then Configure a Collector Group for the managed collector and perform a Collector Group commit.

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

1. Connect to the M-Series appliance in one of the following ways:
   - Attach a serial cable from your computer to the Console port on the M-Series appliance. Then use a terminal emulation software (9600-8-N-1) to connect.
   - Use terminal emulation software such as PuTTY to open an SSH session to the IP address that you specified for the MGT interface of the M-Series appliance during initial configuration.
2. Log in to the CLI when prompted. Use the default admin account and the password that you specified during initial configuration.
3. Use the ping utility to verify network connectivity to the Palo Alto Networks Update Server as shown in the following example. Verify that DNS resolution occurs and the response includes the IP address for the Update Server (10.101.16.13, in this example); the Update Server does not respond to a ping request.

   \[ > \text{ping host updates.paloaltonetworks.com} \]
   PING updates.paloaltonetworks.com (10.101.16.13) 56(84) bytes of data.

   After verifying DNS resolution, press Ctrl+C to stop the ping request.
4. Use the following CLI command to retrieve information on the support entitlement for Panorama from the Update Server:
If you have connectivity, the Update Server responds with the support status for Panorama. Because Panorama is not registered, the Update Server returns the following message:

Contact Us
https://www.paloaltonetworks.com/company/contact-us.html
Support Home
https://www.paloaltonetworks.com/support/tabs/overview.html
Device not found on this update server

STEP 9 | Next steps...
1. Register Panorama and Install Licenses.
2. Install Content and Software Updates for Panorama.

As a best practice, replace the default certificate that Panorama uses to secure HTTPS traffic over the MGT interface.

Set Up the M-Series Appliance as a Log Collector

If you want a dedicated appliance for log collection, configure an M-100 or M-500 appliance in Log Collector mode. To do this, you first perform the initial configuration of the appliance in Panorama mode, which includes licensing, installing software and content updates, and configuring the management (MGT) interface. You then switch the M-100 or M-500 appliance to Log Collector mode and complete the Log Collector configuration. Additionally, if you want to use dedicated M-Series Appliance Interfaces (recommended) instead of the MGT interface for log collection and Collector Group communication, you must first configure the interfaces for the Panorama management server, then configure them for the Log Collector, and then perform a Panorama commit followed by a Collector Group commit.

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

Switching the M-Series appliance from Panorama mode to Log Collector mode reboots the appliance, deletes the local Log Collector, deletes any existing log data, and deletes all configurations except the management access settings. Switching the mode does not delete licenses, software updates, or content updates.

STEP 1 | Set up the Panorama management server that will manage the Log Collector if you have not already done so.
Perform one of the following tasks:
• Set Up the Panorama Virtual Appliance
• Set Up the M-Series Appliance

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

STEP 3 | Set up the M-Series appliance that will serve as a Dedicated Log Collector.

If you previously deployed this appliance as a Panorama management server, you can skip this step because the MGT interface is already configured and the licenses and updates are already installed.

The M-Series appliance in Log Collector mode does not have a web interface for configuration tasks, only a CLI. Therefore, before changing the mode on the M-Series appliance, use the web interface in Panorama mode to:

1. Perform Initial Configuration of the M-Series Appliance.
2. Register Panorama and Install Licenses.
3. Install Content and Software Updates for Panorama.

STEP 4 | Access the CLI of the M-Series appliance.

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

STEP 5 | Switch from Panorama mode to Log Collector mode.

1. Switch to Log Collector mode by entering the following command:

   ```
   > request system system-mode logger
   ```

2. Enter y to confirm the mode change. The M-Series appliance reboots. If the reboot process terminates your terminal emulation software session, reconnect to the M-Series appliance to see the Panorama login prompt.

   If you see a CMS Login prompt, this means the Log Collector has not finished rebooting. Press Enter at the prompt without typing a username or password.

3. Log back in to the CLI.
4. Verify that the switch to Log Collector mode succeeded:

   ```
   > show system info | match system-mode
   ```

   If the mode change succeeded, the output displays:

   ```
   system-mode: logger
   ```

STEP 6 | Configure the logging disks as RAID1 pairs.

If you previously deployed the appliance as a Panorama management server, you can skip this step because the disk pairs are already configured and available.

The time required to configure the drives varies from several minutes to a couple of hours, based on the amount of data on the drives.
1. Determine which disk pairs are present for configuring as RAID pairs on the M-Series appliance:

   > show system raid detail

   Perform the remaining steps to configure each disk pair that has present disks. This example uses disk pair A1/A2.

2. To add the first disk in the pair, enter the following command and enter \textit{y} when prompted to confirm the request:

   > request system raid add A1

   Wait for the process to finish before adding the next disk in the pair. To monitor the progress of the RAID configuration, re-enter:

   > show system raid detail

   After the process finishes for the first disk, the output displays the disk pair status as \textit{Available but degraded}.

3. Add the second disk in the pair:

   > request system raid add A2

4. Verify that the disk setup is complete:

   > show system raid detail

   After the process finishes for the second disk, the output displays the disk pair status as \textit{Available and clean}:

<table>
<thead>
<tr>
<th>Disk Pair</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Available clean</td>
</tr>
</tbody>
</table>

**STEP 7 |** Enable connectivity between the Log Collector and Panorama management server.

Enter the following commands at the Log Collector CLI, where <IPaddress1> is for the MGT interface of the solitary (non-HA) or active (HA) Panorama and <IPaddress2> is for the MGT interface of the passive (HA) Panorama, if applicable.

   > configure
   # set deviceconfig system panorama-server <IPaddress1> panorama-server-2 <IPaddress2>
   # commit
   # exit

**STEP 8 |** Record the serial number of the Log Collector.

You need the serial number to add the Log Collector as a managed collector on the Panorama management server.

1. At the Log Collector CLI, enter the following command to display its serial number.
2. Record the serial number.

STEP 9 | Add the Log Collector as a managed collector to the Panorama management server.

1. Select Panorama > Managed Collectors and Add a managed collector.
2. In the General settings, enter the serial number (Collector S/N) you recorded for the Log Collector.
3. In the Panorama Server IP field, enter the IP address or FQDN of the solitary (non-HA) or active (HA) Panorama. For HA deployments, enter the IP address or FQDN of the passive Panorama peer in the Panorama Server IP 2 field.

These IP addresses must specify a Panorama interface that has Device Management and Device Log Collection services enabled. By default, these services are enabled only on the MGT interface. However, you might have enabled the services on other interfaces when you Set Up the M-Series Appliance that is a Panorama management server.

4. Select Interfaces, click Management, and configure one or both of the following field sets for the MGT interface based on the IP protocols of your network.
   - IPv4—IP Address, Netmask, and Default Gateway
   - IPv6—I Pv6 Address/Prefix Length and Default IPv6 Gateway

5. Click OK twice to save your changes to the Log Collector.
6. Select Commit > Commit to Panorama and Commit your changes to the Panorama configuration.
   This step is required before you can enable logging disks.
7. Verify that Panorama > Managed Collectors lists the Log Collector you added. The Connected column displays a check mark to indicate that the Log Collector is connected to Panorama. You might have to wait a few minutes before the page displays the updated connection status.

   At this point, the Configuration Status column displays Out of Sync and the Run Time Status column displays disconnected. The status will change to In Sync and connected after you configure a Collector Group (Step Assign the Log Collector to a Collector Group).

STEP 10 | Enable the logging disks.

1. Select Panorama > Managed Collectors and edit the Log Collector.
2. Select Disks and Add each RAID disk pair.
3. Click OK to save your changes.
4. Select Commit > Commit to Panorama and Commit your changes to the Panorama configuration.

STEP 11 | (Recommended) Configure the Ethernet1, Ethernet2, Ethernet3, Ethernet4, and Ethernet5 interfaces if the Panorama management server and Log Collector will use them for Device Log Collection (receiving logs from firewalls) and Collector Group Communication.

If you previously deployed the Log Collector as a Panorama management server and configured these interfaces, you must reconfigure them because switching to Log Collector mode (Switch from Panorama mode to Log Collector mode.) would have deleted all configurations except the management access settings.

1. Configure each interface on the Panorama management server (other than the MGT interface) if you haven’t already:
   1. Select Panorama > Setup > Interfaces and click the Interface Name.
   2. Select <interface-name> to enable the interface.
   3. Complete one or both of the following field sets based on the IP protocols of your network:

© 2019 Palo Alto Networks, Inc.
IPv4—IP Address, Netmask, and Default Gateway
IPv6—IPv6 Address/Prefix Length and Default IPv6 Gateway

4. Select the Device Management Services that the interface supports:

   Device Management and Device Log Collection—You can assign one or more interfaces.
   Collector Group Communication—You can assign only one interface.
   Device Deployment (software and content updates)—You can assign only one interface.

5. Click OK to save your changes.

2. Configure each interface on the Log Collector (other than the MGT interface):

   1. Select Panorama > Managed Collectors and edit the Log Collector.
   2. Select Interfaces and click the name of the interface.
   3. Select <interface-name> to enable the interface.

   4. Complete one or both of the following field sets based on the IP protocols of your network:
      IPv4—IP Address, Netmask, and Default Gateway
      IPv6—IPv6 Address/Prefix Length and Default IPv6 Gateway

5. Select the Device Management Services that the interface supports:

   Device Log Collection—You can assign one or more interfaces.
   Collector Group Communication—You can assign only one interface.

6. Click OK to save your changes to the interface.

3. Click OK to save your changes to the Log Collector.

4. Select Commit > Commit to Panorama and Commit your changes to the Panorama configuration.

---

STEP 12 | (Optional) If your deployment is using custom certificates for authentication between Panorama and managed devices, deploy the custom client device certificate. For more information, see Set Up Authentication Using Custom Certificates.

1. Select Panorama > Certificate Management > Certificate Profile and choose the certificate profile from the drop-down or click New Certificate Profile to create one.
2. Select Panorama > Managed Collectors > Add > Communication for a Log Collector.
3. Select the Secure Client Communication check box.
4. Select the type of device certificate the Type drop-down.
   - If you are using a local device certificate, select the Certificate and Certificate Profile from the respective drop-downs.
   - If you are using SCEP as the device certificate, select the SCEP Profile and Certificate Profile from the respective drop-downs.
5. Click OK.

STEP 13 | (Optional) Configure Secure Server Communication on a Log Collector. For more information, see Set Up Authentication Using Custom Certificates.

1. Select Panorama > Managed Collectors > Add > Communication.
2. Verify that the Custom Certificate Only check box is not selected. This allows you to continue managing all devices while migrating to custom certificates.
3. Select the SSL/TLS service profile from the SSL/TLS Service Profile drop-down. This SSL/TLS service profile applies to all SSL connections between the Log Collector and devices sending it logs.
4. Select the certificate profile from the Certificate Profile drop-down.
5. Select **Authorize Client Based on Serial Number** to have the server check clients against the serial numbers of managed devices. The client certificate must have the special keyword $UDID set as the CN to authorize based on serial numbers.

6. In **Disconnect Wait Time (min)**, enter the number of minutes Panorama should wait before breaking and reestablishing the connection with its managed devices. This field is blank by default and the range is 0 to 44,640 minutes.

   *The disconnect wait time does not begin counting down until you commit the new configuration.*

7. **(Optional)** Configure an authorization list.
   1. Click **Add** under Authorization List.
   2. Select the **Subject** or **Subject Alt Name** as the Identifier type.
   3. Enter an identifier of the selected type.
   4. Click **OK**.
   5. Select **Check Authorization List** to enforce the authorization list.

8. Click **OK**.

9. Select **Commit > Commit to Panorama**.

**STEP 14 | Assign the Log Collector to a Collector Group.**

1. **Configure a Collector Group.** You must perform a Panorama commit and then a Collector Group commit to synchronize the Log Collector configuration with Panorama and to put the Eth1, Eth2, Eth3, Eth4, and Eth5 interfaces (if you configured them) in an operational state on the Log Collector.

   *In any single Collector Group, all the Log Collectors must run on the same Panorama model: all M-500 appliances, all M-100 appliances, or all Panorama virtual appliances.*

   *As a best practice, Enable log redundancy across collectors if you add multiple Log Collectors to a single Collector group. This option requires each Log Collector to have the same number of logging disks.*

2. Select **Panorama > Managed Collectors** to verify that the Log Collector configuration is synchronized with Panorama.

   The Configuration Status column should display In Sync and the Run Time Status column should display connected.

3. Access the Log Collector CLI and enter the following command to verify that its interfaces are operational:

   ```
   > show interface all
   ```

   The output displays the state as up for each interface that is operational.

4. If the Collector Group has multiple Log Collectors, verify they can communicate with each other by running the following command for each interface that the Log Collectors use. For the source IP address, specify the interface of the Log Collector on which you run the command. For the host IP address, specify the matching interface of another Log Collector in the same Collector Group.

   ```
   > ping source <IP-address> host <IP-address>
   ```

   For example, if a Collector Group contains Log Collector A with an MGT interface set to 192.0.2.1 and Log Collector B with an MGT interface set to 192.0.2.2, log in to Log Collector A and enter:

   ```
   > ping source 192.0.2.1 host 192.0.2.2
   ```
If the Log Collectors can communicate over their MGT interfaces, the output displays:

PING 192.0.2.2 (192.0.2.2) from 192.0.2.1 : 56(84) bytes of data.

**STEP 15 | Next steps...**

To enable the Log Collector to receive firewall logs:

1. Configure Log Forwarding to Panorama.
2. Verify Log Forwarding to Panorama.

**Increase Storage on the M-Series Appliance**

After you Perform Initial Configuration of the M-Series Appliance, you can increase log storage capacity of the appliance by upgrading the existing drive pairs to larger capacity drives or by installing additional drive pairs in empty drive bays. For example, you can choose to upgrade the existing 1TB drives to 2TB on an M-100 appliance, or you can add 2TB drives to the empty drive bays (B1 through D2).

> The M-Series appliances leverage RAID 1 for data redundancy in the event of disk failure. Therefore, the pair of drives in a RAID 1 array need to be identical. However, you are free to mix drive capacities across different RAID 1 arrays. For example, the drives in the A1/A2 RAID 1 array can be 1TB drives, and the drives in the B1/B2 RAID 1 array can be 2TB drives.

The following table lists the maximum number of drive bays and the available drive capacities supported on M-Series appliances.

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Number of Supported Drive Bays</th>
<th>Supported Drive Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>M-100 Appliance</td>
<td>8</td>
<td>1TB or 2TB</td>
</tr>
<tr>
<td>M-500 Appliance</td>
<td>24</td>
<td>1TB or 2TB</td>
</tr>
</tbody>
</table>

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

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

- Add Additional Drives to an M-Series Appliance
- Upgrade Drives on M-Series Appliances Running Panorama 7.0.8 or a Later Release
Add Additional Drives to an M-Series Appliance

STEP 1 | Install the new drives in the appropriate drive bays.

Make sure to add the drives sequentially in the next open drive bays. For example, add drives to B1 and B2 before adding drives to C1 and C2.

STEP 2 | Access the command line interface (CLI) on the M-Series appliance.

Connect to the M-Series appliance in one of two ways:

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

STEP 3 | When prompted, log in to the appliance.

Use the default administrator account and the assigned password.

STEP 4 | Configure each array.

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

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

1. Enter the following commands and confirm the request when prompted:

   > request system raid add B1
   > request system raid add B2

2. To monitor the progress of the RAID configuration, enter the following command:

   > show system raid detail

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

<table>
<thead>
<tr>
<th>Disk Pair A</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>clean</td>
</tr>
<tr>
<td>Disk id A1</td>
<td>Present</td>
</tr>
<tr>
<td>model       : ST91000640NS</td>
<td></td>
</tr>
<tr>
<td>size        : 953869 MB</td>
<td></td>
</tr>
<tr>
<td>status      : active sync</td>
<td></td>
</tr>
<tr>
<td>Disk id A2</td>
<td>Present</td>
</tr>
<tr>
<td>model       : ST91000640NS</td>
<td></td>
</tr>
<tr>
<td>size        : 953869 MB</td>
<td></td>
</tr>
<tr>
<td>status      : active sync</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Disk Pair B</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>clean</td>
</tr>
<tr>
<td>Disk id B1</td>
<td>Present</td>
</tr>
<tr>
<td>model       : ST91000640NS</td>
<td></td>
</tr>
<tr>
<td>size        : 953869 MB</td>
<td></td>
</tr>
<tr>
<td>status      : active sync</td>
<td></td>
</tr>
<tr>
<td>Disk id B2</td>
<td>Present</td>
</tr>
<tr>
<td>model       : ST91000640NS</td>
<td></td>
</tr>
</tbody>
</table>
STEP 5 | Make the array available for logging.

To enable the array for logging, you must first add the appliance as a managed collector on Panorama. If not already added, see Configure a Managed Collector.

1. Log in to the web interface of the Panorama management server that manages this Log Collector.
2. Select Panorama > Managed Collectors and edit the Log Collector.
3. Select Disks and Add each array.
4. Click OK to save your changes.
5. Select Commit > Commit to Panorama and Commit your changes.
6. Select Commit > Push to Devices, select the Collector Group, and Push your changes.

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

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

Connect to the M-Series appliance in one of two ways:

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

STEP 2 | When prompted, log in to the appliance.

Use the default administrator account and the assigned password.

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

Enter the following command to view RAID status:

```
> show system raid detail
```

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

<table>
<thead>
<tr>
<th>Disk Pair A</th>
<th>Available</th>
<th>Status</th>
<th>Disk id A1</th>
<th>Present</th>
<th>model</th>
<th>size</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Disk Pair B</th>
<th>Available</th>
<th>Status</th>
<th>Disk id A2</th>
<th>Present</th>
<th>model</th>
<th>size</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Disk Pair B</th>
<th>Available</th>
<th>Status</th>
<th>Disk id A2</th>
<th>Present</th>
<th>model</th>
<th>size</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Disk Pair B</th>
<th>Available</th>
<th>Status</th>
<th>Disk id A2</th>
<th>Present</th>
<th>model</th>
<th>size</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**STEP 4 |** Remove the first 1TB drive and replace it with a 2TB drive.

1. To remove the first drive from the RAID 1 array configuration (A1 in this example), enter the following command and enter `y` when prompted to confirm the request:

```
> request system raid remove A1
```

2. Physically remove the first drive from the drive bay. Press the ejector button on the drive carrier in drive bay A1 to release the ejector handle. Then pull the handle toward you and slide the drive out of the appliance.

3. Remove a 2TB drive from its packaging and place the drive on a table next to the drive you just removed. Take note of how the drive is installed in the carrier because you will install the 2TB drive in this same carrier.

4. Remove the four screws holding the 1TB drive in the carrier and remove the drive from the carrier.

5. Attach the 2TB drive to the carrier using the same four screws you removed from the 1TB drive and then reinsert the carrier with the 2TB drive into drive bay A1.

6. Enter the following command to verify the 2TB drive is recognized:

```
> show system raid detail
```

Verify that the A1 disk shows the correct model and size (about 2TB). If the model and size are not correct, run the above command again until the correct model and size are shown.

If the wrong model and size are consistently shown, enter the following command:

```
> request system raid remove A1
```

Wait for 30 seconds once you run the above command, then remove the disk and reinsert it and repeat the `show system raid detail` command to verify the size and model.

**STEP 5 |** Copy the data from the remaining installed 1TB drive in the RAID 1 array to the newly installed 2TB drive in that array.

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

1. To copy the data from the 1TB drive in drive bay A2 to the newly installed 2TB drive in drive bay A1, enter the following command and enter `y` when prompted:

```
> request system raid copy from A2 to A1
```

2. To view the status of the copy process, run the following command:

```
> show system raid detail
```

---

**Disk id B1**

<table>
<thead>
<tr>
<th>model</th>
<th>ST91000640NS</th>
</tr>
</thead>
<tbody>
<tr>
<td>size</td>
<td>953869 MB</td>
</tr>
<tr>
<td>status</td>
<td>active sync</td>
</tr>
</tbody>
</table>

**Disk id B2**

<table>
<thead>
<tr>
<th>model</th>
<th>ST91000640NS</th>
</tr>
</thead>
<tbody>
<tr>
<td>size</td>
<td>953869 MB</td>
</tr>
<tr>
<td>status</td>
<td>active sync</td>
</tr>
</tbody>
</table>
Continue running this command to view the RAID detail output until you see that the array (A1/A2 in this example) shows Available.

At this point, drive A2 will show not in use because there is a drive size mismatch.

STEP 6 | Upgrade the second drive in the RAID 1 array to a 2TB drive.

1. Remove the second 1TB drive (from drive bay A2 in the current example) for the RAID 1 array configuration:

   > request system raid remove A2

2. Insert the carrier with the newly installed 2TB drive into drive bay A2 and add it to the RAID 1 array configuration:

   > request system raid add A2

   The system will copy the data from A2 to A1 to mirror the drives.

3. To view the status of the copy process, run the following command:

   > show system raid detail

   Continue to view the RAID detail output until you see that the array (A1/A2 in this example) shows Available and both disks show active sync.

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

   Disk id A2     Present
   model        : ST2000NX0253
   size         : 1907138 MB
   status       : active sync

STEP 7 | Upgrade drives for additional RAID 1 arrays as needed.

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

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

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

If it is important to you to retain logs, you must upgrade to Panorama 7.0.8 or a later release and then use the Upgrade Drives on M-Series Appliances Running Panorama 7.0.8 or a Later Release procedure.
STEP 1 | Access the command line interface (CLI) on the M-Series appliance.

Connect to the M-Series appliance in one of two ways:

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

STEP 2 | When prompted, log in to the appliance.

Use the default administrator account and the assigned password.

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

Enter the following command to view RAID status:

> show system raid detail

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

<table>
<thead>
<tr>
<th>Disk Pair A</th>
<th>Available</th>
<th>clean</th>
<th>Present</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk id A1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>model</td>
<td>ST91000640NS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>size</td>
<td>953869 MB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>status</td>
<td>active sync</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk id A2</td>
<td>Present</td>
<td></td>
<td></td>
</tr>
<tr>
<td>model</td>
<td>ST91000640NS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>size</td>
<td>953869 MB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>status</td>
<td>active sync</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Disk Pair B</th>
<th>Available</th>
<th>clean</th>
<th>Present</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk id B1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>model</td>
<td>ST91000640NS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>size</td>
<td>953869 MB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>status</td>
<td>active sync</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk id B2</td>
<td>Present</td>
<td></td>
<td></td>
</tr>
<tr>
<td>model</td>
<td>ST91000640NS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>size</td>
<td>953869 MB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>status</td>
<td>active sync</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

1. To remove the drives from the RAID 1 array configuration (A1 and A2 in this example), enter the following commands and enter \textbf{y} when prompted to confirm each request:

   > request system raid remove A1
   > request system raid remove A2

2. Physically remove the drives from the drive bays. Press the ejector button on each drive carrier to release the ejector handle. Then pull the handle toward you and slide the drives out of the appliance.
3. Remove two 2TB drives from their packaging and place them on a table next to the drives you just removed. Take note of how the drives are installed in the carrier because you will install the 2TB drives in these same carriers.
4. Remove the four screws holding each drive in its carrier and remove the drives from the carriers.
5. Attach the 2TB drives to the carriers using the same screws you just removed and then insert the carriers with the newly installed 2TB drives into the drive bays (A1 and A2 in this example).

**STEP 5 |** Create a new RAID 1 array for the newly installed 2TB drives and ensure that both drives are in the new array.

1. To create a new array that includes the drive in drive bay A1, enter the following command:

   ```
   > request system raid add A1
   ```

2. To view and confirm the status of the new RAID 1 array configuration, enter the following command:

   ```
   > show system raid detail
   ```

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

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

   Disk Pair A       Available
   Status           clean, degraded
   Disk id A1       Present
   model            : ST91000640NS
   size             : 953869 MB
   status           : active sync
   Disk id A2       Present
   model            : ST91000640NS
   size             : 953869 MB
   status           : not in use

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

   ```
   > request system raid add A2
   ```

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

**STEP 6 |** Upgrade drives for additional RAID 1 arrays as needed.

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

**Configure Panorama to Use Multiple Interfaces**

In a large-scale network, you can improve security and reduce congestion by implementing network segmentation, which involves segregating the subnetworks based on resource usage, user roles, and security requirements. Panorama supports network segmentation by enabling you to use multiple M-Series Appliance Interfaces for managing devices (firewalls, Log Collectors, and WildFire appliances and appliance clusters) and collecting logs; you can assign separate interfaces to the devices on separate subnetworks. Using multiple interfaces to collect logs also provides the benefit of load balancing, which is particularly useful in environments where the firewalls forward logs at high rates to the Log Collectors.
Because administrators access and manage Panorama over the MGT interface, securing that interface is especially important. One method for improving the security of the MGT interface is to offload Panorama services to other interfaces. In addition to device management and log collection, you can also offload Collector Group communication and deployment of software and content updates to firewalls, Log Collectors, and WildFire appliances and appliance clusters. By offloading these services, you can reserve the MGT interface for administrative traffic and assign it to a secure subnetwork that is segregated from the subnetworks where your firewalls, Log Collectors, and WildFire appliances and appliance clusters reside.

- Multiple Interfaces for Network Segmentation Example
- Configure Panorama for Network Segmentation

Multiple Interfaces for Network Segmentation Example

Figure 11: Multiple Panorama Interfaces illustrates a deployment that uses multiple interfaces on M-500 appliances in Panorama mode and Log Collector mode. In this example, the interfaces support network segmentation as follows:

- **Panorama management network**—To protect the Panorama web interface, CLI, and XML API from unauthorized access, the MGT interface on Panorama connects to a subnetwork that only administrators can access.
- **Internet**—Panorama uses the MGT interface to communicate with external services such as the Palo Alto Networks Update Server.
- **Perimeter Gateway and Data Center**—Panorama uses a separate pair of interfaces to manage the firewalls and Log Collectors in each of these subnetworks. Managing firewalls typically generates less traffic than querying Log Collectors for report information. Therefore, Panorama uses 1Gbps interfaces (Eth1 and Eth2) for managing the firewalls and uses 10Gbps interfaces (Eth4 and Eth5) for querying and managing the Log Collectors. Each Log Collector uses its MGT interface to respond to the queries but uses its Eth4 and Eth5 interfaces for the heavier traffic associated with collecting logs from the firewalls.
- **Software and content updates**—The firewalls and Log Collectors in both subnetworks retrieve software and content updates over the Eth3 interface on Panorama.
Configure Panorama for Network Segmentation

To offload Panorama services from the MGT interface to other interfaces, start by configuring the interfaces on the Panorama management server. If your network has heavy log traffic, remember that the Eth4 and Eth5 interfaces on the M-500 appliance support higher throughput (10Gbps) than the other interfaces (1Gbps). Then, configure the Log Collectors in each subnetwork to connect with specific interfaces on Panorama. For each Log Collector, you also select an interface for Collector Group communication and one or more interfaces for collecting logs from firewalls. Finally, configure the firewalls in each subnetwork to connect with interfaces on Panorama.

Palo Alto Networks recommends that you specify the IP address, netmask (for IPv4) or prefix length (for IPv6), and default gateway for the MGT interface. If you omit one of these settings (such as the default gateway), you can access the M-Series appliance only through the console port for future configuration changes.

Perform the following steps to configure Panorama and Dedicated Log Collectors to use multiple interfaces:
STEP 1 | Verify that the M-Series appliances and firewalls have the prerequisite software versions and configurations.

- The M-Series appliances must run Panorama 8.0 or later to use a separate interface for deploying updates and to use multiple interfaces for device management and log collection.
- The M-Series appliances must run Panorama 6.1 or later to use separate interfaces for log collection or Collector Group communication.
- The initial configuration of each Panorama management server is complete. This includes configuration of the MGT interface.
- Log Collectors and Collector Groups are configured. This includes configuration of the MGT interface on the Log Collectors.
- The initial configuration of the firewalls is complete, you have added the firewalls to Panorama as managed devices, and the firewalls in each subnetwork are assigned to a separate template.
- The initial configuration of WildFire appliances is complete and you have added WildFire appliances to Panorama as managed devices.

STEP 2 | Configure the interfaces on the solitary (non-HA) or active (HA) Panorama management server.

Because the MGT interface was configured during initial Panorama configuration, you don’t have to configure it again.

Perform these steps for each interface:

1. Log in to the Panorama Web Interface of the solitary (non-HA) or active (HA) Panorama management server.
2. Select Panorama > Setup > Interfaces.
3. Click an Interface Name to edit the interface.
4. Select <interface-name> to enable the interface.
5. Configure one or both of these field sets based on the IP protocols of your network:
   - IPv4—IP Address, Netmask, and Default Gateway
   - IPv6—IPv6 Address/Prefix Length and Default IPv6 Gateway
6. Select the services that the interface supports:
   - Device Management and Device Log Collection—Manage firewalls, Log Collectors, and WildFire appliances and appliance clusters, collect logs that the Log Collectors generate, and query the Log Collectors for report information. To support a segmented network, you can enable these services on multiple interfaces.
   - Collector Group Communication—Communicate with the Collector Groups that Panorama manages across all subnetworks.
   - Device Deployment—Deploy software and content updates to managed firewalls, Log Collectors, and WildFire appliances and appliance clusters across all subnetworks.
7. Click OK to save your changes to the interface.
8. Click Commit > Commit to Panorama and Commit your changes.

STEP 3 | (HA only) Configure the interfaces on the passive Panorama management server.

1. Log in to the Panorama Web Interface of the active Panorama management server.
2. Select Panorama > Managed Collectors and select the passive HA peer.
3. Select Interfaces and click an interface to edit.
4. Check the Enable Interface box to enable the interface.
5. Configure one or both of these field sets based on the IP protocols of your network:
   - IPv4—IP Address, Netmask, and Default Gateway
   - IPv6—IPv6 Address/Prefix Length and Default IPv6 Gateway
6. Select the services that the interface supports:

- **Device Management and Device Log Collection**—Manage firewalls, Log Collectors, and WildFire appliances and appliance clusters, collect logs that the Log Collectors generate, and query the Log Collectors for report information. To support a segmented network, you can enable these services on multiple interfaces.
- **Collector Group Communication**—Communicate with the Collector Groups that Panorama manages across all subnetworks.
- **Device Deployment**—Deploy software and content updates to managed firewalls, Log Collectors, and WildFire appliances and appliance clusters across all subnetworks.

7. Click **OK** to save your changes to the interface.

8. Select **Commit > Commit and Push** to commit your changes to Panorama and to push the changes to Collector Groups that contain the passive HA peer you modified.

**STEP 4 |** Configure each Log Collector to connect with a Panorama interface.

To support a segmented network, you can connect the Log Collectors in each subnetwork to separate Panorama interfaces. The interfaces must have **Device Management and Device Log Collection** enabled, as described in the previous step.

1. **Log in to the Panorama Web Interface** of the solitary (non-HA) or active (HA) Panorama management server.
2. Select **Panorama > Managed Collectors** and edit the Log Collector.
3. In the **Panorama Server IP** field, enter the IP address of an interface on the solitary (non-HA) or active (HA) Panorama.
4. **(HA only)** In the **Panorama Server IP 2** field, enter the IP address of an interface on the passive Panorama that will support **Device Management and Device Log Collection** if failover occurs on the active Panorama.
5. Click **OK** to save your changes.
6. Select **Commit > Commit and Push** to commit your changes to Panorama and to push the changes to Collector Groups that contain the Log Collector you modified.

7. Perform the following steps on each Dedicated Log Collector:
   1. Access the Log Collector CLI by using emulation software such as PuTTY to open a SSH session to the Log Collector using its MGT interface IP address. When prompted, log in using Panorama administrator credentials.
   2. Run the following commands, where `<IPaddress1>` is for the solitary (non-HA) or active (HA) Panorama and `<IPaddress2>` is for the passive Panorama (if applicable).

```
> configure
  # set deviceconfig system panorama-server <IPaddress1> panorama-server-2 <IPaddress2>
  # commit
```

**STEP 5 |** **(HA only)** Configure an interface on the passive Panorama management server to deploy updates in case the active Panorama falls over.

1. **Log in to the Panorama Web Interface** of the passive Panorama management server.
2. Select **Panorama > Setup > Interfaces**.
3. Click an Interface Name to edit the interface.
4. Select `<interface-name>` check box to enable the interface.
5. Configure one or both of these field sets based on the IP protocols of your network:
   - **IPv4**—IP Address, Netmask, and Default Gateway
   - **IPv6**—IPv6 Address/Prefix Length and Default IPv6 Gateway
6. Select **Device Deployment**.
7. Click **OK** to save your changes.

**STEP 6** | Configure the interfaces that the Log Collectors will use to collect logs from firewalls and communicate with other Log Collectors.

> Because the MGT interface was configured during initial configuration of the Log Collectors, you don’t have to configure it again.

1. **Log in to the Panorama Web Interface** of the solitary (non-HA) or active (HA) Panorama management server.
2. Select **Panorama > Managed Collectors** and edit the Log Collector.
3. Select **Interfaces** and perform the following steps for each interface:
   1. Click an interface name to edit that interface.
   2. Select `<interface-name>` to enable the interface.
   3. Configure one or both of the following field sets based on the IP protocols of your network.
      - **IPv4**—IP Address, Netmask, and Default Gateway
      - **IPv6**—IPv6 Address/Prefix Length and Default IPv6 Gateway
4. Select the functions that the interface supports:
   - **Device Log Collection**—Collect logs from firewalls. You can load balance the logging traffic by enabling multiple interfaces to perform this function.
   - **Collector Group Communication**—Communicate with other Log Collectors in the Collector Group.
5. Click **OK** to save your changes to the interface.
4. Click **OK** to save your changes to the Log Collector.
5. Select **Commit > Commit and Push** to commit your changes to Panorama and to push the changes to Collector Groups that contain the Log Collectors you modified.
6. Select **Panorama > Managed Collectors** to verify that the Log Collectors are synchronized and connected with Panorama.

   The Configuration Status column should display **InSync** and the Run Time Status column should display **connected**.

**STEP 7** | Configure the firewalls to connect with a Panorama interface.

To support a segmented network, you can connect the firewalls in each subnetwork to separate Panorama interfaces. The interfaces must have **Device Management and Device Log Collection** enabled. This step assumes that you use separate templates to configure the firewalls in separate subnetworks.

> In this example deployment, Panorama uses these interfaces to manage the firewalls but not to collect firewall logs. You specify which Dedicated Log Collectors will collect firewall logs when you configure Collector Groups.

1. **Log in to the Panorama Web Interface** of the solitary (non-HA) or active (HA) Panorama management server.
2. On Panorama, select **Device > Setup > Management**, select a **Template** and edit the Panorama Settings.
3. In the first **Panorama Servers** field, enter the IP address of an interface on the solitary (non-HA) or active (HA) Panorama.
4. (HA only) In the second **Panorama Servers** field, enter the IP address of an interface on the passive Panorama that will support device management if failover occurs.
5. Click **OK** to save your changes.
6. Select **Commit** > **Commit and Push** to commit your changes to Panorama and push the template changes to firewalls.

7. Select **Panorama** > **Managed Devices** to verify that the firewalls are synchronized and connected with Panorama.

   The Device State column should display **Connected**. The Shared Policy and Template columns should display **InSync**.
Register Panorama and Install Licenses

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

If you want to use the cloud-based Logging Service, you require a Logging Service license, in addition to the firewall management license and premium support license. To purchase licenses, contact your Palo Alto Networks Systems Engineer or reseller.

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

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

Register Panorama

STEP 1 | 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 model:
- M-Series appliance—Log in to the Panorama web interface and record the Serial # value in the Dashboard tab, General Information section.
- Panorama virtual appliance—See the order fulfillment email.

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

- If this is the first Palo Alto Networks appliance you are registering and you don't yet have a login:
  2. Click Activate My Account.
3. Enter Your Email Address, Enter the characters from the picture, and Submit.

4. Select Register device using Serial Number or Authorization Code and Submit.

5. Enter the contact details for the person in your organization who will own this account. Required fields are indicated by red asterisks.
6. Create a UserID and Password for the account. Required fields are indicated by a red asterisks.
7. Enter the Panorama Serial Number or Auth Code.
8. Enter your Sales Order Number or Customer Id.
9. To ensure that you are always alerted to the latest updates and security advisories, Subscribe to Content Update Emails, Subscribe to Security Advisories, and Subscribe to Software Update Emails.
10. Select the check box to agree to the End User Agreement and Submit.

- If you already have a support account:
  2. Click Register a Device in the Quick Actions section.
4. Select **Register device using Serial Number or Authorization Code**, and click **Submit**.

5. Enter the Panorama **Serial Number** along with the required Location Information (as indicated by the asterisks).

6. Read the End User License Agreement ("EULA") and the Support Agreement and then **Agree and Submit**.

After you see the registration complete message, close the Device Registration dialog.

---

**Activate a Panorama Support License**

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

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

**STEP 1** | Log in to the Palo Alto Networks **customer support** portal to activate the auth-code.

1. Select **Assets > Devices** and enter your Panorama serial number to Filter by the **Serial Number**.
2. Click the pencil icon in the Action column, select **Activate Auth-Code** and enter your support license **Authorization Code**, and click **Agree and Submit**.

**STEP 2 |** Log in to the Panorama web interface, and select **Panorama > Support > Activate support using authorization code**.

**STEP 3 |** Enter the **Authorization Code** and click **OK**.

**STEP 4 |** Verify that the subscription is activated. Check the details (for example, the **Expiry Date**, support **Level**, and **Description**) in the Support section of the page.
Activate/Retrieve a Firewall Management License on the Panorama Virtual Appliance

In order to manage devices on Panorama, you need to activate a firewall management license generated by PAN-OS. The device management license you activate determines the number of devices Panorama can manage. Log Collectors and WildFire appliances are not treated as managed devices and do not count toward the number of devices allotted by the device management license.

Before activating and retrieving a firewall management license on the Panorama virtual appliance, you must Register Panorama. If you are running an evaluation license and want to apply a license that you purchased, you must still register and activate/retrieve the purchased license. Additionally, you must then change the serial number of the Panorama from the evaluation serial number to the production serial number.

**STEP 1 |** Log in to the Panorama Web Interface.

**STEP 2 |** Select Panorama > Setup > Management and edit the General Settings.

**STEP 3 |** Enter the Panorama Serial Number (included in the order fulfillment email) and click OK.

**STEP 4 |** Select Panorama > Licenses to activate or retrieve the firewall management license:

- **Retrieve license keys from license server**—Panorama automatically retrieves and activates the firewall management license from the Panorama Update Server.
- **Activate feature using authorization code**—Enter the firewall management license authorization code and click OK to activate the license. The authorization code can be obtained from the order fulfillment email or by logging in to the Palo Alto Networks Customer Support web site by finding the Panorama management server.
- **Manually upload license key**—Log in to the Palo Alto Networks Customer Support web site, find your Panorama management server, and download the firewall management license key to your local device. After you download the license key, click Choose File to select the license key and click OK.

**STEP 5 |** Verify the firewall management license is activated.

The Device Management License section now appears displaying the date the license was issued, when the license expires, and a description of the firewall management license.

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

In order to manage devices on Panorama, you will need to activate a Capacity License. The Capacity License you activate will determine the number of devices Panorama can manage. Log Collectors and WildFire appliances are not treated as managed devices and will not count toward the number of devices allotted by the Capacity License.

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

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

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

To activate and retrieve the license, the options are:

• **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-Series Appliance**) but you have not activated the license on the **Palo Alto Networks Customer Support web site**.

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.

• **Retrieve the license key from the license server.**

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

1. Activate the license on the **Palo Alto Networks Customer Support web site**.
   1. On a host with internet access, use a web browser to access the **Palo Alto Networks Customer Support web site** and log in.
   2. Select **Assets > Devices**, find your M-Series appliance and, in the Action column, click the edit icon ( ).
   3. Select **Activate Auth-Code**, enter the **Authorization Code** and click **Agree and Submit** to activate the license.
2. Configure Panorama to connect to the update server: see **Perform Initial Configuration of the M-Series Appliance**.
3. Select **Panorama > Licenses** and click **Retrieve license keys from the license server**. Panorama retrieves the activated license.

• **Manually upload the license from a host to Panorama.** Panorama must have access to that host.

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

1. Activate and download the license from the **Palo Alto Networks Customer Support web site**.
   1. On a host with internet access, use a web browser to access the **Palo Alto Networks Customer Support web site** and log in.
   2. Select **Assets > Devices**, find your M-Series appliance and, in the Action column, click the edit icon ( ).
   3. Select **Activate Auth-Code**, enter the **Authorization Code** and click **Agree and Submit** to activate the license.
   4. In the Action column, click the download icon and save the license key file to the host.
2. In the Panorama web interface, select **Panorama > Licenses**, click **Manually upload license key** and click **Browse**.
3. Select the key file you downloaded to the host and click **Open**.
4. Click **OK** to upload the activated license key.
Install Content and Software Updates for Panorama

A valid support subscription enables access to the Panorama™ software image and release notes. To take advantage of the latest fixes and security enhancements, upgrade to the latest software and content updates that your reseller or a Palo Alto Networks® Systems Engineer recommends for your deployment. 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, Firewall, and WildFire Version Compatibility
- Install Updates for Panorama in an HA Configuration
- Install Updates for Panorama with an Internet Connection
- Install Updates for Panorama without an Internet Connection
- Migrate Panorama Logs to the New Log Format

Panorama, Log Collector, Firewall, and WildFire Version Compatibility

For best results, adhere to the following Panorama™ compatibility guidelines:

- Install the same Panorama release on both the Panorama management server and the Dedicated Log Collectors.
- Panorama can manage firewalls that are running the same or an earlier PAN-OS® feature release. You must upgrade Panorama to PAN-OS 8.0 before upgrading the firewalls it manages to 8.0.

  *Panorama 6.1 and later versions cannot push configurations to firewalls running PAN-OS 6.0.0 through PAN-OS 6.0.3.*

- Panorama 8.0 can manage WildFire® appliances and appliance clusters that are running the same or an earlier PAN-OS 8.0 release.
- The content release version on the Panorama management server must be the same (or earlier) version as the content release version on any Dedicated Log Collectors or managed firewalls.

  *Palo Alto Networks® recommends installing the same Applications database version on Panorama as on the Dedicated Log Collectors and firewalls.*

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

Install Updates for Panorama in an HA Configuration

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

Panorama 8.0 requires the following minimum content release versions:
- Applications and Threats content release version 655
- Antivirus content release version 2137

STEP 1 | Upgrade the Panorama software on the Secondary_B (passive) peer.

Perform one of the following tasks on the Secondary_B peer:
- Install Updates for Panorama with an Internet Connection
- Install Updates for Panorama When Not Internet-Connected

After the upgrade, this Panorama transitions to a non-functional state because the peers are no longer running the same software release.

STEP 2 | Suspend the Primary_A peer to force a failover.

On the Primary_A peer:
1. In the Operational Commands section (Panorama > High Availability), Suspend local Panorama.
2. Verify that state is suspended (displayed on bottom-right corner of the web interface).

The resulting failover should cause the Secondary_B peer to transition to active state.

STEP 3 | Upgrade the Panorama software on the Primary_A (currently passive) peer.

Perform one of the following tasks on the Primary_A peer:
- Install Updates for Panorama with an Internet Connection
- Install Updates for Panorama When Not Internet-Connected

After you reboot, the Primary_A peer is initially still in the passive state. Then, if preemption is enabled (default), the Primary_A peer automatically transitions to the active state and the Secondary_B peer reverts to the passive state.

If you disabled preemption, manually Restore the Primary Panorama to the Active State.

STEP 4 | Verify that both peers are now running any newly installed content release versions and the newly installed Panorama release.

On the Dashboard of each Panorama peer, check the Panorama Software Version and Application Version and confirm that they are the same on both peers and that the running configuration is synchronized.

STEP 5 | Migrate Panorama Logs to the New Log Format.

When you upgrade to a Panorama 8.0 (or later) release, Panorama Log Collectors use a new log storage format. Because Panorama can no longer generate reports or ACC data from logs in the pre-8.0-release log format, you must migrate the existing logs as soon as you upgrade Panorama and its Log Collectors from a PAN-OS 7.1 or earlier release to a PAN-OS 8.0 or later release. Log migration is a one-time task; after you migrate the logs on the Log Collector as part an upgrade to a PAN-OS 8.0 or later release, you do not need to migrate them again.
Install Updates for Panorama with an Internet Connection

If Panorama™ has a direct connection to the internet, perform the following steps to install Panorama software and content updates as needed. If Panorama is running in a high availability (HA) configuration, upgrade the Panorama software on each peer (see Install Updates for Panorama in an HA Configuration).

Upgrading the software on the Panorama virtual appliance does not change the system mode; switching to Panorama mode or Legacy mode is a manual task that requires additional settings as described when you Set Up the Panorama Virtual Appliance with Local Log Collector.

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

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

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

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

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

STEP 3 | (As needed) Install content updates.

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

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

1. Check Now (Panorama > Dynamic Updates) for the latest updates. If the value in the Action column is Download, an update is available.
2. (As needed) Before you update the content release version on Panorama, be sure to upgrade managed firewalls and then Log Collectors (see Upgrade Log Collectors When Panorama Is Internet-Connected) to the same (or a later) content release version.
   If you do not need to install content updates at this time, then skip ahead to Step 4.
3. Install remaining content updates, as needed. When installed, the Currently Installed column displays a check mark.
1. **Download** and **Install** the Applications or Applications and Threats update. Regardless of your subscription, Panorama installs and needs only the Applications content update, not the Threats content. For details, see Panorama, Log Collector, Firewall, and WildFire Version Compatibility.

2. **Download** and **Install** other updates (Antivirus, WildFire®, or URL Filtering) as needed, one at a time, and in any sequence.

**STEP 4** | Determine the software upgrade path. Refer to the New Features Guide for the upgrade path to PAN-OS® 8.0.

Check which version has a check mark in the Currently Installed column (Panorama > Software) and proceed as follows.

- If a Panorama 7.1 release is currently installed, skip ahead to Step 6 to upgrade to a Panorama 8.0 release.
- If a release earlier than Panorama 7.1 is installed, proceed to Step 5 and follow the upgrade path to Panorama 7.1.0 before you upgrade to a Panorama 8.0 release.

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

**STEP 5** | Use the upgrade path identified in Step 4 to upgrade to a Panorama 7.1 release.

Repeat the following procedure until the appliance is running a Panorama 7.1 release—do not skip installation of any major release version in the path to your target Panorama 8.0 release.

1. **Check Now** (Panorama > Software) for the latest updates. If an update is available, the Action column displays a **Download** link.

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

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

3. **Install** the software update.

   - If prompted to reboot, click Yes. If you see a CMS Login prompt, press Enter without typing a username or password. When the Panorama login prompt appears, enter the username and password you specified during initial configuration.
   - If you are not prompted to reboot, **Reboot Panorama** from the Device Operations section (Panorama > Setup > Operations).

4. Repeat these for each release in your upgrade path until you are running Panorama 7.1.

**STEP 6** | Install Panorama 8.0.

1. **Check Now** (Panorama > Software) for the latest updates. If an update is available, the Action column displays **Download**.

   *If you are upgrading to Panorama 8.0.3 or a later release, first download the Panorama 8.0.2 base image.*
2. Locate and Download the model-specific file for the release version to which you are upgrading. For example, to upgrade an M-Series appliance to Panorama 8.0.2, download the Panorama_m-8.0.2 image; to upgrade a Panorama virtual appliance to Panorama 8.0.2, download the Panorama_pc-8.0.2 image. After a successful download, the Action column changes from Download to Install for the downloaded image.

3. (Required for the target release; also required for the base image—Panorama 8.0.2—if you manually download or upload the base image when upgrading to Panorama 8.0.3 or a later release) Install the downloaded image and then reboot.

1. Install the image.

   As a best practice, when you upgrade to Panorama 8.0.3 or a later release, install the Panorama 8.0.2 base image and reboot the appliance before you download and install the maintenance release even if you downloaded the base image directly from the Software Updates server.

2. After the installation completes successfully, reboot using one of the following methods:
   - If prompted to reboot, click Yes. If you see a CMS Login prompt, press Enter without typing a username or password. When the Panorama login prompt appears, enter the username and password you specified during initial configuration.
   - If you are not prompted to reboot, Reboot Panorama from the Device Operations section (Panorama > Setup > Operations).

4. (Required only if upgrading to PAN-OS 8.0.3 or a later release) After completing the above steps for the PAN-OS 8.0.2 base image, repeat steps a through c to upgrade to the target maintenance release.

STEP 7 | (Best Practice) Schedule recurring, automatic content updates.

   Panorama does not synchronize content update schedules across HA peers. You must perform this task on both the active and passive Panorama.

In the header row for each update type (Panorama > Dynamic Updates), the Schedule is initially set to None. Perform the following steps for each update type.

1. Click None and select the update frequency (Recurrence). The frequency options depend on the update type.

2. Select the schedule action:
   - Download And Install (Best Practice)—Panorama automatically installs updates after downloading them.
   - Download Only—You must manually install updates after Panorama downloads them.

3. Based on the best practices for the security posture of your organization, configure a delay (Threshold) after an update becomes available before Panorama downloads the update.

4. Click OK to save your changes.

5. Select Commit > Commit to Panorama and Commit your changes.

STEP 8 | Migrate Panorama Logs to the New Log Format.

When you upgrade to a Panorama 8.0 or later release, Panorama Log Collectors use a new log storage format. Because Panorama can no longer generate reports or ACC data from logs in the pre-8.0-release log format, you must migrate the existing logs as soon as you upgrade Panorama and its Log Collectors from a PAN-OS 7.1 or earlier release to a PAN-OS 8.0 or later release. Log migration is a one-time task; after you migrate the logs on the Log Collector as part an upgrade to a PAN-OS 8.0 or later release, you do not need to migrate them again.
Install Updates for Panorama When Not Internet-Connected

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

Upgrading the software on the Panorama virtual appliance does not change the system mode; switching to Panorama mode or Legacy mode is a manual task that requires additional settings as described when you Set Up the Panorama Virtual Appliance with Local Log Collector.

Before updating Panorama, refer to the Release Notes for the minimum content release version required for PAN-OS® 8.0.

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

☐ Refer to the Release Notes for the minimum content release version you must install for a Panorama software release. If you intend to upgrade Log Collectors and firewalls to a particular release, you must first upgrade Panorama to that (or a later) release.

☐ For a Panorama virtual appliance that runs on an ESXi server, ensure that the server meets the Setup Prerequisites for the Panorama Virtual Appliance.

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

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

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

STEP 3 | Determine which content updates you need to install.

Palo Alto Networks® highly recommends that Panorama, Log Collectors, and all managed firewalls run the same content release version.

1. For each content update, determine whether you need updates and which content updates you need to download in Step 4.

Ensure that Panorama is running the same but not a later content release version than is running on managed firewalls and Log Collectors.

2. (As needed) Before you update the content release version on Panorama, be sure to upgrade managed firewalls and then Log Collectors (see Upgrade Log Collectors When Panorama Is Internet-Connected) to the same (or a later) content release version.

STEP 4 | (As needed) Download content updates to a host that can connect and upload content to Panorama either over SCP or HTTPS.

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

1. Use a host that has internet access to log in to the Palo Alto Networks Customer Support website.
2. Download content updates as needed:

   1. Click Updates > Dynamic Updates in the Resources section.
2. **Download** the appropriate content updates and save the files to the host. Perform this step for each content type you need to update.

**STEP 5 | Install content updates as needed.**

*You must install content updates before software updates and you must Upgrade Firewalls When Panorama Is Not Internet-Connected first and then Upgrade Log Collectors When Panorama Is Not Internet-Connected before you install them on the Panorama management server.*

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

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

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

1. Click **Upload**, select the content **Type**, **Browse** to the location on the host to which you downloaded the update, select the update, and click **OK**.

2. **Install From File**, select the **Package Type**, and click **OK**.

**STEP 6 | Determine the software upgrade path.** Refer to the New Features Guide for the upgrade path to a PAN-OS 8.0 release.

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

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

**STEP 7 | Download the software updates** to a host that can connect and upload content to Panorama either over SCP or HTTPS.

1. Use a host with internet access to log in to the Palo Alto Networks Customer Support web site.

2. Download software updates:

   1. On the main page of Palo Alto Networks Customer Support website, click **Software Updates** (Resources section).

   2. For the first (or next) Panorama release in your upgrade path, identify the model-specific file. For example, to upgrade an M-Series appliance to Panorama 8.0.8, download the Panorama_m-8.0.8 image; to upgrade a Panorama virtual appliance to Panorama 8.0.8, download the Panorama_pc-8.0.8 image.

   *You can quickly locate Panorama images by selecting Panorama M Images (M-Series appliances) or Panorama Updates (virtual appliances) from the Filter By drop-down.*

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

   4. Repeat steps 7.b.ii and 7.b.iii for any additional release versions in your upgrade path as determined in Step 6.

**STEP 8 | Install the software updates.**
For each release in your upgrade path (starting with the earliest), perform the following steps:

1. Click Upload (Panorama > Software).
2. **Browse** to the location on the host to which you downloaded the update, select the update, **Sync To Peer** if Panorama is in an HA configuration (to push the software image to the secondary peer), and click **OK**.
3. Install the software image and reboot.

For an HA configuration, **Install Updates for Panorama in an HA Configuration**; otherwise:

1. Install the downloaded image.
2. After you successfully complete the installation, reboot using one of the following methods:
   - If prompted to reboot, click **Yes**. If you see a CMS Login prompt, press Enter without typing a username or password. When the Panorama login prompt appears, enter the username and password you specified during initial configuration.
   - If you are not prompted to reboot, **Reboot Panorama** from the Device Operations section (Panorama > Setup > Operations).
4. Repeat steps 8.a through 8.c for each release in your path.

**STEP 9 | Migrate Panorama Logs to the New Log Format.**

When you upgrade to a Panorama 8.0 or later release, Panorama Log Collectors use a new log storage format. Because Panorama can no longer generate reports or ACC data from logs in the pre-8.0-release log format, you must migrate the existing logs as soon as you upgrade Panorama and its Log Collectors from a PAN-OS 7.1 or earlier release to a PAN-OS 8.0 or later release. Log migration is a one-time task; after you migrate the logs on the Log Collector as part an upgrade to a PAN-OS 8.0 or later release, you do not need to migrate them again.

**Migrate Panorama Logs to the New Log Format**

After you upgrade to a Panorama™ 8.0 (or later) release, Panorama Log Collectors use a new log storage format. Because Panorama cannot generate reports or ACC data from logs in the pre-8.0-release log format after you upgrade, you must migrate the existing logs as soon as you upgrade Panorama and its Log Collectors from a PAN-OS® 7.1 or earlier release to a PAN-OS 8.0 or later release and you must do this before you upgrade your managed firewalls. Panorama will continue to collect logs from managed devices during the log migration but will store the incoming logs in the new log format after you upgrade to PAN-OS 8.0 or a later release. Additionally, Panorama migrates the most recent logs first and works towards the oldest logs. For this reason, you will see only partial data in the ACC and in Reports until Panorama completes the log migration process.

Log migration to the new format is a one time task that you must perform when you upgrade to PAN-OS 8.0 or later release; you do not need to perform this migration again when you upgrade to a later PAN-OS release. If you are upgrading from PAN-OS 7.1 to PAN-OS 8.1 or later release, you can perform the migration after you upgrade to your target PAN-OS release. If PAN-OS 8.0 is your target release then you must migrate logs to the new logging format upon successful upgrade.

The amount of time Panorama takes to complete the log migration process depends on the volume of new logs being written to Panorama, the size of the logging disks, quantity of logging disk pairs, the size of the log database you are migrating, CPU load, and available RAM. The log migration process is throttled to only use idle CPU cycles. Because log migration is a CPU-intensive process, begin the migration during a time when the logging rate is lower. You can always stop migration during peak times if you notice that CPU utilization rates are high and resume the migration when the incoming log rate is lower.
After you upgrade Panorama and upgrade the Log Collectors, migrate the logs as follows:

- **View the incoming logging rate.**
  For best results, start log migration when the incoming log rate is low. To check the rate, run the following command from the Log Collector CLI:

  ```
  admin@M500-LC> debug log-collector log-collection-stats show incoming-logs
  ```

  *High CPU utilization (close to 100%) during log migration is expected and operations will continue to function normally. Log migration is throttled in favor of incoming logs and other processes in the event of resource contention.*

- **Start migrating the logs on each Log Collector to the new format.**
  - To begin the migration, enter the following command from the Panorama CLI:

    ```
    admin@M500-MGR> request logdb migrate lc serial-number <ser_num> start
    ```

    or

  - To begin the migration, enter the following command from the CLI of each Log Collector:

    ```
    admin@M500-LC> request logdb migrate lc start
    ```

- **View the log migration status to estimate the amount of time it will take to finish migrating all existing logs to the new format.**
  - From the Panorama CLI:

    ```
    admin@M500-MGR> request logdb migrate lc serial-number <ser_num> status
    Slot: all
    Migration State: In Progress
    Percent Complete: 0.04
    Estimated Time Remaining: 451 hour(s) 47 min(s)
    ```

  or

  - From the CLI of each Log Collector:

    ```
    admin@M500-LC> request logdb migrate lc status
    Slot: all
    Migration State: In Progress
    Percent Complete: 0.04
    Estimated Time Remaining: 5 hour(s) 32 min(s)
    ```

- **Stop the log migration process.**
  - To temporarily stop the log migration process, enter the following command from the Panorama CLI:

    ```
    admin@M500-MGR request logdb migrate lc serial-number <ser_num> stop
    ```

    or
• To temporarily stop the log migration process, enter the following command from the CLI of each Log Collector:

```
admin@M500-LC request logdb migrate lc stop
```
Transition to a Different Panorama Model

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

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

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

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

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

STEP 1 | Plan the migration.

☐ Upgrade the software on the Panorama virtual appliance before the migration if the M-Series appliance requires a later release of the current software (the M-500 appliance requires Panorama 7.0 or a later release). For important details about software versions, see Panorama, Log Collector, Firewall, and WildFire Version Compatibility.

☐ Schedule a maintenance window for the migration. Although firewalls can buffer logs after the Panorama virtual appliance goes offline and then forward the logs after the M-Series appliance comes online, completing the migration during a maintenance window minimizes the risk that logs will exceed the buffer capacities and be lost during the transition between Panorama models.

☐ Consider whether to maintain access to the Panorama virtual appliance after the migration to access existing logs. The most efficient approach is to assign a new IP address to the Panorama virtual appliance and reuse its old IP address for the M-Series appliance. This ensures that the Panorama virtual appliance remains accessible and that firewalls can point to the M-Series appliance without reconfiguring the Panorama IP address on each firewall.

STEP 2 | Migrate your subscriptions to the new appliance.

1. Purchase the new support license and migration license.
2. Provide your sales representative the serial number of the Panorama virtual appliance you will phase out, the auth-code you received when you purchased the new M-Series appliance, and the effective date for the migration. On the effective date, Palo Alto Networks will automatically apply the auth-code to the serial number of the M-Series appliance, phase out support for the Panorama virtual appliance, and trigger support for the M-Series appliance. Consult your sales representative regarding how much time is available to complete the migration after the effective date. At the end of that period, Palo Alto Networks terminates the support entitlement on the Panorama virtual appliance, after which it can no longer receive software or content updates.
STEP 3 | Export the Panorama configuration from the Panorama virtual appliance.
1. Log in to the Panorama virtual appliance and select Panorama > Setup > Operations.
2. Click Save named Panorama configuration snapshot, enter a Name to identify the configuration, and click OK.
3. Click Export named Panorama configuration snapshot, select the Name of the configuration you just saved, and click OK. Panorama exports the configuration to your client system as an XML file.

STEP 4 | Power off the Panorama virtual appliance if you won’t need to access to it after the migration or assign a new IP address to its management (MGT) interface if you will need access to it.

To power off the Panorama virtual appliance, see the documentation for your VMware product.

To change the IP address on the Panorama virtual appliance:
1. Select Panorama > Setup > Management, and edit the Management Interface Settings.
2. Enter the new IP Address and click OK.
3. Select Commit > Commit to Panorama and Commit your changes.

STEP 5 | Perform the initial setup of the M-Series appliance.
1. Rack mount the M-Series appliance. Refer to the M-100 or M-500 Appliance Hardware Reference Guide for instructions.
2. Perform Initial Configuration of the M-Series Appliance to define the network connections required to activate licenses and install updates.
3. Register Panorama.
4. Activate a Panorama Support License.
5. Activate/Retrieve a Firewall Management License on the M-Series Appliance. Use the auth-code associated with the migration license.
6. Install Content and Software Updates for Panorama. Install the same versions as those on the Panorama virtual appliance.

STEP 6 | Load the Panorama configuration snapshot that you exported from the Panorama virtual appliance into the M-Series appliance.
2. Click Import named Panorama configuration snapshot, Browse to the Panorama configuration file you exported from the Panorama virtual appliance, and click OK.
3. Click Load named Panorama configuration snapshot, select the Name of the configuration you just imported, select a Decryption Key (the master key for Panorama), and click OK. Panorama overwrites its current candidate configuration with the loaded configuration. Panorama displays any errors that occur when loading the configuration file.
4. If errors occurred, save them to a local file. Resolve each error to ensure the migrated configuration is valid.

STEP 7 | Modify the configuration on the M-Series appliance.
Required if the M-Series appliance will use different values than the Panorama virtual appliance. If you will maintain access to the Panorama virtual appliance to access its logs, use a different hostname and IP address for the M-Series appliance.
1. Select Panorama > Setup > Management.
2. Edit the General Settings, modify the Hostname, and click OK.
3. Edit the Management Interface Settings, modify the values as necessary, and click OK.

STEP 8 | Add the default managed collector and Collector Group back to the M-Series appliance.
Loading the configuration from the Panorama virtual appliance (Step Load the Panorama configuration snapshot that you exported from the Panorama virtual appliance into the M-Series appliance.) removes the default managed collector and Collector Group that are predefined on each M-Series appliance.

1. **Configure a Managed Collector** that is local to the M-Series appliance.
2. **Configure a Collector Group** for the default managed collector.
3. Select **Commit > Commit to Panorama** and **Commit** your changes to the Panorama configuration.

**STEP 9 | Synchronize the M-Series appliance with the firewalls to resume firewall management.**

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

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

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

You can migrate the Panorama configuration from an M-100 or M-500 appliance to a Panorama virtual appliance in Panorama mode. However, you cannot migrate the logs because the log format on the M-Series appliances is incompatible with that on the Panorama virtual appliances. Therefore, if you want to maintain access to the old logs stored on the M-Series appliance, you must continue running the M-Series appliance as a Dedicated Log Collector after the migration and add it to the Panorama virtual appliance as a managed collector. The M-Series appliance will continue to collect the new logs that firewalls forward after the migration.

**STEP 1 | Plan the migration.**

- Determine the required software version of the Panorama virtual appliance. **Upgrade the software** on the M-Series appliance before the migration if the Panorama virtual appliance requires a more recent Panorama release (the M-500 appliance requires Panorama 7.0 or a later release). For important details about software versions, see Panorama, Log Collector, Firewall, and WildFire Version Compatibility.

- Schedule a maintenance window for the migration. Although firewalls can buffer logs after the M-Series appliance goes offline and then forward the logs after the Panorama virtual appliance comes online, completing the migration during a maintenance window minimizes the risk that logs will exceed the buffer capacities and be lost during the transition between Panorama models.

**STEP 2 | Purchase management and support licenses for the new Panorama virtual appliance.**

1. Get the auth-code for the Panorama virtual appliance and the support license.
2. Provide your sales representative the serial number of the M-Series appliance you will phase out, the auth-code you received when you purchased the new Panorama Virtual appliance, and the effective
date for the migration. On the effective date, Palo Alto Networks will automatically apply the existing auth-code to the serial number of the Panorama virtual appliance, apply the new management license to the M-Series appliance, and trigger support for the M-Series appliance. Consult your sales representative regarding how much time is available to complete the migration after the effective date.

**STEP 3 | Export the configuration from the M-Series appliance.**

1. Log in to the M-Series appliance and select Panorama > Setup > Operations.
2. Click Save named Panorama configuration snapshot, enter a Name to identify the configuration, and click OK.
3. Click Export named Panorama configuration snapshot, select the Name of the configuration you just saved, and click OK. Panorama exports the configuration to your client system as an XML file. Save the configuration to a location external to the Panorama appliance.

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

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

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

**STEP 5 | Perform the initial setup of the Panorama virtual appliance.**

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

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

**STEP 6 | Load the Panorama configuration snapshot that you exported from the M-Series appliance into the Panorama virtual appliance.**

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

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

**STEP 7** | Modify the configuration on the Panorama virtual appliance.

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

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

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

*Loading the configuration from the M-Series appliance (Step Load the Panorama configuration snapshot that you exported from the M-Series appliance into the Panorama virtual appliance.) removes the default managed collector and Collector Group that are predefined on each M-Series appliance.*

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

**STEP 9** | Synchronize the Panorama virtual appliance with the firewalls to resume firewall management.

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

1. On the Panorama virtual appliance, select Panorama > Managed Devices and verify that the Device State column displays Connected for the firewalls.

   At this point, the Shared Policy (device groups) and Template columns display Out of sync for the firewalls.

2. Push your changes to device groups and templates:
   1. Select Commit > Push to Devices and Edit Selections.
   2. Select Device Groups, select every device group, Include Device and Network Templates, and click OK.
   3. Push your changes.

3. In the Panorama > Managed Devices page, verify that the Shared Policy and Template columns display In sync for the firewalls.

---

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

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

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

**If you will migrate only the logs and not the Panorama configuration, perform the task**

**Migrate Logs to a New M-Series Appliance in Log Collector Mode** or **Migrate Logs to a New M-Series Appliance in Panorama Mode**.

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

**STEP 1 | Plan the migration.**

- **Upgrade the software** on the M-100 appliance if its current release is earlier than 7.0; the M-500 appliance requires Panorama 7.0 or a later release. For important details about software versions, see Panorama, Log Collector, Firewall, and WildFire Version Compatibility.
- **Forward the System and Config logs** that Panorama and Log Collectors generate to an external destination before the migration if you want to preserve those logs. The M-Series appliance in Panorama mode stores these log types on its SSD, which you cannot move between models. You can move only the RAID drives, which store firewall logs.
- **Schedule a maintenance window for the migration.** Although firewalls can buffer logs after the M-100 appliance goes offline and then forward the logs after the M-500 appliance comes online, completing the migration during a maintenance window minimizes the risk that logs will exceed the buffer capacities and be lost during the transition between Panorama models.

**STEP 2 | Migrate your subscriptions to the new appliance.**

1. Purchase the new support license and migration license.
2. At the time you purchase the new M-500 appliance, provide your sales representative the serial number and device management auth-code of the M-100 appliance you are phasing out, as well as a license migration date of your choosing. On receipt of your M-500 appliance, register the appliance and activate the device management and support licenses using the migration and support auth-codes provided by Palo Alto Networks. On the migration date, the device management license on the M-100 is decommissioned, and you can no longer manage devices or collect logs using the M-100 appliance. However, the support license is preserved and the Panorama appliance remains under support. You can complete the migration after the effective date, but you are unable to commit any configuration changes on the now decommissioned M-100 appliance.

**STEP 3 | Export the Panorama configuration from each M-100 appliance in Panorama mode.**

Perform this task on each M-100 appliance HA peer:

1. Log in to the M-100 appliance and select **Panorama > Setup > Operations**.
2. Click **Save named Panorama configuration snapshot**, enter a **Name** to identify the configuration, and click **OK**.
3. Click **Export named Panorama configuration snapshot**, select the **Name** of the configuration you just saved, and click **OK**. Panorama exports the configuration to your client system as an XML file.

**STEP 4 | Power off each M-100 appliance in Panorama mode.**

1. Log in to the M-100 appliance HA peer that you will power off.
2. Select **Panorama > Setup > Operations**, and click **Shutdown Panorama**.
STEP 5 | Perform the initial setup of each M-500 appliance.
2. Perform Initial Configuration of the M-Series Appliance to define the network connections required to activate licenses and install updates.
3. Register Panorama.
4. Activate a Panorama Support License.
5. Activate a firewall management license. Use the auth-code associated with the migration license.
6. Install Content and Software Updates for Panorama. Install the same versions as those on the M-100 appliance.
7. (Dedicated Log Collector only) Set Up the M-Series Appliance as a Log Collector.

STEP 6 | Load the Panorama configuration snapshot that you exported from each M-100 appliance into each M-500 appliance in Panorama mode (both HA peers).
Perform this task on each M-500 appliance HA peer:
1. Log in to the M-500 appliance and select Panorama > Setup > Operations.
2. Click Import named Panorama configuration snapshot, Browse to the configuration file you exported from the M-100 appliance that has the same HA priority (primary or secondary) as the M-500 appliance will have, and click OK.
3. Click Load named Panorama configuration snapshot, select the Name of the configuration you just imported, select a Decryption Key (the master key for Panorama), and click OK. Panorama overwrites its current candidate configuration with the loaded configuration. Panorama displays any errors that occur when loading the configuration file. If errors occurred, save them to a local file. Resolve each error to ensure the migrated configuration is valid.
4. Select Commit > Commit to Panorama and Validate Commit. Resolve any errors before proceeding.
5. Commit your changes to the Panorama configuration.

STEP 7 | Synchronize the configuration between the M-500 appliance HA peers in Panorama mode.
1. On the active M-500 appliance, select the Dashboard tab and, in the High Availability widget, click Sync to peer.
2. In the High Availability widget, verify that the Local (primary M-500 appliance) is active, the Peer is passive, and the Running Config is synchronized.

STEP 8 | Move the RAID drives from each M-100 appliance to its replacement M-500 appliance to migrate the logs collected from firewalls.
In the following tasks, skip any steps that you already completed on the M-500 appliance.
- Migrate Logs to a New M-Series Appliance in Panorama Mode, Migrate logs from the M-100 appliance only if it uses a default managed collector for log collection.
- Migrate Logs to a New M-Series Appliance in Log Collector Mode.

STEP 9 | Synchronize the active M-500 appliance in Panorama mode with the firewalls to resume firewall management.
Complete this step during a maintenance window to minimize network disruption.
1. In the active M-500 appliance, select Panorama > Managed Devices, and verify that the Device State column displays Connected for the firewalls.
At this point, the Shared Policy (device groups) and Template columns display Out of sync for the firewalls.
2. Push your changes to device groups and templates:
   1. Select Commit > Push to Devices and Edit Selections.
   2. Select Device Groups, select every device group, Include Device and Network Templates, and click OK.
   3. Push your changes.
3. In the Panorama > Managed Devices page, verify that the Shared Policy and Template columns display In sync for the firewalls.
Access and Navigate Panorama Management Interfaces

Panorama provides three management interfaces:

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

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

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

Log in to the Panorama Web Interface

**STEP 1** | Launch an internet browser and enter the Panorama IP address using a secure connection (https://<IP address>).

**STEP 2** | Log in to Panorama according to the type of authentication used for your account. If logging in to Panorama for the first time, use the default value `admin` for your username and password.

- **SAML**—Click Use Single Sign-On (SSO). If Panorama performs authorization (role assignment) for administrators, enter your **Username** and **Continue**. If the SAML identity provider (IdP) performs authorization, **Continue** without entering a **Username**. In both cases, Panorama redirects you to the IdP, which prompts you to enter a username and password. After you authenticate to the IdP, the Panorama web interface displays.

- **Any other type of authentication**—Enter your user **Name** and **Password**. Read the login banner and select I Accept and Acknowledge the Statement Below if the login page has the banner and check box. Then click **Login**.

**STEP 3** | Read and **Close** any messages of the day.

Navigate the Panorama Web Interface

Use the Panorama web interface to configure Panorama, manage and monitor firewalls, Log Collectors, and WildFire appliances and appliance clusters, and access the web interface of each firewall through the **Context** drop-down. Refer to the Panorama online help for details on the options and fields in each web interface tab. The following is an overview of the tabs:
<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>Device Groups &gt; Policies</td>
<td>Create centralized policy rules and apply them to multiple firewalls/device groups. You must Add a Device Group for this tab to display.</td>
</tr>
<tr>
<td>Device Groups &gt; Objects</td>
<td>Define policy objects that policy rules can reference and that managed firewalls/device groups can share. You must Add a Device Group for this tab to display.</td>
</tr>
<tr>
<td>Templates &gt; Network</td>
<td>Configure network setting, such as network profiles, and apply them to multiple firewalls. You must Add a Template for this tab to display.</td>
</tr>
<tr>
<td>Templates &gt; Device</td>
<td>Configure device settings, such as server profiles and admin roles, and apply them to multiple firewalls. You must Add a Template for this tab to display.</td>
</tr>
<tr>
<td>Panorama</td>
<td>Configure Panorama, manage licenses, set up high availability, access software updates and security alerts, manage administrative access, and manage the deployed firewalls, Log Collectors, and WildFire appliances and appliance clusters.</td>
</tr>
</tbody>
</table>

Log in to the Panorama CLI

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

- Use SSH to log in to the Panorama CLI.

  The same instructions apply to an M-Series appliance in Log Collector mode.

  Optionally, you can Configure an Administrator with SSH Key-Based Authentication for the CLI.

1. Ensure the following prerequisites are met:
   - You have a computer with network access to Panorama.
   - You know the Panorama IP address.
   - The Management interface supports SSH, which is the default setting. If an administrator disabled SSH and you want to re-enable it: select Panorama > Setup > Interfaces, click Management,
select SSH, click OK, select Commit > Commit to Panorama, and Commit your changes to the Panorama configuration.

2. To access the CLI using SSH:
   1. Enter the Panorama IP address in the SSH client and use port 22.
   2. Enter your administrative access credentials when prompted. After you log in, the message of the day displays, followed by the CLI prompt in Operational mode. For example:

   admin@ABC_Sydney>

   • Use a serial port connection to log in to the Panorama CLI.
     1. Make sure that you have the following:
        • A null-modem serial cable that connects Panorama to a computer with a DB-9 serial port
        • A terminal emulation program running on the computer
     2. Use the following settings in the terminal emulation software to connect: 9600 baud; 8 data bits; 1 stop bit; No parity; No hardware flow control.
     3. Enter your administrative access credentials when prompted. After you log in, the message of the day displays, followed by the CLI prompt in Operational mode.

   • Change to Configuration mode.
     To switch to Configuration mode, enter the following command at the prompt:

   admin@ABC_Sydney> configure

   The prompt changes to admin@ABC_Sydney#.
Set Up Administrative Access to Panorama

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

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

Configure an Admin Role Profile

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

**STEP 1 | Select Panorama > Admin Roles and click Add.**

**STEP 2 | Enter a Name for the profile and select the Role type: Panorama or Device Group and Template.**

**STEP 3 | Configure access privileges to each functional area of Panorama (Web UI) and firewalls (Context Switch UI) by toggling the icons to the desired setting: Enable (read-write), Read Only, or Disable.**

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

You cannot manage access to the firewall CLI or XML API through context-switching privileges in Panorama roles.

**STEP 4 | If the Role type is Panorama, configure access to the XML API by toggling the Enabled/Disabled icon for each functional area.**

**STEP 5 | If the Role type is Panorama, select an access level for the Command Line interface: None (default), superuser, superreader, or panorama-admin.**

**STEP 6 | Click OK to save the profile.**

Configure an Access Domain

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

**STEP 1 | Select Panorama > Access Domain and click Add.**

**STEP 2 | Enter a Name to identify the access domain.**
STEP 3 | Select an access privilege for Shared Objects:

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

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

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

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

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

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

Configure Administrative Accounts and Authentication

If you have already configured an authentication profile or you don’t require one to authenticate administrators, you are ready to Configure a Panorama Administrator Account. Otherwise, perform one of the other procedures listed below to configure administrative accounts for specific types of authentication.

- Configure a Panorama Administrator Account
- Configure Local or External Authentication for Panorama Administrators
- Configure a Panorama Administrator with Certificate-Based Authentication for the Web Interface
- Configure an Administrator with SSH Key-Based Authentication for the CLI
- Configure RADIUS Authentication for Panorama Administrators
- Configure TACACS+ Authentication for Panorama Administrators
- Configure SAML Authentication for Panorama Administrators

**Configure a Panorama Administrator Account**

Administrative accounts specify Administrative Roles and authentication for Panorama administrators. The service that you use to assign roles and perform authentication determines whether you add the accounts on Panorama, on an external server, or both (see Administrative Authentication). For an external authentication service, you must configure an authentication profile before adding an administrative account (see Configure Administrative Accounts and Authentication). If you already configured the authentication profile or you will use the authentication mechanism that is local to Panorama, perform the following steps to add an administrative account on Panorama.

You can’t add an administrator account to a Dedicated Log Collector (M-Series appliance in Log Collector mode). Only the predefined administrator account with the default username (admin) is available on Dedicated Log Collectors.
STEP 1 | Select Panorama > Administrators and Add an account.

STEP 2 | Enter a user Name for the administrator.

STEP 3 | Select an Authentication Profile or sequence if you configured either for the administrator. This is required if Panorama will use Kerberos SSO or an external service for authentication. If Panorama will use local authentication, set the Authentication Profile to None and enter a Password and then Confirm Password.

STEP 4 | Select the Administrator Type:
- Dynamic—Select a predefined administrator role.
- Custom Panorama Admin—Select the Admin Role Profile you created for this administrator (see Configure an Admin Role Profile).
- Device Group and Template Admin—Map access domains to administrative roles as described in the next step.

STEP 5 | (Device Group and Template Admin only) In the Access Domain to Administrator Role section, click Add, select an Access Domain from the drop-down (see Configure an Access Domain), click the adjacent Admin Role cell, and select an Admin Role profile.

STEP 6 | Click OK to save your changes.

STEP 7 | Select Commit > Commit to Panorama and Commit your changes.

Configure Local or External Authentication for Panorama Administrators

You can use an external authentication service or the service that is local to Panorama to authenticate administrators who access Panorama. These authentication methods prompt administrators to respond to one or more authentication challenges, such as a login page for entering a username and password.

If you use an external service to manage both authentication and authorization (role and access domain assignments), see:
- Configure RADIUS Authentication for Panorama Administrators
- Configure TACACS+ Authentication for Panorama Administrators
- Configure SAML Authentication for Panorama Administrators

To authenticate administrators without a challenge-response mechanism, you can Configure a Panorama Administrator with Certificate-Based Authentication for the Web Interface and Configure an Administrator with SSH Key-Based Authentication for the CLI.

STEP 1 | (External authentication only) Enable Panorama to connect to an external server for authenticating administrators.

1. Select Panorama > Server Profiles, select the service type (RADIUS, TACACS+, SAML, LDAP, or Kerberos), and configure a server profile:
   - Configure RADIUS Authentication for Panorama Administrators.
• Configure TACACS+ Authentication for Panorama Administrators.
• Add a SAML IdP server profile. You cannot combine Kerberos single sign-on (SSO) with SAML SSO; you can use only one type of SSO service.
• Add a Kerberos server profile.
• Add a LDAP Server Profile.

STEP 2 | (Optional) Define password complexity and expiration settings if Panorama uses local authentication.
These settings help protect Panorama against unauthorized access by making it harder for attackers to guess passwords.
1. Define global password complexity and expiration settings for all local administrators.
   2. Select Enabled.
   3. Define the password settings and click OK.
2. Define a Password Profile.
   You assign the profile to administrator accounts for which you want to override the global password expiration settings.
   1. Select Panorama > Password Profiles and Add a profile.
   2. Enter a Name to identify the profile.
   3. Define the password expiration settings and click OK.

STEP 3 | (Kerberos SSO only) Create a Kerberos keytab.
A keytab is a file that contains Kerberos account information for Panorama. To support Kerberos SSO, your network must have a Kerberos infrastructure.

STEP 4 | Configure an authentication profile.
If your administrative accounts are stored across multiple types of servers, you can create an authentication profile for each type and add all the profiles to an authentication sequence.
In the authentication profile, specify the Type of authentication service and related settings:
• External service—Select the Type of external service and select the Server Profile you created for it.
• Local authentication—Set the Type to None.
• Kerberos SSO—Specify the Kerberos Realm and Import the Kerberos Keytab you created.

STEP 5 | (Device group and template administrators only) Configure an Access Domain.
Configure one or more access domains.

STEP 6 | (Custom roles only) Configure an Admin Role Profile.
Configure one or more Admin Role profiles.
For custom Panorama administrators, the profile defines access privileges for the account. For device group and template administrators, the profile defines access privileges for one or more access domains associated with the account.

STEP 7 | Configure an administrator.
1. Configure a Panorama Administrator Account.
Configure a Panorama Administrator with Certificate-Based Authentication for the Web Interface

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

Configuring certificate-based authentication for any administrator disables the username/password logins for all administrators on Panorama and all administrators thereafter require the certificate to log in.

STEP 1 | Generate a certificate authority (CA) certificate on Panorama.
You will use this CA certificate to sign the client certificate of each administrator.
Create a self-signed root CA certificate.

Alternatively, you can import a certificate from your enterprise CA.

STEP 2 | Configure a certificate profile for securing access to the web interface.
2. Enter a Name for the certificate profile and set the Username Field to Subject.
3. Select Add in the CA Certificates section and select the CA Certificate you just created.
4. Click OK to save the profile.

STEP 3 | Configure Panorama to use the certificate profile for authenticating administrators.
1. Select the Panorama > Setup > Management and edit the Authentication Settings.
2. Select the Certificate Profile you just created and click OK.

STEP 4 | Configure the administrator accounts to use client certificate authentication.
Configure a Panorama Administrator Account for each administrator who will access the Panorama web interface. Select the Use only client certificate authentication (Web) check box.

If you have already deployed client certificates that your enterprise CA generated, skip to Step 8. Otherwise, continue with Step 5.

STEP 5 | Generate a client certificate for each administrator.
Generate a certificate on Panorama. In the Signed By drop-down, select the CA certificate you created.

STEP 6 | Export the client certificates.
1. Export the certificates.
2. Select Commit > Commit to Panorama and Commit your changes.
Panorama restarts and terminates your login session. Thereafter, administrators can access the web interface only from client systems that have the client certificate you generated.

**STEP 7 |** Import the client certificate into the client system of each administrator who will access the web interface.

Refer to your web browser documentation as needed to complete this step.

**STEP 8 |** Verify that administrators can access the web interface.

1. Open the Panorama IP address in a browser on the computer that has the client certificate.
2. When prompted, select the certificate you imported and click **OK**. The browser displays a certificate warning.
3. Add the certificate to the browser exception list.
4. Click **Login**. The web interface should appear without prompting you for a username or password.

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

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

**STEP 1 |** Use an SSH key generation tool to create an asymmetric key pair on the client system of the administrator.

The supported key formats are IETF SECSH and Open SSH. The supported algorithms are DSA (1024 bits) and RSA (768-4096 bits).

For the commands to generate the key pair, refer to your SSH client documentation.

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

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

1. Configure a Panorama Administrator Account.
   - Configure one of two authentication methods to use as a fallback if SSH key authentication fails:
     - **External authentication service**—Select an **Authentication Profile**.
     - **Local authentication**—Set the **Authentication Profile** to **None** and enter a **Password** and **Confirm Password**.
   - Select the **Use Public Key Authentication (SSH)** check box, click **Import Key**, **Browse** to the public key you just generated, and click **OK**.
2. Click **OK** to save the administrative account.
3. Select **Commit > Commit to Panorama** and **Commit** your changes.

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

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

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

1. Use a browser on the client system of the administrator to go to the Panorama IP address.
2. Log in to the Panorama CLI as the administrator. After entering a username, you will see the following output (the key value is an example):

   Authenticating with public key “dsa-key-20130415”

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

Configure RADIUS Authentication for Panorama Administrators

You can use a RADIUS server to authenticate administrative access to the Panorama web interface. You can also define Vendor-Specific Attributes (VSAs) on the RADIUS server to manage administrator authorization. Using VSAs enables you to quickly change the roles, access domains, and user groups of administrators through your directory service, which is often easier than reconfiguring settings on Panorama.

You can Import the Palo Alto Networks RADIUS dictionary into RADIUS server to define the authentication attributes needed for communication between Panorama and the RADIUS server.

You can also use a RADIUS server to implement multi-factor authentication (MFA) for administrators.

STEP 1 | Add a RADIUS server profile.

   The profile defines how Panorama connects to the RADIUS server.

1. Select Panorama > Server Profiles > RADIUS and Add a profile.
2. Enter a Profile Name to identify the server profile.
3. Enter a Timeout interval in seconds after which an authentication request times out (range is 1-20; default is 3).

   If you use the server profile to integrate Panorama with an MFA service, enter an interval that gives administrators enough time to respond to the authentication challenge. For example, if the MFA service prompts for a one-time password (OTP), administrators need time to see the OTP on their endpoint device and then enter the OTP in the MFA login page.

4. Select the Authentication Protocol (default is CHAP) that Panorama uses to authenticate to the RADIUS server.

   Select CHAP if the RADIUS server supports that protocol; it is more secure than PAP.

5. Add each RADIUS server and enter the following:
   - Name to identify the server
   - RADIUS Server IP address or FQDN
   - Secret/Confirm Secret (a key to encrypt usernames and passwords)
   - Server Port for authentication requests (default is 1812)

6. Click OK to save the server profile.

STEP 2 | Assign the RADIUS server profile to an authentication profile.

   The authentication profile defines authentication settings that are common to a set of administrators.

1. Select Panorama > Authentication Profile and Add a profile.
2. Enter a Name to identify the authentication profile.
3. Set the Type to RADIUS.
4. Select the Server Profile you configured.
5. Select **Retrieve user group from RADIUS** to collect user group information from VSAs defined on the RADIUS server.
   Panorama matches the group information against the groups you specify in the Allow List of the authentication profile.

6. Select **Advanced** and, in the Allow List, **Add** the administrators that are allowed to authenticate with this authentication profile.

7. Click **OK** to save the authentication profile.

**STEP 3** | Configure Panorama to use the authentication profile for all administrators.

1. Select **Panorama > Setup > Management** and edit the Authentication Settings.
2. Select the **Authentication Profile** you configured and click **OK**.

**STEP 4** | Configure the roles and access domains that define authorization settings for administrators.

1. **Configure an Admin Role Profile** if the administrator uses a custom role instead of a predefined (dynamic) role.
2. **Configure an Access Domain** if the administrator uses a Device Group and Template role.

**STEP 5** | Commit your changes.

Select **Commit > Commit to Panorama** and **Commit** your changes.

**STEP 6** | Configure the RADIUS server.

Refer to your RADIUS server documentation for the specific instructions to perform these steps:

1. Add the Panorama IP address or hostname as the RADIUS client.
2. Add the administrator accounts.

   *If the RADIUS server profile specifies CHAP as the Authentication Protocol, you must define accounts with reversibly encrypted passwords. Otherwise, CHAP authentication will fail.*

3. Define the vendor code for Panorama (25461) and define the RADIUS VSAs for the role, access domain, and user group of each administrator.

   For detailed instructions, refer to the following Knowledge Base articles:
   - For Windows 2003 Server, Windows 2008 (and later), and Cisco Secure Access Control Server (ACS) 4.0—**RADIUS Vendor-Specific Attributes (VSAs)**
   - For Cisco ACS 5.2—**Configuring Cisco ACS 5.2 for use with Palo AltoVSA**

**STEP 7** | Verify that the RADIUS server performs authentication and authorization for administrators.

1. Log in the Panorama web interface using an administrator account that you added to the RADIUS server.
2. Verify that you can access only the web interface pages that are allowed for the role you associated with the administrator.
3. In the **Monitor**, **Policies**, and **Objects** tabs, verify that you can access only the device groups that are allowed for the access domain you associated with the administrator.

**Configure TACACS+ Authentication for Panorama Administrators**

You can use a **TACACS+** server to authenticate administrative access to the Panorama web interface. You can also define **Vendor-Specific Attributes (VSAs)** on the TACACS+ server to manage administrator authorization. Using VSAs enables you to quickly change the roles, access domains, and user groups.
of administrators through your directory service, which is often easier than reconfiguring settings on Panorama.

**STEP 1 | Add a TACACS+ server profile.**

The profile defines how Panorama connects to the TACACS+ server.

1. Select **Panorama > Server Profiles > TACACS+** and **Add** a profile.
2. Enter a **Profile Name** to identify the server profile.
3. Enter a **Timeout** interval in seconds after which an authentication request times out (default is 3; range is 1–20).
4. Select the **Authentication Protocol** (default is **CHAP**) that Panorama uses to authenticate to the TACACS+ server.

   *Select CHAP if the TACACS+ server supports that protocol; it is more secure than PAP.*

5. **Add** each TACACS+ server and enter the following:
   - **Name** to identify the server
   - **TACACS+ Server** IP address or FQDN
   - **Secret/Confirm Secret** (a key to encrypt usernames and passwords)
   - **Server Port** for authentication requests (default is 49)
6. Click **OK** to save the server profile.

**STEP 2 | Assign the TACACS+ server profile to an authentication profile.**

The authentication profile defines authentication settings that are common to a set of administrators.

1. Select **Panorama > Authentication Profile** and **Add** a profile.
2. Enter a **Name** to identify the profile.
3. Set the **Type** to **TACACS+**.
4. Select the **Server Profile** you configured.
5. Select **Retrieve user group from TACACS+** to collect user group information from VSAs defined on the TACACS+ server.

   Panorama matches the group information against the groups you specify in the Allow List of the authentication profile.

6. Select **Advanced** and, in the Allow List, **Add** the administrators that are allowed to authenticate with this authentication profile.
7. Click **OK** to save the authentication profile.

**STEP 3 | Configure Panorama to use the authentication profile for all administrators.**

1. Select **Panorama > Setup > Management** and edit the Authentication Settings.
2. Select the **Authentication Profile** you configured and click **OK**.

**STEP 4 | Configure the roles and access domains that define authorization settings for administrators.**

1. **Configure an Admin Role Profile** if the administrator will use a custom role instead of a predefined (dynamic) role.
2. **Configure an Access Domain** if the administrator uses a Device Group and Template role.

**STEP 5 | Commit your changes.**

Select **Commit > Commit to Panorama** and **Commit** your changes.

**STEP 6 | Configure the TACACS+ server to authenticate and authorize administrators.**
Refer to your TACACS+ server documentation for the specific instructions to perform these steps:

1. Add the Panorama IP address or hostname as the TACACS+ client.
2. Add the administrator accounts.

   \textit{If you selected CHAP as the Authentication Protocol, you must define accounts with reversibly encrypted passwords. Otherwise, CHAP authentication will fail.}
3. Define TACACS+ VSAs for the role, access domain, and user group of each administrator.

**STEP 7** | Verify that the TACACS+ server performs authentication and authorization for administrators.

1. Log in the Panorama web interface using an administrator account that you added to the TACACS+ server.
2. Verify that you can access only the web interface pages that are allowed for the role you associated with the administrator.
3. In the **Monitor**, **Policies**, and **Objects** tabs, verify that you can access only the virtual systems that are allowed for the access domain you associated with the administrator.

**Configure SAML Authentication for Panorama Administrators**

You can use Security Assertion Markup Language (SAML) 2.0 for administrative access to the Panorama web interface (but not the CLI). You can also use SAML attributes to manage administrator authorization. SAML attributes enable you to quickly change the roles, access domains, and user groups of administrators through your directory service instead of reconfiguring settings on Panorama.

To configure SAML single sign-on (SSO) and single logout (SLO), you must register Panorama and the IdP with each other to enable communication between them. If the IdP provides a metadata file containing registration information, you can import it onto Panorama to register the IdP and to create an IdP server profile. The server profile defines how to connect to the IdP and specifies the certificate that the IdP uses to sign SAML messages. You can also use a certificate for Panorama to sign SAML messages. Using certificates is optional but recommended to secure communications between Panorama and the IdP.

**STEP 1** | (Recommended) Obtain the certificates that the IdP and Panorama will use to sign SAML messages.

   If the certificates don't specify key usage attributes, all usages are allowed by default, including signing messages. In this case, you can obtain certificates by any method.

   If the certificates do specify key usage attributes, one of the attributes must be Digital Signature, which is not available on certificates that you generate on Panorama. In this case, you must import the certificates:

   - **Certificate Panorama uses to sign SAML messages**—Import the certificate from your enterprise certificate authority (CA) or a third-party CA.
   - **Certificate the IdP uses to sign SAML messages**—Import a metadata file containing the certificate from the IdP (see the next step). The IdP certificate is limited to the following algorithms:
     - **Public key algorithms**—RSA (1,024 bits or larger) and ECDSA (all sizes).
     - **Signature algorithms**—SHA1, SHA256, SHA384, and SHA512.

**STEP 2** | Add a SAML IdP server profile.

The server profile registers the IdP with Panorama and defines how they connect.

In this example, you import a SAML metadata file from the IdP so that Panorama can automatically create a server profile and populate the connection, registration, and IdP certificate information.
1. Export the SAML metadata file from the IdP to a client system that Panorama can access.
   The certificate specified in the file must meet the requirements listed in the preceding step. Refer to your IdP documentation for instructions on exporting the file.
2. Select Panorama > Server Profiles > SAML Identity Provider and Import the metadata file onto Panorama.
3. Enter a Profile Name to identify the server profile.
5. (Recommended) Select Validate Identity Provider Certificate (default) to have Panorama validate the Identity Provider Certificate. Validation occurs only after you assign the server profile to an authentication profile and Commit. Panorama uses the Certificate Profile in the authentication profile to validate the certificate.

Validating the certificate is a best practice for improved security.

6. Enter the Maximum Clock Skew, which is the allowed difference in seconds between the system times of the IdP and Panorama at the moment when Panorama validates IdP messages (default is 60; range is 1 to 900). If the difference exceeds this value, authentication fails.
7. Click OK to save the server profile.
8. Click the server profile Name to display the profile settings. Verify that the imported information is correct and edit it if necessary.

STEP 3 | Configure an authentication profile.

The authentication profile specifies a SAML IdP server profile and defines options for the authentication process, such as SLO.
1. Select Panorama > Authentication Profile and Add a profile.
2. Enter a Name to identify the profile.
3. Set the Type to SAML.
4. Select the IdP Server Profile you configured.
5. Select the Certificate for Signing Requests.

Panorama uses this certificate to sign messages it sends to the IdP.
6. (Optional) Enable Single Logout (disabled by default).
7. Select the Certificate Profile that Panorama will use to validate the Identity Provider Certificate.
8. Enter the Username Attribute that IdP messages use to identify users (default username).

If you manage administrator authorization through the IdP identity store, specify the Admin Role Attribute and Access Domain Attribute also.
9. Select Advanced and Add the administrators who are allowed to authenticate with this authentication profile.
10. Click OK to save the authentication profile.

STEP 4 | Configure Panorama to use the authentication profile for all administrators.
1. Select Panorama > Setup > Management, edit the Authentication Settings, and select the Authentication Profile you configured.
2. Select **Commit > Commit to Panorama** to activate your changes on Panorama and to validate the **Identity Provider Certificate** that you assigned to the SAML IdP server profile.

**STEP 5 | Create a SAML metadata file to register Panorama on the IdP.**

1. Select **Panorama > Authentication Profile** and, in the Authentication column for the authentication profile you configured, click **Metadata**.
2. Set the **Management Choice** to **Interface** (default is selected) and select the management (MGT) interface.
3. Click **OK** and save the metadata file to your client system.
4. Import the metadata file into the IdP server to register Panorama. Refer to your IdP documentation for instructions.

**STEP 6 | Verify that administrators can authenticate using SAML SSO.**

1. Go to the URL of the Panorama web interface.
2. Click **Use Single Sign-On**.
3. Click **Continue**.

   Panorama redirects you to authenticate to the IdP, which displays a login page. For example:

   ![Login Page Screenshot]

4. Log in using your SSO username and password.
   After you successfully authenticate on the IdP, it redirects you back to Panorama, which displays the web interface.
5. Use your Panorama administrator account to request access to another SSO application.
   Successful access indicates SAML SSO authentication succeeded.
Set Up Authentication Using Custom Certificates

By default, Panorama, firewalls, and Log Collectors use predefined certificates for mutual authenticate to establish the SSL connections used for management access and inter-device communication. However, you can configure authentication using custom certificates instead. Additionally, you can use custom certificates to secure the High Availability (HA) connections between Panorama HA peers. Custom certificates allow you to establish a unique chain of trust to ensure mutual authentication between Panorama and the managed firewalls and log collectors. See Certificate Management for detailed information about the certificates and how to deploy them on Panorama, Log Collectors, and firewalls.

The following topics describe how to configure Panorama to use custom certificate and how to manage those certificates.

- How Are SSL/TLS Connections Mutually Authenticated?
- Configure Authentication Using Custom Certificates on Panorama
- Configure Authentication Using Custom Certificates on Managed Devices
- Add New Client Devices
- Change Certificates

How Are SSL/TLS Connections Mutually Authenticated?

In a regular SSL connection, only the server need to identify itself to the client by presenting its certificate. However, in mutual SSL authentication, the client presents its certificate to the server as well. Panorama and Log Collectors can act as the server. Firewalls, Log Collectors, and the secondary Panorama HA peer can act as the client. The role that a device takes on depends the deployment. For example, in the diagram below, Panorama manages a number of firewalls and a collector group and acts as the server for the firewalls and Log Collectors. The Log Collector acts as the server to the firewalls that send logs to it.

To deploy custom certificates for mutual authentication in your deployment, you need:

- **SSL/TLS Service Profile**—An SSL/TLS service profile defines the security of the connections by referencing your custom certificate and establishing the of SSL/TLS protocol versions used by Panorama or Log Collector to communicate with client devices.

- **Server Certificate and Profile**—Panorama and Log Collectors in the server role require a certificate and certificate profile to identify themselves to the client devices. You can deploy this certificate from your enterprise public key infrastructure (PKI), purchase one from a trusted third-party CA, or generate a self-signed certificate locally. The server certificate must include the IP address or FQDN of the Panorama management interface in the certificate common name (CN) or Subject Alt Name. The client firewall or Log Collector matches the CN or Subject Alt Name in the certificate the server presents against the server’s IP address or FQDN to verify the server’s identity.

  Additionally, use the certificate profile to define certificate revocation status (OCSP/CRL) and the actions taken based on the revocation status.

- **Client Certificates and Profile**—Each managed device requires a client certificates and certificate profile. The firewall or Log Collector uses its certificate to identify itself to Panorama or server Log Collector. You can deploy certificates from your enterprise PKI using Simple Certificate Enrollment Protocol (SCEP), purchase one from a trusted third-party CA, or generate a self-signed certificate locally.

  Custom certificates can be unique to each managed device or common across all devices. The unique device certificates uses a hash of the serial number of the managed device and CN. Set the CN or certificate signing request (CSR) to the special keyword $UDID and the generated certificate or CSR contains a hash of the firewall serial number as the Subject. Panorama matches the CN or the subject alt name against the configured serial numbers of the managed devices. For client certificate validation
based on the CN to occur, the Username must be set to Subject common-name. The client certificate behavior also applies to Panorama HA peer connections.

You can configure the client certificate and certificate profile on each client device or push the configuration from Panorama to each device as part of a template.

Configure Authentication Using Custom Certificates on Panorama

Complete the following procedure to configure the server side (Panorama) to use custom certificates instead of predefined certificates for mutual authentication with managed devices in your deployment. See Set Up Authentication Using Custom Certificates Between HA Peers to configure custom certificates on a Panorama HA pair.

**STEP 1 |** Deploy the server certificate.

You can **deploy certificates** on Panorama or a server Log Collector by generating a self-signed certificate on Panorama or obtaining a certificate from your enterprise CA or a trusted third-party CA.

**STEP 2 |** On Panorama, configure a certificate profile This certificate profile defines what certificate to use and what certificate field to look for the IP address or FQDN in.

1. Select **Panorama > Certificate Management > Certificate Profile**.
2. **Configure a certificate profile**.

   *If you configure an intermediate CA as part of the certificate profile, you must include the root CA as well.*

**STEP 3 |** Configure an SSL/TLS service profile.

1. Select **Panorama > Certificate Management > SSL/TLS Service Profile**.
2. **Configure an SSL/TLS profile** to define the certificate and protocol that Panorama and its managed devices use for SSL/TLS services.
**STEP 4 |** Configure Secure Server Communication on Panorama or a Log Collector in the server role.

1. Select one of the following navigation paths:
   - For Panorama: Panorama > Setup > Management and Edit the Panorama Settings
   - For a Log Collector: Panorama > Managed Collectors > Add > Communication

2. Verify that the **Allow Custom Certificate Only** check box is not selected. This allows you to continue managing all devices while migrating to custom certificates.

   *When the Custom Certificate Only check box is selected, Panorama does not authenticate and cannot manage devices using predefined certificates.*

3. Select the **SSL/TLS Service Profile**. This SSL/TLS service profile applies to all SSL connections between Panorama, firewalls, Log Collectors, and Panorama HA peers.

4. Select the **Certificate Profile** that identifies the certificate to use to establish secure communication with clients such as firewalls.

5. *(Optional)* Configure an authorization list. The authorization list adds an additional layer of security beyond certificate authentication. The authorization list checks the client certificate Subject or Subject Alt Name. If the Subject or Subject Alt Name presented with the client certificate does not match an identifier on the authorization list, authentication is denied.

   You can also authorize client devices based on their serial number.

   1. **Add** an Authorization List.
   2. Select the **Subject** or **Subject Alt Name** configured in the certificate profile as the Identifier type.
   3. Enter the Common Name if the identifier is Subject or and IP address, hostname or email if the identifier is Subject Alt Name.
   4. Click **OK**.
   5. Select **Check Authorization List** to enforce the authorization list.
   6. Select **Authorize Client Based on Serial Number** to have the server authenticate client based on the serial numbers of managed devices. The CN or subject in the client certificate must have the special keyword $UDID to enable this type of authentication.
   7. In **Disconnect Wait Time (min)**, specify how long Panorama should wait before terminating the current session and reestablishing the connection with its managed devices. This field is blank by default and the range is 0 to 44,640 minutes. Leaving this field blank is the same as setting it to 0.

   *The disconnect wait time does not begin counting down until you commit the new configuration.*

8. Click **OK**.
9. **Commit** your changes.

### Configure Authentication Using Custom Certificates on Managed Devices

Complete the following procedure to configure the client side (firewall or Log Collector) to use custom certificates instead of predefined certificates for mutual authentication with managed devices in your deployment.

**STEP 1 |** Upgrade each managed firewall or Log Collector. All managed devices must be running PAN-OS 8.0 or later to enforce custom certificate authentication.

Upgrade the firewall to PAN-OS 8.0 or later. After upgrade, each firewall connects to Panorama using the default predefined certificates.

**STEP 2 |** Obtain or generate the device certificate.
You can deploy certificates on Panorama or a server Log Collector by generating a self-signed certificate on Panorama or obtaining a certificate from your enterprise CA or a trusted third-party CA.

Set the common name to $UDID or subject to CN=$UDID (in the SCEP profile) if authorizing client devices based on serial number.

- You can generate a self-signed certificate on Panorama or obtain a certificate from your enterprise CA or a trusted third-party CA.
- If you are using SCEP for the device certificate, configure a SCEP profile. SCEP allows you to automatically deploy certificates to managed devices. When a new client devices with a SCEP profile attempts to authenticate with Panorama, the certificate is sent by the SCEP server to the device.

**STEP 3 |** Configure the certificate profile for the client device.

You can configure this on each client device individually or you can push this configuration to the managed device as part of a template.

1. Select one of the following navigation paths:
2. Configure the certificate profile.

**STEP 4 |** Deploy custom certificates on each firewall or Log Collector.

1. Select one of the following navigation paths:
   - For firewalls: Select Device > Setup > Management and Edit the Panorama Settings
   - For Log Collectors: Select Panorama > Managed Collectors and Add a new Log Collector or select an existing one. Select Communication.
2. Select the Secure Client Communication check box (firewall only).
3. Select the Certificate Type.
   - If you are using a local device certificate, select the Certificate and Certificate Profile.
   - If you are using SCEP to deploy device certificate, select the SCEP Profile and Certificate Profile.
4. (Optional) Enable Check Server Identity. The firewall or Log Collector checks the CN in the server certificate against Panorama's IP address or FQDN to verify its identity.
5. Click OK.
6. Commit your changes.

After committing your changes, the managed device does not terminate its current session with Panorama until the Disconnect Wait Time is complete.

**STEP 5 |** After deploying custom certificates on all managed devices, enforce authentication using custom certificates.

*The WildFire appliance does not currently support custom certificates. If your Panorama is managing a WildFire appliance, do not select Allow Custom Certificates Only.*

1. Select Panorama > Setup > Management and Edit the Panorama settings.
2. Select Allow Custom Certificate Only.
3. Click OK.
4. Commit your changes.

After committing this change, all devices managed by Panorama must use custom certificates. If not, authentication between Panorama and the device fails.
Add New Client Devices

When adding a new firewall or Log Collector to Panorama, the workflow depends on whether or not these devices are configured to use custom certificates only for mutual authentication.

- If the Custom Certificates Only is not selected on Panorama, you can add the device to Panorama and then deploy the custom certificate by following the process beginning in step Configure Authentication Using Custom Certificates on Managed Devices.
- If the Custom Certificates Only is selected on Panorama, you must deploy the custom certificates on the firewall before adding it to Panorama. If not, the managed device will not be able to authenticate with Panorama. This can be done manually through the firewall web interface or through bootstrapping as part of the bootstrap.xml file.

Change Certificates

If a custom certificate in your deployment has expired or been revoked and needs to be replaced, you can complete one of the tasks below.

- Change a Server Certificate
- Change a Client Certificate
- Change a Root or Intermediate CA Certificate

Change a Server Certificate

Complete the following task to replace a server certificate.

STEP 1 | Deploy the new server certificate.

You can deploy certificates on Panorama or a server Log Collector by generating a self-signed certificate on Panorama or obtaining a certificate from your enterprise CA or a trusted third-party CA.

STEP 2 | Change the certificate in the SSL/TLS Service Profile.

1. Select Panorama > Certificate Management > SSL/TLS Service Profile and select the SSL/TLS service profile.
2. Select the Certificate.
3. Click OK.

STEP 3 | Reestablish the connection between the server (Panorama or a Log Collector) and client devices.

1. Select Panorama > Setup > Management and Edit the Panorama Settings for Panorama or select Panorama > Managed Collectors > Add > Communication for a Log Collector.
2. Set the Disconnect Wait Time.
3. Click OK.
4. Commit your changes.

Change a Client Certificate

Complete the following task to replace a client certificate.

STEP 1 | Obtain or generate the device certificate.

You can deploy certificates on Panorama or a server Log Collector by generating a self-signed certificate on Panorama or obtaining a certificate from your enterprise CA or a trusted third-party CA.

Set the common name to $UDID or subject to CN=$UDID (in the SCEP profile) if authorizing client devices based on serial number.
• You can generate a self-signed certificate on Panorama or obtain a certificate from your enterprise CA or a trusted third-party CA.
• If you are using SCEP for the device certificate, configure a SCEP profile. SCEP allows you to automatically deploy certificates to managed devices. When a new client devices with a SCEP profile attempts to authenticate with Panorama, the certificate is sent by the SCEP server to the device.

STEP 2 | Change the certificate in the certificate profile.
2. Under CA Certificates, Add the new certificate to assign to the certificate profile.
3. Click OK.
4. Commit your changes.

Change a Root or Intermediate CA Certificate

Complete the following task to replace a root or intermediate CA certificate.

STEP 1 | Configure the server to accept predefined certificates from clients.
1. Select Panorama > Setup > Management and Edit the Panorama Settings.
2. Uncheck Custom Certificate Only.
4. Click OK.
5. Commit your changes.

STEP 2 | Deploy the new root or intermediate CA certificate.
You can deploy certificates on Panorama or a server Log Collector by generating a self-signed certificate on Panorama or obtaining a certificate from your enterprise CA or a trusted third-party CA.

STEP 3 | Update the CA certificate in the server certificate profile.
2. Delete the old CA certificate.
3. Add the new CA Certificate.
4. Click OK.

STEP 4 | Generate or import the new client certificate.
1. Select Device > Certificate Management > Certificates.
2. Create a self-signed root CA certificate or import a certificate from your enterprise CA.

STEP 5 | Update the CA certificate in the client certificate profile.
1. Select Device > Setup > Management and click the Edit icon in Panorama Settings for a firewall or Select Panorama > Managed Collectors > Add > Communication for a Log Collector and select the certificate profile to update.
2. Delete the old CA certificate.
3. Add the new CA Certificate.
4. Click OK.

STEP 6 | After updating the CA certificates on all managed devices, enforce custom-certificate authentication.
1. Select Panorama > Setup > Management and Edit the Panorama Settings.
2. Select Custom Certificate Only.
3. Click OK.
4. **Commit** your changes.

   After committing this change, all devices managed by Panorama must use custom certificates. If not, authentication between Panorama and the device fails.
Manage Firewalls

To use the Panorama™ management server 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 Panorama Deployment to understand the deployment options.

- Add a Firewall as a Managed Device
- Manage Device Groups
- Manage Templates and Template Stacks
- Redistribute User-ID Information to Managed Firewalls
- 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 managing your firewalls, you will need to enable a connection between the firewall and Panorama. This connection requires you enter the Panorama IP address on each firewall that will be managed, and to enter the serial number of each firewall on Panorama.

The firewall uses the Panorama server IP address to set up an SSL connection to register with Panorama. Panorama and the firewall authenticate each other using 2,048-bit certificates and AES-256 encrypted SSL connections for configuration management and log collection. Prepare Panorama, and each firewall as follows:

**STEP 1 |** Configure the firewall to communicate with Panorama.

Repeat this step for each firewall Panorama will manage.

1. **Perform initial configuration** on the firewall so that it is accessible and can communicate with Panorama over the network.
2. **Configure each data interface** you plan to use on the firewall and attach it to a security zone so that you can push configuration and policy from Panorama.
3. Add the Panorama IP address to the firewall.
   1. Select **Device > Setup > Management** and edit the Panorama Settings.
   2. Enter the Panorama IP address in the first field.
   3. **(Optional)** If you have set up a High Availability pair in Panorama, enter the IP address of the secondary Panorama in the second field.
   4. Click **OK**.
   5. Select **Commit** and **Commit** your changes.

**STEP 2 |** Add the firewall to Panorama.

1. Select **Panorama > Managed Devices** and click **Add**.
2. Enter the serial number for each firewall (one entry per line) that you want to manage centrally using Panorama, and then click **OK**. The Managed Devices page displays the new firewall.
3. **(Optional)** Add a **Tag**. Tags make it easier for you to find a firewall from a large list; they help you to dynamically filter and refine the list of firewalls that display. For example, if you add a tag called branch office, you can filter for all branch office firewalls across your network.
   1. Select the check box beside the firewall and click **Tag**.
   2. Click **Add**, enter a string of up to 31 characters (no empty spaces), and click **OK**.
4. If your deployment is using custom certificates for authentication between Panorama and managed devices, deploy the custom client device certificate. For more information, see Set Up Authentication Using Custom Certificates and Add New Client Devices.
5. Select **Commit > Commit to Panorama** and **Commit** your changes.

**STEP 3 |** Verify that the firewall is connected to Panorama.

In the **Panorama > Managed Devices** page, the Device State column displays whether the firewall is connected or disconnected to Panorama.
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 1,024), 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.

**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 Group HA Peers 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 to save your changes.

**STEP 8** | Select Commit > Commit and Push and then Commit and Push your changes to the Panorama configuration and to the device group you added.

Create a Device Group Hierarchy
STEP 1 | Plan the Device Group Hierarchy.

1. Decide the device group levels, and which firewalls and virtual systems you will assign to each device group and the Shared location. You can assign any one firewall or virtual system (vsys) to only one device group. If a device group will be just an organizational container for lower level device groups, you don’t need to assign firewalls to it.

2. Remove firewall or vsys assignments from existing device groups if those assignments don’t fit your planned hierarchy.
   1. Select Panorama > Device Groups and select the device group.
   2. In the Devices section, clear the check boxes of firewalls and virtual systems you want to remove, and click OK.
   3. If necessary, add more firewalls that you will assign to device groups: see Add a Firewall as a Managed Device.

STEP 2 | For each top-level device group, Add a Device Group.

1. In the Panorama > Device Groups page, click Add and enter a Name to identify the device group.
2. In the Devices section, select check boxes to assign firewalls and virtual systems to the device group.
3. Leave the Parent Device Group option at Shared (the default) and click OK.

STEP 3 | For each lower-level device group, Add a Device Group.

- For new device groups at each lower level, repeat Step For each top-level device group, Add a Device Group. but set the Parent Device Group to a device group at the next level above.
- For each existing device group, in the Device Groups page, select the device group to edit it, select a Parent Device Group, and click OK.

If you move a device group to a different parent, all its descendant device groups move with it, along with all firewalls, policy rules, and objects associated with the device group and its descendants. If the new parent is in another access domain, the moved device group will no longer have membership in the original access domain. If the new access domain has read-write access for the parent device group, it will also have read-write access for the moved device group. If the new access domain has read-only access for the parent, it will have no access for the moved device group. To reconfigure access for device groups, see Configure an Access Domain.

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 see Step 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.

Commit to Panorama and push to device groups after any change to the hierarchy.

You must also push changes to templates if a template references objects in a device group (such as interfaces referencing addresses), and a firewall assigned to the template is no longer assigned to that device group because of a hierarchy change.

Select Commit > Commit and Push and then Commit and Push your changes to the Panorama configuration and to the device groups you added or changed.

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 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 Shared.
4. The Disable Override option 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 every Category for which you want notification.
6. In the Action column, select Alert.
7. Click OK to save your changes to the object.
8. Select Commit > Commit to Panorama and Commit your changes.

• 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 option cleared.
4. The Disable Override option 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 Disable Override option.
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 to save your changes to the object.
7. Select Commit > Commit and Push and then Commit and Push your changes to the Panorama configuration and to the device group where you added the object.

- View shared objects and device group objects in 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 (_mob) 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 Step 5
For details on object inheritance and overrides, see Device Group Objects.

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 | Select Commit > Commit and Push and then Commit and Push your changes to the Panorama configuration and to the device group where you reverted the object.

Manage Unused Shared Objects

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

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

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

STEP 1 | Select Panorama > Setup > Management, and edit the Panorama Settings.

STEP 2 | Clear the Share Unused Address and Service Objects with Devices option to push only the shared objects that rules reference, or select the option to re-enable pushing all shared objects.

STEP 3 | Click OK to save your changes.

STEP 4 | Select Commit > Commit to Panorama and Commit your changes.

Manage Precedence of Inherited Objects

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

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.

STEP 1 | Select Panorama > Setup > Management and edit the Panorama Settings.
STEP 2 | If you want to reverse the default order of precedence, select Objects defined in ancestors will take higher precedence. The dialog then displays the Find Overridden Objects link, which provides the option to see how many overridden (shadowed) objects will have ancestor values after you commit this change. You can hover over the quantity message to display the object names.

If you want to revert to the default order of precedence, clear Objects defined in ancestors will take higher precedence.

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

STEP 3 | Click OK to save your changes.

STEP 4 | Select Commit > Commit to Panorama and Commit your changes.

STEP 5 | (Optional) If you selected Objects defined in ancestors will take higher precedence, Panorama does not push the ancestor objects until you push configuration changes to device groups: select Commit > Push to Devices and Push your changes.

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).

When cloning multiple policy rules, the order by which you select the rules will determine the order they are copied to the device group. For example, if you have rules 1-4 and your selection order is 2-1-4-3, the device group where these rules will be cloned will display the rules in the same order you selected. However, you can reorganize the rules as you see fit once they have been successfully copied.

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

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

STEP 3 | Perform one of the following steps:

- (Rules only) Move > Move to other device group
- (Objects only) Move
- (Rules or objects) Clone

STEP 4 | In the Destination drop-down, select the new device group or Shared. The default is the Device Group selected in Step Select the Device Group and select one or more rules or objects.
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 | Select **Commit > Commit and Push**, **Edit Selections** in the Push Scope, select **Device Groups**, select the original and destination device groups, click **OK**, and then **Commit and Push** your changes to the Panorama configuration and to the device groups.

Select a URL Filtering Vendor on Panorama

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

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

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

The following topics describe how to change the URL filtering vendor on Panorama or on both Panorama and managed firewalls. You can also **change the URL filtering vendor on just the firewalls**.

- **Must Panorama and Firewalls Have Matching URL Filtering Vendors?**
- **Change the URL Filtering Vendor on HA Panorama**
- **Change the URL Filtering Vendor on non-HA Panorama**
- **Migrate Panorama and HA Firewalls from BrightCloud to PAN-DB**
- **Migrate Panorama and non-HA Firewalls from BrightCloud to PAN-DB**

**Must Panorama and Firewalls Have Matching URL Filtering Vendors?**

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

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

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

Change the URL Filtering Vendor on HA Panorama

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

STEP 1 | Change the URL filtering vendor on each Panorama HA peer.

1. Log in to the Panorama web interface.
2. Select Panorama > High Availability and Suspend local Panorama.
   
   When you perform this step on Panorama1, failover occurs and Panorama2 becomes active.
4. Select the URL Filtering Database vendor: paloaltonetworks (PAN-DB) or brightcloud.
5. Select Panorama > High Availability and Make local Panorama functional.
   
   When you perform this step on Panorama1 with preemption enabled on both HA peers, Panorama1 automatically reverts to active status and Panorama2 reverts to passive status.

STEP 2 | Verify that the URL categories are available for referencing in policies.

2. Click Add and verify that the Categories tab of the URL Filtering profile dialog displays the URL categories associated with the selected vendor.

Change the URL Filtering Vendor on non-HA Panorama

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

STEP 1 | Change the URL filtering vendor.

1. Select Panorama > Setup > Management and edit the General Settings.
2. Select the URL Filtering Database vendor: paloaltonetworks (PAN-DB) or brightcloud.

STEP 2 | Verify that the URL categories are available for referencing in policies.

2. Click Add and verify that the Categories tab of the URL Filtering profile dialog displays the URL categories associated with the selected vendor.

Migrate Panorama and HA Firewalls from BrightCloud to PAN-DB

Perform this procedure to migrate the URL filtering vendor from BrightCloud to PAN-DB on Panorama and firewalls when the firewalls are deployed in a high availability (HA) configuration. In this example, the active
(or active-primary) firewall is named fw1 and the passive (or active-secondary) firewall is named fw2. The migration automatically maps BrightCloud URL categories to PAN-DB URL categories.

**STEP 1 |** Determine which firewalls require new PAN-DB URL filtering licenses.

1. Log in to Panorama and select Panorama > Device Deployment > Licenses.
2. Check the URL column to determine which firewalls have PAN-DB licenses and whether the licenses are valid or expired.

A firewall can have valid licenses for both BrightCloud and PAN-DB, but only one license can be active.

*If you’re not sure whether a PAN-DB URL filtering license is active, access the firewall web interface, select Device > Licenses, and verify that the Active field displays Yes in the PAN-DB URL Filtering section.*

3. Purchase a new license for each firewall that does not have a valid PAN-DB license.

In HA deployments, each firewall peer needs a distinct PAN-DB license and authorization code. Palo Alto Networks sends an email containing activation codes for the licenses you purchase. If you can’t find this email, contact Customer Support before proceeding.

**STEP 2 |** Change the URL filtering vendor to PAN-DB on Panorama.

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

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

**STEP 3 |** Configure the TCP session settings on both firewall HA peers to ensure sessions that are not yet synchronized will fail over when you suspend a peer.

Log in to the CLI of each firewall and run the following command:

```
> set session tcp-reject-non-syn no
```

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

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

1. Access the firewall web interface, select Device > High Availability > Operational Commands, and Suspend local device.

Performing this step on fw1 triggers failover to fw2.

2. Select Device > Licenses.
3. In the License Management section, select Activate feature using authorization code, enter the Authorization Code and click OK.

Activating the PAN-DB license automatically deactivates the BrightCloud license.

4. In the PAN-DB URL Filtering section, Download the seed file, select your region, and click OK.

5. Commit and push your configuration changes:

   1. Access the Panorama web interface.
   2. Select Commit > Commit and Push and Edit Selections in the Push Scope
   3. Select Device Groups, select the firewall, and click OK.
   4. Commit and Push your changes to the Panorama configuration and to device groups.
6. Access the firewall web interface, select Device > High Availability > Operational Commands, and Make local device functional.

When you perform this step on fw1 with preemption enabled on both firewalls, fw1 automatically reverts to active (or active-primary) status and fw2 reverts to passive (or active-secondary) status.

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

Run the following command at the CLI of each firewall:

```
> set session tcp-reject-non-syn yes
```

---

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

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

**STEP 1** | Determine which firewalls require new PAN-DB URL filtering licenses.

1. Log in to Panorama and select Panorama > Device Deployment > Licenses.
2. Check the URL column to determine which firewalls have PAN-DB licenses and whether the licenses are valid or expired.

A firewall can have valid licenses for both BrightCloud and PAN-DB, but only one license can be active.

*If you’re not sure whether a PAN-DB URL filtering license is active, access the firewall web interface, select Device > Licenses, and verify that the Active field displays Yes in the PAN-DB URL Filtering section.*

3. Purchase new licenses for the firewalls that don’t have valid PAN-DB licenses.

Palo Alto Networks sends an email containing activation codes for the licenses you purchase. If you can’t find this email, contact Customer Support before proceeding.

**STEP 2** | Change the URL filtering vendor to PAN-DB on Panorama.

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

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

**STEP 3** | Migrate the URL filtering vendor to PAN-DB on each firewall.

1. Access the firewall web interface and select Device > Licenses.
2. In the License Management section, select Activate feature using authorization code, enter the Authorization Code, and click OK.

Activating the PAN-DB license automatically deactivates the BrightCloud license.

3. In the PAN-DB URL Filtering section, Download the seed file, select your region, and click OK.
4. Commit and push your configuration changes:

   1. Access the Panorama web interface.
   2. Select Commit > Commit and Push and Edit Selections in the Push Scope
   3. Select Device Groups, select the firewall, and click OK.
   4. Commit and Push your changes to the Panorama configuration and to device groups.
Push a Policy Rule to a Subset of Firewalls

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

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

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 firewall, the rule is added to none of the firewalls in the device group.*

4. Click OK to add the rule.

STEP 3 | Commit and push the configuration changes.

1. Select Commit > Commit and Push and Edit Selections in the Push Scope
2. Select Device Groups, select the device group where you added the rule, and click OK.
3. Commit and Push your changes to the Panorama configuration and to device groups.

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.

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

STEP 2 | Delete or disable rules, if necessary.
To determine which rules a firewall doesn’t currently use, select that firewall in the
Context drop-down on Panorama, select the rulebase (for example, Policies > Security),
and select the Highlight Unused Rules check box. A dotted orange background indicates
the rules that the firewall doesn’t use.

1. Select the rulebase (for example, Policies > Security > Pre Rules) that contains the rule you will delete
or disable.
2. Select the Device Group that contains the rule.
3. Select the rule, and click Delete or Disable as desired. Disabled rules appear in italicized font.

STEP 3 | Reposition rules within a rulebase, if necessary.
To reposition local rules on a firewall, access its web interface by selecting that firewall in
the Context drop-down before performing this step.

1. Select the rulebase (for example, Policies > Security > Pre Rules) that contains the rule you will move.
2. Select the Device Group that contains the rule.
3. Select the rule, select Move, and select:
   • Move Top—Moves the rule above all other rules in the device group (but not above rules inherited
     from Shared or ancestor device groups).
   • Move Up—Moves the rule above the one that precedes it (but not above rules inherited from
     Shared or ancestor device groups).
   • Move Down—Moves the rule below the one that follows it.
   • Move Bottom—Moves the rule below all other rules.
   • Move to other device group—See Move or Clone a Policy Rule or Object to a Different Device
     Group.

STEP 4 | If you modified the rules, commit and push the changes.
1. Select Commit > Commit and Push and Edit Selections in the Push Scope
2. Select Device Groups, select the device group that contains the rules you changed or deleted, and
   click OK.
3. **Commit and Push** your changes to the Panorama configuration and to device groups.
Manage Templates and Template Stacks

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

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

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

Template Capabilities and Exceptions

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

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

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

Add a Template

You must add at least one template before Panorama will display the Device and Network tabs required to define the network set up and device configuration elements for firewalls. Panorama supports up to 1,024 templates.

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

STEP 1 | Add a template.

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

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

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

6. Click OK to save the template.
7. Select Commit > Commit and Push and then Commit and Push your changes to the Panorama configuration and to the template.

STEP 2 | Verify that the template is available.

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

STEP 3 | Use the template to push a configuration change to firewalls.

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. Select Commit > Commit and Push and then Commit and Push your changes to the Panorama configuration and to the template.

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 (green cog) to indicate that settings in the section have values pushed from a template.

Configure a Template Stack

A template stack is a combination of templates: Panorama pushes the settings from every template in the stack to the firewalls you assign to that stack. Panorama supports up to 1,024 template stacks. 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.

-------------------------------

**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 push 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.*

*Renaming a vsys is allowed only on the local firewall. Renaming a vsys on Panorama is not supported. If you rename a vsys on Panorama, you will create an entirely new vsys, or the new vsys name may get mapped to the wrong vsys on the firewall.*

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**.

1. Depending on the settings you will configure, select the **Network** or **Device** tab and select the stack in the **Template** drop-down. The tab settings are read-only when you select a stack.
2. Filter the tabs to display only the mode-specific settings you want to edit:
   - In the **Mode** drop-down, select or clear the **Multi VSYS**, **Operational Mode**, and **VPN Mode** filter options.
   - Set all the **Mode** options to reflect the mode configuration of a particular firewall by selecting it in the **Device** drop-down.
3. 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:
   - If the page displays a table, select **Columns > Template** 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 **Template** drop-down changes to that template, at which point you can edit the setting.
• If the page doesn't display a table, hover over the template icon (green cog) 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 Template drop-down, select the template that the tooltip displays to edit the setting.

4. Edit the settings as needed.

5. Select Commit > Commit and Push, Edit Selections in the Push Scope, select Templates, select the firewalls assigned to the template stack, and then Commit and Push your changes to the Panorama configuration and to the template stack.

STEP 4 | Verify that the template stack works as expected.

Perform the same verification steps as when you Add a Template but select the template stack from the Template drop-down:

1. Step Use the template to push a configuration change to firewalls.

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

Override a Template Setting

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

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

STEP 1 | Access the web interface of the firewall.

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.

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 (green cog) for the Primary DNS Server to enable overrides for that field.

3. Enter a new IP address for the Primary DNS Server. Note that the dialog now displays a template override icon (orange-overlapping-green cogs) to indicate that the value is overridden.

4. Click OK and Commit.

Disable/Remove Template Settings

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

If you want to override a single setting instead of disabling or removing every template or stack setting, see Override a Template Setting.

See Templates and Template Stacks for details on how to use these for managing firewalls.
STEP 1 | Access the web interface of the managed firewall as an administrator with the Superuser role. You can directly access the firewall by entering its IP address in the browser URL field or, in Panorama, select the firewall in the Context drop-down.

STEP 2 | Select Device > Setup > Management and edit the Panorama Settings.

STEP 3 | Click Disable Device and Network Template.

STEP 4 | (Optional) Select Import Device and Network Template before disabling, to save the configuration settings locally on the firewall. If you do not select this option, PAN-OS will delete all Panorama-pushed settings from the firewall.

STEP 5 | Click OK twice and then Commit the changes.
Redistribute User-ID Information to Managed Firewalls

To ensure all the firewalls that enforce policies and generate reports have the required IP address-to-username mappings and authentication timestamps for your entire user base, you can leverage your Panorama and distributed log collection infrastructure to redistribute the mappings and timestamps.

Before you configure User-ID Redistribution Using Panorama and Log Collectors:

- Configure the firewalls to redistribute User-ID information.
- Configure a Dedicated Log Collector to redistribute User-ID information.

A Log Collector that is local to the Panorama management server does not redistribute User-ID information.

1. Add Panorama, firewalls, or virtual systems as User-ID redistribution points to a Log Collector:
   1. Select Panorama > Managed Collectors and select the Log Collector to edit it.
   2. Select User-ID Agents and Add a redistribution point.
      1. Enter a Name to identify the redistribution point.
      2. Enter the Host name or IP address of the interface on the firewall or Panorama that will respond to User-ID information queries from the Log Collector.
      3. Enter the Port number on which Panorama or the firewall will listen for User-ID information queries (default is 5007).
      4. If the redistribution point is a firewall or virtual system, enter the Collector Name and Collector Pre-Shared Key.
   5. Click OK to save your changes.

2. Enable the management (MGT) interface of the Log Collector to respond to User-ID information queries from Panorama or firewalls:
   1. Select Panorama > Managed Collectors and select the Log Collector to edit it.
   2. Select Interfaces and Management.
   3. Select User-ID in the Network Connectivity Services section and click OK.
   4. Click OK to save your changes to the Log Collector.

3. Click OK to save your changes to the Log Collector.

4. Select Commit > Commit and Push to activate your changes on Panorama and push the changes to the Log Collector.

- Configure the Panorama management server to redistribute User-ID information.
  1. Add Log Collectors, firewalls, or virtual systems as redistribution points to Panorama:
     1. Select Panorama > User Identification and Add each redistribution point.
     2. Enter a Name to identify the redistribution point.
     3. Enter the Host name or IP address of the MGT interface on the Log Collector or firewall.
     4. Enter the Port number on which the Log Collector or firewall will listen for User-ID information queries (default is 5007).
5. If the redistribution point is a firewall or virtual system, enter the **Collector Name** and **Collector Pre-Shared Key**.
6. Click **OK** to save the configuration.

2. Enable the Panorama MGT interface to respond to User-ID information queries from Log Collectors or firewalls:

   If the Panorama management server has a high availability (HA) configuration, perform this step on each HA peer as a best practice so that redistribution continues if Panorama fails over.

1. Select **Panorama > Setup > Interfaces and Management**.
2. Select **User-ID** in the Network Connectivity Services section and click **OK**.
3. Select **Commit > Commit to Panorama** to activate your changes on Panorama.

- **Configure firewalls to receive User-ID information from Panorama or Log Collectors.**

   If you are using Panorama to manage both your firewall and the Dedicated Log Collector (DLC), and you want to configure the firewall to receive User-ID information from Panorama or the log collectors, add the User-ID agent using the serial number to the Panorama template, then push the template to the firewall. If you add the User-ID agent on the firewall using the serial number, you will only see Panorama and not the DLC, and you will need to add the DLC to the firewall using the host and port number.

1. Select **Device > User Identification > User-ID Agents**, select the **Template** to which the firewalls are assigned, and **Add** one of the following as a redistribution point:
   - **Panorama**—Add an Agent Using the **Serial Number**, and set the **Serial Number** to *panorama* for the active or solitary Panorama or to *panorama2* (HA only) for the passive Panorama.
   - **Log Collector**—Add an Agent Using the **Host and Port**. Enter the **Host** name or IP address of the MGT interface on the Log Collector. Then enter the **Port** number on which the Log Collector listens for User-ID information queries (default is 5007).
2. Click **OK** to save the configuration.
3. Select **Commit > Commit and Push** to activate your changes on Panorama and push the changes to the firewalls.

- **Verify that Panorama, Log Collectors, and firewalls receive redistributed user mappings.**

1. Access the CLI of a firewall, Log Collector, or Panorama management server that redistributes User-ID information.
2. Display all the user mappings by running the following command:

   ```
   > show user ip-user-mapping all
   ```
3. Record the IP address associated with any one username.
4. Access the CLI of a firewall, Log Collector, or Panorama management server that receives redistributed User-ID information.
5. Display the mapping information and authentication timestamp for the `<IP-address>` you recorded:

   ```
   > show user ip-user-mapping ip <IP-address>
   IP address: 192.0.2.0 (vsys1)
   User: corpdomain\username1
   From: UIA
   Idle Timeout: 10229s
   Max. TTL: 10229s
   ```
This example output shows the timestamp for a response to one authentication challenge (factor). For Authentication rules that use multi-factor authentication (MFA), the output shows multiple timestamps.
Transition a Firewall to Panorama Management

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

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

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

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

Plan the Transition to Panorama Management

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

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

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

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

- Determine if the firewall has configuration elements (policies, objects, and other settings) that you don’t want to import, either because Panorama already contains similar elements or because those elements are firewall-specific (for example, timezone settings) and you won’t use Panorama to manage them. You can perform a global find to determine if similar elements exist on Panorama.
Decide the common zones for each device group. This includes a zone-naming strategy for the firewalls and virtual systems in each device group. For example, if you have zones called Branch LAN and WAN, Panorama can push policy rules that reference those zones without being aware of the variations in port or media type, model, or logical addressing schema.

Create a post-migration test plan.

You will use the test plan to verify that the firewalls work as efficiently after the migration as they did before. The plan might include tasks such as:

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

Migrate a Firewall to Panorama Management

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

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

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

Panorama can import configurations from firewalls that are already managed devices but only if they are not already assigned to device groups or templates.

STEP 1 | Plan the migration.

See the checklist in Plan the Transition to Panorama Management.

STEP 2 | Add the firewall as a managed device.

Add a Firewall as a Managed Device:

1. Log in to Panorama, select Panorama > Managed Devices and click Add.
2. Enter the serial number of the firewall and click OK.

   If you will import multiple firewall configurations, enter the serial number of each one on a separate line. Optionally, you can copy and paste the serial numbers from a Microsoft Excel worksheet.

3. Select Commit > Commit to Panorama and Commit your changes.

STEP 3 | Set up a connection from the firewall to Panorama.

1. Log in to the firewall, select Device > Setup, and edit the Panorama Settings.
2. In the Panorama Servers fields, enter the IP addresses of the Panorama management server.
3. Click OK and Commit.
STEP 4 | Import the firewall configuration into Panorama.

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

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

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

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

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

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

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

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

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

6. Select Commit > Commit to Panorama and Commit your changes.

STEP 5 | Push the configuration from Panorama to the newly added device.

To prevent duplicate rule or object names, push the device group configuration from Panorama to the firewall to avoid commit errors.

This step is required to successfully migrate firewall management to the Panorama management server. Failure to perform this step successfully causes configuration errors and commit failures.

1. Log in to the Panorama Web Interface and select Panorama > Setup > Operations and click Export or push device config bundle.
2. Click Export or push device config bundle, select the Device from the drop-down menu, and click OK.
3. Select the **Device** from which you imported the configuration, click **OK**, and click **Push & Commit**. Panorama pushes the bundle and initiates a commit on the firewall.

4. Click **Close** after the push has committed successfully.

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

6. On the Panorama web interface, **Select Panorama > Managed Devices > Summary**, and verify that the device group and template stack are in sync for the passive firewall. Verify policy rules, objects and network settings on the passive firewall match the active firewall. On the firewall web interface, verify that configuration objects display a green cog (.), signifying that the configuration object is pushed from Panorama.

7. **Select Commit > Commit to Panorama** and **Commit** your changes.

**STEP 6 | Fine-tune the imported configuration.**

1. In Panorama, select **Panorama > Config Audit**, select the **Running config** and **Candidate config** for the comparison, click **Go**, and review the output.

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

**STEP 7 | Push the firewall configuration bundle to the firewall to remove all policy rules and objects from its local configuration.**

This step is necessary to prevent duplicate rule or object names, which would cause commit errors when you push the device group configuration from Panorama to the firewall in the next step.

1. In Panorama, select **Commit > Commit to Panorama** and **Commit** your changes.

2. Select **Panorama > Setup > Operations** and click **Export or push device config bundle**.

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

**STEP 8 | Push the device group and template configurations to complete the transition to centralized management.**

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

1. Select **Commit > Commit and Push** and **Edit Selections** in the Push Scope.

2. Select **Device Groups** and select the device groups that contain the imported firewall configurations.

3. Select **Merge with Device Candidate Config, Include Device and Network Templates, and Force Template Values**.

4. Click **OK** to save your changes to the Push Scope.

5. **Commit and Push** your changes.

**STEP 9 | Consolidate all the imported firewall configurations.**

Required if you are migrating multiple firewalls. Settings might be duplicated among the firewalls. For example, if you imported an object with the same name from two firewalls, you must delete one object in Panorama before performing a commit on Panorama.
1. After importing all the firewall configurations, update the device groups and templates as needed to eliminate redundancy and streamline configuration management: see Fine-tune the imported configuration. (You don't need to push firewall configuration bundles again.)

2. Configure any firewall-specific settings.

   If the firewalls will have local zones, you must create them before performing a device group or template commit; Panorama can't poll the firewalls for zone name or zone configuration. If you will use local firewall rules, ensure their names are unique (not duplicated in Panorama). If necessary, you can Override a Template Setting with a firewall-specific value.

3. Commit and push your changes:
   
   2. Select Device Groups, select the device groups you changed, and Include Device and Network Templates.
   3. Click OK to save your changes to the Push Scope.
   4. Commit and Push your changes.

STEP 10 | Perform your post-migration test plan.

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

Migrate a Firewall HA Pair to Panorama Management

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

STEP 1 | Plan the migration.

See the checklist in Plan the Transition to Panorama Management.

STEP 2 | Disable configuration synchronization between the HA peers.

Repeat these steps for both firewalls in the HA pair.

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

STEP 3 | Connect each firewall to Panorama.

   If Panorama is already receiving logs from these firewalls, you do not need to perform this step. Continue to Step 5.

Repeat these steps for both firewalls in the HA pair.

1. Log in to the web interface on each firewall, select Device > Setup > Management and edit the Panorama Settings.
2. In the Panorama Servers fields, enter the IP addresses of the Panorama management servers, confirm Panorama Policy and Objects and Device and Network Template are enabled and select OK.
3. **Commit** the configuration changes on each firewall.

**STEP 4 | Add each firewall as a managed device.**

*If Panorama is already receiving logs from these firewalls, you do not need to perform this step. Continue to Step 5.*

**Add a Firewall as a Managed Device.**

1. Log in to Panorama, select *Panorama > Managed Devices* and click *Add.*
2. Enter the serial number of each firewall and click *OK.*
3. Select *Commit > Commit to Panorama* and *Commit* your changes.
4. Verify that the Device State for each firewall is *Connected.*

**STEP 5 | Import each firewall configuration into Panorama.**

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

1. From Panorama, select *Panorama > Setup > Operations,* click *Import device configuration to Panorama,* and select a HA peer *Device.*

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

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

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

4. **Commit to Panorama.**
5. Select *Panorama > Setup > Operations* and *Export or push device config bundle.* Select the *Device,* select *OK* and *Push & Commit* the configuration.
HA Config Sync in Step 2 must be disabled on both firewalls before you push the device group and template.

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

7. On Panorama, select Panorama > Managed Devices, and verify that the device group and template are in sync for the passive firewall. Verify policy rules, objects and network settings on the passive firewall match the active firewall. On the firewall web interface, verify that configuration objects a green cog (.), signifying that the configuration object is pushed from Panorama.

8. Commit to Panorama.

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

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

10. Select Commit > Commit to Panorama and Commit your changes.

STEP 6 | Add the HA firewall pair into the same device group and template.

   Skip this step if the HA firewall pair are in an active/active configuration.

   Do not combine the HA firewall pair in to a single template if a unique Hostname, management IP address, or HA configuration is configured for each HA peer. You may also configure a unique Hostname, management IP address, or HA configuration locally on the firewalls.

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

STEP 7 | Enable configuration synchronization between the HA peers.

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

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

Load a Partial Firewall Configuration into Panorama

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

STEP 1 | Plan the transition to Panorama.

   See the checklist in Plan the Transition to Panorama Management.

STEP 2 | Resolve how to manage duplicate settings, which are those that have the same names in Panorama as in a firewall.
Before you load a partial firewall configuration, Panorama and that firewall might already have duplicate settings. Loading a firewall configuration might also add settings to Panorama that are duplicates of settings in other managed firewalls.

If Panorama has policy rules or objects with the same names as those on a firewall, a commit failure will occur when you try to push device group settings to that firewall. If Panorama has template settings with the same names as those on a firewall, the template values will override the firewall values when you push the template.

1. On Panorama, perform a global find to determine if duplicate settings exist.
2. Delete or rename the duplicate settings on the firewall if you will use Panorama to manage them, or delete or rename the duplicate settings on Panorama if you will use the firewall to manage them. If you will use the firewall to manage device or network settings, instead of deleting or renaming the duplicates on Panorama, you can also push the settings from Panorama (Step 6) and then Override a Template Setting on the firewall with firewall-specific values.

STEP 3 | Export the entire firewall configuration to your local computer.
1. On the firewall, select Device > Setup > Operations.
2. Click Save named configuration snapshot, enter a Name to identify the configuration, and click OK.
3. Click Export named configuration snapshot, select the Name of the configuration you just saved, and click OK. The firewall exports the configuration as an XML file.

STEP 4 | Import the firewall configuration snapshot into Panorama.
2. Click Import named Panorama configuration snapshot, Browse to the firewall configuration file you exported to your computer, and click OK.

After using this option to import a firewall configuration file, you can't use the Panorama web interface to load it. You must use the XML API or CLI, as described in the next step.

STEP 5 | Load the desired part of the firewall configuration into Panorama.
To specify a part of the configuration (for example, all application objects), you must identify the:
- Source xpath—The XML node in the firewall configuration file from which you are loading.
- Destination xpath—The node in the Panorama configuration to which you are loading.

Use the XML API or CLI to identify and load the partial configuration:
1. Use the firewall XML API or CLI to identify the source xpath.
   For example, the xpath for application objects in vsys1 of the firewall is:

   /config/devices/entry[@name='localhost.localdomain']/vsys/vsys1/application

2. Use the Panorama XML API or CLI to identify the destination xpath.
   For example, to load application objects into a device group named US-West, the xpath is:

   /config/devices/entry[@name='localhost.localdomain']/device-group/entry[@name='US-West']/application

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

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

STEP 6 | Push the partial configuration from Panorama to the firewall to complete the transition to centralized management.

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

2. On Panorama, push the partial configuration to the firewall.
   1. Select **Commit > Commit and Push** and **Edit Selections** in the Push Scope.
   2. Select **Device Groups** and select the device groups that contain the imported firewall configurations.
   3. Select **Merge with Device Candidate Config**, **Include Device and Network Templates**, and **Force Template Values**.
   4. Click **OK** to save your changes to the Push Scope.
   5. **Commit and Push** your changes.

3. If the firewall has a device or network setting that you won’t use Panorama to manage, **Override a Template Setting** on the firewall.

STEP 7 | Perform your post-migration test plan.

Perform the verification tasks that you devised during the migration planning to confirm that the firewall works as efficiently with the Panorama-pushed configuration as it did with its original local configuration: see **Create a post-migration test plan**.
Use Case: Configure Firewalls Using Panorama

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

Figure 13: Firewall Distribution Example

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

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

Device Groups in this Use Case

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

- DG_BranchAndRegional for grouping firewalls that serve as the security gateways at the branch offices and at the regional head offices. We placed the branch office firewalls and the regional office firewalls in the same device group because firewalls with similar functions will require similar policy rulebases.
- DG_DataCenter for grouping the firewalls that secure the servers at the data centers.
We can then administer shared policy rules across both device groups as well as administer distinct device group rules for the regional office and branch office groups. Then for added flexibility, the local administrator at a regional or branch office can create local rules that match specific source, destination, and service flows for accessing applications and services that are required for that office. In this example, we create the following hierarchy for security rules. You can use a similar approach for any of the other rulebases.

Figure 14: Security Rules Hierarchy

Templates in this Use Case

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

- T_Branch for the branch office firewalls
- T_Regional for the regional office firewalls
- T_DataCenter for the data center firewalls
If you plan to deploy your firewalls in an active/active HA configuration, assign each firewall in the HA pair to a separate template. Doing so gives you the flexibility to set up separate networking configurations for each peer. For example, you can manage the networking configurations in a separate template for each peer so that each can connect to different northbound and southbound routers, and can have different OSPF or BGP peering configurations.

Set Up Your Centralized Configuration and Policies

In Use Case: Configure Firewalls Using Panorama, we would need to perform the following tasks to centrally deploy and administer firewalls:

- Add the Managed Firewalls and Deploy Updates
- Use Templates to Administer a Base Configuration
- Use Device Groups to Push Policy Rules
- Preview the Rules and Commit Changes

Add the Managed Firewalls and Deploy Updates

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

STEP 1 | For each firewall that Panorama will manage, Add a Firewall as a Managed Device.

In this example, add 12 firewalls.

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 Use the Panorama Task Manager.

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.

Figure 15: Device Group Example

If you plan to deploy your firewalls in an active/active HA configuration, assign each firewall in the HA pair to a separate template. Doing so gives you the flexibility to set up separate networking configurations for each peer. For example, you can manage the networking configurations in a separate template for each peer so that each can connect to different northbound and southbound routers, and can have different OSPF or BGP peering configurations.
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

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

### 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:
   1. Select **Device > Setup > Services > Global** and edit the Services.
   2. In the **Services** tab, enter an IP address for the **Primary DNS Server**.

   *For any firewall that has more than one virtual system (vsys), for each vsys, add a DNS server profile to the template (Device > Server Profiles > DNS).*

3. In the **NTP** tab, enter an IP address for the **Primary NTP Server**.
4. Click **OK** to save your changes.
5. Add a login banner: select **Device > Setup > Management**, edit the General Settings, enter text for the **Login Banner** and click **OK**.
6. **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** as, set the **Alert** packets/second to **100**, set the **Activate** packets/second to **1000**, and set the **Maximum** packets/second to **10000**.
4. For this example, enable alerts—In the **Reconnaissance Protection** tab, select the **Enable** check boxes for **TCP Port Scan**, **Host Sweep**, and **UDP Port Scan**. Ensure the Action values are set to **alert** (the default value).

5. Click **OK** to save the Zone Protection profile.

**STEP 5** | Configure the interface and zone settings in the data center template (T_DataCenter), and then attach the Zone Protection profile you just created.

Before performing this step, you must have configured the interfaces locally on the firewalls. As a minimum, for each interface, you must have defined the interface type, assigned it to a virtual router (if needed), and attached a security zone.

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

**STEP 6** | Push your template changes.

1. Select **Commit > Commit and Push** and **Edit Selections** in the Push Scope.
2. Select **Templates** and select the firewalls assigned to the templates where you made changes.
3. **Commit and Push** your changes to the Panorama configuration and to the template.

**Use Device Groups to Push Policy Rules**

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

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

In this example, create device groups named DG_BranchAndRegional and DG_DataCenter.

When configuring the DG_BranchAndRegional device group, you must assign a **Master** firewall. This is the only firewall in the device group that gathers user and group mapping information for policy evaluation.

**STEP 2** | Create a shared pre-rule to allow DNS and SNMP services.

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

2. Create the shared rule.
   1. Select the **Policies** tab and, in the **Device Group** drop-down, select **Shared**.
   2. Select the **Security > Pre-Rules** rulebase.
3. Click Add and enter a Name for the security rule.
4. In the Source and Destination tabs for the rule, click Add and enter a Source Zone and a Destination Zone for the traffic.
5. In the Applications tab, click Add, type the name of the applications group object you just created, and select it from the drop-down.
6. 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:
   1. Click Add and click New Application Filter in the footer of the drop-down.
   2. Enter a Name, and select the Shared check box.
   3. In the Risk column, select levels 3, 4, and 5.
   4. In the Technology column, select peer-to-peer.
   5. 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.

**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 (see 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.
   1. Select Objects > Addresses and, in the Device Group drop-down, select DG_DataCenter.
   2. Click Add and enter a Name for the address object.
3. Select the **Type**, and specify an IP address and netmask (**IP Netmask**), range of IP addresses (**IP Range**), or **FQDN**.
4. Click **OK** to save the object.

2. Create a security rule that allows access to the Amazon cloud application.

1. Select **Policies > Security > Pre-Rules** and, in the **Device Group** drop-down, select **DG_DataCenter**.
2. Click **Add** and enter a **Name** for the security rule.
3. Select the **Source** tab, **Add** the Source Zone for the data center, and **Add** the address object (**Source Address**) you just defined.
4. Select the **Destination** tab and **Add** the Destination Zone.
5. Select the **Application** tab, click **Add**, type **amazon**, and select the Amazon applications from the list.
6. Select the **Action** tab and set the **Action** to **Allow**.
7. Click **OK** to save the rule.

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

**Preview the Rules and Commit Changes**

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

**STEP 1** | Preview the rules.

This preview enables you to visually evaluate how rules are layered for a particular rulebase.
1. Select **Policies** and **Preview Rules**.
2. Select a **Rulebase**, **Device Group**, and **Device**.
3. Close the preview dialog when you finish.

**STEP 2** | Commit and push your configuration changes.
1. Select **Commit > Commit and Push** and **Edit Selections** in the Push Scope.
2. Select **Device Groups**, select the device groups you added, and **Include Device and Network Templates**.
3. Click **OK** to save your changes to the Push Scope.
4. **Commit and Push** your changes.

**STEP 3** | Verify that Panorama applied the template and policy configurations.
1. In the Panorama header, set the **Context** to the firewall to access its web interface.
2. Review the template and policy configurations to ensure your changes are there.
Manage Log Collection

All Palo Alto Networks 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 the Panorama™ management server or to Log Collectors that Panorama manages. Optionally, you can then configure Panorama to forward the logs to external logging destinations (such as syslog servers). If you forward logs to a Panorama virtual appliance in Legacy mode, you don’t need to perform any additional tasks to enable logging. If you forward logs to Log Collectors, you must configure them as managed collectors and assign them to Collector Groups. A managed collector can be local to an M-500 appliance, M-100 appliance, or Panorama virtual appliance in Panorama mode or can be an M-500 or M-100 appliance in Log Collector mode (Dedicated Log Collector). To determine whether to deploy either or both types of managed collectors, see Local and Distributed Log Collection.

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

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

To enable the Panorama management server to manage a Log Collector, you must add it as a managed collector. You can add two types of managed collectors:

- **Dedicated Log Collector**—To set up a new M-500 or M-100 appliance as a Log Collector or switch an existing M-Series appliance from Panorama mode to Log Collector mode, see [Set Up the M-Series Appliance as a Log Collector](#). Keep in mind that switching from Panorama Mode to Log Collector Mode removes the local Log Collector that is predefined on the M-Series appliance in Panorama mode.

- **Local Log Collector**—A Log Collector can run locally on the M-500 appliance, M-100 appliance, or Panorama virtual appliance in Panorama mode. On the M-Series appliances, the Log Collector is predefined; on the virtual appliance, you must add the Log Collector. When the Panorama management server has a high availability (HA) configuration, each HA peer can have a local Log Collector. However, relative to the primary Panorama, the Log Collector on the secondary Panorama is remote, not local. Therefore, to use the Log Collector on the secondary Panorama, you must manually add it to the primary Panorama (for details, see [Deploy Panorama M-Series Appliances with Local Log Collectors](#) or [Deploy Panorama Virtual Appliances with Local Log Collectors](#)). If you delete a local Log Collector, you can later add it back. The following steps describe how to add a local Log Collector.

> **As a best practice, retain a local Log Collector and Collector Group on the Panorama management server, regardless of whether it manages Dedicated Log Collectors.**

> **If the Panorama virtual appliance is in Legacy mode, you must switch to Panorama mode to create a Log Collector. For details, see [Set Up the Panorama Virtual Appliance with Local Log Collector](#).**

**STEP 1 |** Record the serial number of the Log Collector.

You will need this when you add the Log Collector as a managed collector.

1. Access the Panorama web interface.
2. Select Dashboard and record the Serial # in the General Information section.

**STEP 2 |** Add the Log Collector as a managed collector.

1. Select Panorama > Managed Collectors and Add a new Log Collector.
2. In the General settings, enter the serial number (Collector S/N) you recorded for the Log Collector.
3. Click OK to save your changes.
4. Select Commit > Commit to Panorama.

**STEP 3 |** (Optional) Configure the Log Collector admin authentication.

1. Select Panorama > Managed Collectors and edit the Log Collector by clicking its name.
2. Configure the Log Collector admin password:
   1. Select the password Mode.
   2. If you selected Password mode, enter a plaintext Password and Confirm Password. If you selected Password Hash mode, enter a hashed password string of up to 63 characters.
3. Configure the admin login security requirements:

   > **If you set the Failed Attempts to a value other than 0 but leave the Lockout Time at 0, then the admin user is indefinitely locked out until another administrator manually unlocks the locked out admin. If no other administrator has been created, you must**
reconfigure the Failed Attempts and Lockout Time settings on Panorama and push the configuration change to the Log Collector. To ensure that an admin is never locked out, use the default 0 value for both Failed Attempts and Lockout Time.

1. Enter the number of login Failed Attempts value. The range is between the default value 0 to the maximum of 10 where the value 0 specifies unlimited login attempts.
2. Enter the Lockout Time value between the default value 0 to the maximum of 60 minutes.
4. Click OK to save your changes.

STEP 4 | Enable the logging disks.
1. Select Panorama > Managed Collectors and edit the Log Collector by clicking its name.
   The Log Collector name has the same value as the hostname of the Panorama management server.
2. Select Disks and Add each disk pair.
3. Click OK to save your changes.
4. Select Commit > Commit to Panorama.

STEP 5 | (Optional) If your deployment is using custom certificates for authentication between Panorama and managed devices, deploy the custom client device certificate. For more information, see Set Up Authentication Using Custom Certificates.
1. Select Panorama > Certificate Management > Certificate Profile and choose the certificate profile from the drop-down or click New Certificate Profile to create one.
2. Select Panorama > Managed Collectors and Add a new Log Collector or select an existing one. Select Communication.
3. Select the type of device certificate the Type drop-down.
   • If you are using a local device certificate, select the Certificate and Certificate Profile from the respective drop-downs.
   • If you are using SCEP as the device certificate, select the SCEP Profile and Certificate Profile from the respective drop-downs.
4. Click OK.

STEP 6 | (Optional) Configure Secure Server Communication on a Log Collector. For more information, see Set Up Authentication Using Custom Certificates.
1. Select Panorama > Managed Collectors and click Add. Select Communication.
2. Verify that the Custom Certificate Only check box is not selected. This allows you to continue managing all devices while migrating to custom certificates.

When the Custom Certificate Only check box is selected, the Log Collector does not authenticate and cannot receive logs from devices using predefined certificates.
3. Select the SSL/TLS service profile from the SSL/TLS Service Profile drop-down. This SSL/TLS service profile applies to all SSL connections between the Log Collector and devices sending it logs.
4. Select the certificate profile from the Certificate Profile drop-down.
5. Select Authorize Client Based on Serial Number to have the server check clients against the serial numbers of managed devices. The client certificate must have the special keyword $UDID set as the CN to authorize based on serial numbers.
6. In Disconnect Wait Time (min), enter the number of minutes Panorama should before breaking and reestablishing the connection with its managed devices. This field is blank by default and the range is 0 to 44,640 minutes.

The disconnect wait time does not begin counting down until you commit the new configuration.
7. (Optional) Configure an authorization list.
1. Click **Add** under Authorization List.
2. Select the **Subject** or **Subject Alt Name** as the Identifier type.
3. Enter an identifier of the selected type.
4. Click **OK**.
5. Select **Check Authorization List** to enforce the authorization list.
6. Click **OK**.
7. Select **Commit > Commit to Panorama**.

**STEP 7 | Verify your changes.**

1. Verify that the **Panorama > Managed Collectors** page lists the Log Collector you added. The Connected column displays a check mark to indicate that the Log Collector is connected to Panorama. You might have to wait a few minutes before the page displays the updated connection status.

> **Until you Configure a Collector Group and push configuration changes to the Collector Group, the Configuration Status column displays Out of Sync, the Run Time Status column displays disconnected, and the CLI command `show interface all` displays the interfaces as down.**

2. Click **Statistics** in the last column to verify that the logging disks are enabled.

**STEP 8 | Next steps...**

Before a Log Collector can receive firewall logs, you must:

1. **Configure Log Forwarding to Panorama.**
2. **Configure a Collector Group**—On the M-Series appliances, a default Collector Group is predefined and already contains the local Log Collector as a member. On the Panorama virtual appliance, you must add the Collector Group and add the local Log Collector as a member. On both models, assign firewalls to the local Log Collector for log forwarding.
Manage Collector Groups

A Collector Group is 1 to 16 Log Collectors that operate as a single logical unit for collecting firewall logs. You must assign at least one Log Collector to a Collector Group for firewalls to successfully send logs to a Log Collector. Firewall logs are dropped if there is no Collector Group configured or none of the Log Collectors are assigned to a Collector Group. You can configure a Collector Group with multiple Log Collectors to ensure log redundancy or to accommodate logging rates that exceed the capacity of a single Log Collector (see Panorama Models). To understand the risks and recommended mitigations, see Caveats for a Collector Group with Multiple Log Collectors.

The M-500 and M-100 appliances in Panorama mode have a predefined Collector Group that contains a predefined local Log Collector. You can edit all the settings of the predefined Collector Group except its name (default).

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

If you switch an M-Series appliance from Panorama mode to Log Collector mode, the appliance will lose its predefined Collector Group and Log Collector. You would then have to Set Up the M-Series Appliance as a Log Collector, add it as a managed collector to Panorama, and configure a Collector Group to contain the managed collector.

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

Configure a Collector Group

Before configuring Collector Groups, decide whether each one will have a single Log Collector or multiple Log Collectors (up to 16). A Collector Group with multiple Log Collectors supports higher logging rates and log redundancy but has the following requirements:

- In any single Collector Group, all the Log Collectors must run on the same Panorama model: all M-500 appliances, all M-100 appliances, or all Panorama virtual appliances.
- Log redundancy is available only if each Log Collector has the same number of logging disks. To add disks to a Log Collector, see Increase Storage on the M-Series Appliance.
- (Best Practice) All Log Collectors in the same Collector Group should be in the same local area network (LAN). Avoid adding Log Collectors in the same or different wide area networks (WAN) to the same Collector Group as network disruption are much more common and may result in log data loss. Additionally, it is recommended that Log Collectors in the same Collector Group be in close physical proximity to each other to allow Panorama to quickly query the Log Collectors when needed.

STEP 1 | Perform the following tasks before configuring the Collector Group.
1. Add a Firewall as a Managed Device for each firewall that you will assign to the Collector Group.
2. Configure a Managed Collector for each Log Collector that you will assign to the Collector Group.

STEP 2 | Add the Collector Group.
1. Access the Panorama web interface, select Panorama > Collector Groups, and Add a Collector Group or edit an existing one.
2. Enter a Name for the Collector Group if you are adding one.
You cannot rename an existing Collector Group.

3. Enter the **Minimum Retention Period** in days (1 to 2,000) for which the Collector Group will retain firewall logs.

   By default, the field is blank, which means the Collector Group retains logs indefinitely.

4. **Add** Log Collectors (1 to 16) to the Collector Group Members list.

5. **(Recommended)** **Enable log redundancy across collectors** if you are adding multiple Log Collectors to a single Collector group.

   Redundancy ensures that no logs are lost if any one Log Collector becomes unavailable. Each log will have two copies and each copy will reside on a different Log Collector. Enabling redundancy creates more logs and therefore requires more storage capacity. When a Collector Group runs out of space, it deletes older logs. Redundancy also doubles the log processing traffic in a Collector Group, which reduces its maximum logging rate by half, as each Log Collector must distribute a copy of each log it receives.

**STEP 3 | Assign Log Collectors and firewalls to the Collector Group.**

1. Select **Device Log Forwarding** and **Add log forwarding preference lists** for the firewalls.

   A preference list determines the order in which Log Collectors will receive logs from a firewall. Perform the following steps for each set of firewalls that has the same preference list:

   1. In the Devices section, **Modify** the list of firewalls and click **OK**.
   2. In the Collectors section, **Add** Log Collectors to the preference list.

      If you assign multiple Log Collectors, the first one will be the primary; if the primary becomes unavailable, the firewalls send logs to the next Log Collector in the list. To change the priority of a Log Collector, select it and **Move Up** (higher priority) or **Move Down** (lower priority).

   3. Click **OK**.

**STEP 4 | Define the storage capacity (log quotas) and expiration period for each log type.**

1. Return to the **General** tab and click the **Log Storage** value.

   If the field displays **0MB**, verify that you enabled the disk pairs for logging and committed the changes (see **Configure a Managed Collector**, **Disks tab**).

2. Enter the log storage **Quota(%)** for each log type.

3. Enter the **Max Days** (expiration period) for each log type (1 to 2,000).

   By default, the fields are blank, which means the logs never expire.

**STEP 5 | Commit and verify your changes.**

1. Select **Commit > Commit and Push** and then **Commit and Push** your changes to Panorama and the Collector Group you configured.

2. Select **Panorama > Managed Collectors** to verify the Log Collectors in the Collector Group are:

   - **Connected to Panorama**—The Connected column displays a check mark icon to indicate that a Log Collector is connected to Panorama.
   - **Synchronized with Panorama**—The Configuration Status column indicates whether a Log Collector is **In Sync** (green icon) or **Out of Sync** (red icon) with Panorama.

**STEP 6 | Next steps...**

1. **Configure Log Forwarding to Panorama.**

   The Collector Group won’t receive firewall logs until you configure the firewalls to forward to Panorama.

2. **(Optional)** **Configure Log Forwarding from Panorama to External Destinations.**
You can configure each Collector Group to forward logs to separate destinations (such as a syslog server).

Move a Log Collector to a Different Collector Group

M-500 and M-100 appliances can have one or more Log Collectors in each Collector Group. You assign Log Collectors to a Collector Group based on the logging rate and log storage requirements of that Collector Group. If the rates and required storage increase in a Collector Group, the best practice is to Increase Storage on the M-Series Appliance or Configure a Collector Group with additional Log Collectors. However, in some deployments, it might be more economical to move Log Collectors between Collector Groups.

When a Log Collector is local to an M-500 or M-100 appliance in Panorama mode, move it only if the appliance is the passive peer in a high availability (HA) configuration. HA synchronization applies the configurations associated with the new Collector Group. Never move a Log Collector that is local to the active HA peer.

In any single Collector Group, all the Log Collectors must run on the same Panorama model: all M-500 appliances, all M-100 appliances, or all Panorama virtual appliances.

Log redundancy is available only if each Log Collector has the same number of logging disks. To add disks to a Log Collector, see Increase Storage on the M-Series Appliance.

STEP 1 | Remove the Log Collector from Panorama management.
1. Select Panorama > Collector Groups and edit the Collector Group that contains the Log Collector you will move.
2. In the Collector Group Members list, select and Delete the Log Collector.
3. Select Device Log Forwarding and, in the Log Forwarding Preferences list, perform the following steps for each set of firewalls assigned to the Log Collector you will move:
   1. In the Devices column, click the link for the firewalls assigned to the Log Collector.
   2. In the Collectors column, select and Delete the Log Collector.
   
   To reassign the firewalls, Add the new Log Collector to which they will forward logs.

   3. Click OK twice to save your changes.
4. Select Panorama > Managed Collectors and then select and Delete the Log Collector you will move.

STEP 2 | Configure a Collector Group.
Add the Log Collector to its new Collector Group and assign firewalls to the Log Collector.

When you push changes to the Collector Group configuration, Panorama starts redistributing logs across the Log Collectors. This process can take hours for each terabyte of logs. During the redistribution process, the maximum logging rate is reduced. In the Panorama > Collector Groups page, the Log Redistribution State column indicates the completion status of the process as a percentage.

STEP 3 | Configure Log Forwarding to Panorama for the new Collector Group you configured.

STEP 4 | Select Commit > Commit and Push to commit your changes to Panorama and push the changes to device groups, templates, and Collector Groups if you have not already done so.
Remove a Firewall from a Collector Group

If you use a Panorama virtual appliance in Legacy mode to manage Dedicated Log Collectors, you have the option to forward firewall logs to Panorama instead of forwarding to the Log Collectors. For such cases, you must remove the firewall from the Collector Group; the firewall will then automatically forward its logs to Panorama.

To temporarily remove the log forwarding preference list on the firewall, you can delete it using the CLI on the firewall. You must however, remove the assigned firewalls in the Collector Group configuration on Panorama. Otherwise, the next time you push changes to the Collector Group, the firewall will be reconfigured to send logs to the assigned Log Collector.

STEP 1 | Select Panorama > Collector Groups and edit the Collector Group.

STEP 2 | Select Device Log Forwarding, click the firewall in the Devices list, Modify the Devices list, clear the check box of the firewall, and click OK three times.

STEP 3 | Select Commit > Commit and Push and then Commit and Push your changes to Panorama and the Collector Group from which you removed the firewall.
Configure Log Forwarding to Panorama

Each firewall stores its log files locally by default and cannot display the logs that reside on other firewalls. Therefore, to achieve global visibility into the network activity that all your firewalls monitor, you must forward all firewall logs to Panorama and use Panorama for Visibility. In cases where some teams in your organization can achieve greater efficiency by monitoring only the logs that are relevant to their operations, you can create forwarding filters based on any log attributes (such as threat type or source user). For example, a security operations analyst who investigates malware attacks might be interested only in Threat logs with the type attribute set to wildfire-virus.

The following steps describe how to use Panorama templates and device groups for configuring multiple firewalls to forward logs.

If Panorama will manage firewalls running software versions earlier than PAN-OS 7.0, specify a WildFire™ server from which Panorama can gather analysis information for WildFire samples that those firewalls submit. Panorama uses the information to complete WildFire Submissions logs that are missing field values introduced in PAN-OS 7.0. Firewalls running earlier releases won’t populate those fields. To specify the server, select Panorama > Setup > WildFire, edit the General Settings, and enter the WildFire Private Cloud name. The default is wildfire-public-cloud, which is the WildFire cloud hosted in the United States.

You can also forward firewall logs to external services (such as a syslog server). For details, see Log Forwarding Options.

STEP 1 | Add a Device Group for the firewalls that will forward logs.

Panorama requires a device group to push a Log Forwarding profile to firewalls. Create a new device group or assign the firewalls to an existing device group.

STEP 2 | Add a Template for the firewalls that will forward logs.

Panorama requires a template to push log settings to firewalls. Create a new template or assign the firewalls to an existing template.

STEP 3 | Create a Log Forwarding profile.

The profile defines the destinations for Traffic, Threat, WildFire Submission, URL Filtering, Data Filtering, Tunnel and Authentication logs.

1. Select Objects > Log Forwarding, select the Device Group of the firewalls that will forward logs, and Add a profile.
2. Enter a Name to identify the Log Forwarding profile.
3. Add one or more match list profiles.

The profiles specify log query filters, forwarding destinations, and automatic actions such as tagging. For each match list profile:

1. Enter a Name to identify the profile.
2. Select the Log Type.
3. In the Filter drop-down, select Filter Builder. Specify the following and then Add each query:
   - Connector logic (and/or)
   - Log Attribute
Operator to define inclusion or exclusion logic
Attribute Value for the query to match
4. Select Panorama.
4. Click OK to save the Log Forwarding profile.

STEP 4 | Assign the Log Forwarding profile to policy rules and network zones.

Security, Authentication, and DoS Protection rules support log forwarding. In this example, you assign the profile to a Security rule.

Perform the following steps for each rule that will trigger log forwarding:
1. Select the rulebase (for example, Policies > Security > Pre Rules), select the Device Group of the firewalls that will forward logs, and edit the rule.
2. Select Actions and select the Log Forwarding profile you created.
3. Set the Profile Type to Profiles or Group, and then select the security profiles or Group Profile required to trigger log generation and forwarding for:
   - Threat logs—Traffic must match any security profile assigned to the rule.
   - WildFire logs—Traffic must match a WildFire Analysis profile assigned to the rule.
4. For Traffic logs, select Log At Session Start and/or Log At Session End.
5. Click OK to save the rule.

STEP 5 | Configure the destinations for System logs, Configuration logs, User-ID™ logs, and HIP Match logs.

Panorama generates Correlation logs based on the firewall logs it receives, rather than aggregating Correlation logs from firewalls.

1. Select Device > Log Settings and select the Template of the firewalls that will forward logs.
2. For each log type that the firewall will forward, see step Add one or more match list profiles.

STEP 6 | (PA-7000 Series firewalls only) Configure a log card interface to perform log forwarding.

When you configure a data port on one of the PA-7000 Series Network Processing Cards (NPCs) as a Log Card interface, the firewall will automatically begin using this interface to forward logs to the logging destinations you configure and forward files for WildFire analysis. Make sure that the interface you configure can reach the log forwarding destinations and the WildFire cloud, WildFire appliance, or both.

Because PA-7000 Series firewall can now forward logs to Panorama, Panorama no longer treats the PA-7000 Series firewalls it manages as Log Collectors upon upgrade to PAN-OS 8.0. If you have not configured the PA-7000 Series firewalls to forward logs to Panorama, all logs a managed PA-7000 Series firewall generates are only viewable from the local firewall and not from Panorama. If you do not yet have a log forwarding infrastructure that is capable of handling the logging rate and volume from the PA-7000 Series firewalls, starting with PAN-OS 8.0.8 you can enable Panorama to directly query PA-7000 Series firewalls when monitoring logs. To use this functionality, both Panorama and the PA-7000 Series firewalls must be running PAN-OS 8.0.8 or later. Enable Panorama to directly query PA-7000 Series firewalls by entering the following command from the Panorama CLI:

> debug-reportd send-request-to-7k yes

After running this command, you will be able to view logs for managed PA-7000 Series firewalls on the Panorama Monitor tab. Additionally, as with all managed devices, you can
also generate reports that include PA-7000 Series log data by selecting Remote Device Data as the Data Source. If you later decide to enable the PA-7000 Series firewalls to forward logs to Panorama, you must first disable this option using the debug-reportd send-request-to-7k no command.

1. Select Network > Interfaces > Ethernet, select the Template of the firewalls that will forward logs, and Add Interface.
2. Select the Slot and Interface Name.
3. Set the Interface Type to Log Card.
4. Enter the IP Address, Default Gateway, and (for IPv4 only) Netmask.
5. Select Advanced and specify the Link Speed, Link Duplex, and Link State.

These fields default to auto, which specifies that the firewall automatically determines the values based on the connection. However, the minimum recommended Link Speed for any connection is 1000 (Mbps).

6. Click OK to save your changes.

STEP 7 | Configure Panorama to receive the logs.

If you will forward logs to a Panorama virtual appliance in Legacy mode, you can skip this step.

1. For each Log Collector that will receive logs, Configure a Managed Collector.
2. Configure a Collector Group to assign firewalls to specific Log Collectors for log forwarding.

STEP 8 | Commit your configuration changes.

1. Select Commit > Commit and Push and Edit Selections.
2. Select Merge with Device Candidate Config and Include Device and Network Templates, and click OK.

3. Commit and Push your changes to Panorama and push the changes to the device groups, templates, and Collector Groups.
4. Verify Log Forwarding to Panorama to confirm that your configuration is successful.
To change the log forwarding mode that the firewalls use to send logs to Panorama, you can Modify Log Forwarding and Buffering Defaults. You can also Manage Storage Quotas and Expiration Periods for Logs and Reports.
Verify Log Forwarding to Panorama

After you Configure Log Forwarding to Panorama or to the Logging Service test that your configuration succeeded.

After you configure log forwarding to Log Collectors, managed firewalls open a TCP connection to all configured Log Collectors. These connections timeout every sixty (60) seconds and do not indicate that the firewall has lost connection to the Log Collectors. When you configure log forwarding to a local or Dedicated Log Collector over an ethernet interface, the firewall traffic logs show **incomplete sessions** despite the firewall being able to successfully connect to the Log Collectors. If you configure log forwarding over the management port, no traffic logs showing **incomplete sessions** are generated. Traffic logs showing **incomplete sessions** are generated by all firewalls except for the PA-5200 and PA-7000 series firewalls.

**STEP 1 | Access the firewall CLI.**

**STEP 2 | If you configured Log Collectors, verify that each firewall has a log forwarding preference list.**

```shell
> show log-collector preference-list
```

If the Collector Group has only one Log Collector, the output will look something like this:

```
Forward to all: No
Log collector Preference List
Serial Number: 003001000024
IP Address: 10.2.133.48
IPV6 Address: unknown
```

**STEP 3 | Verify that each firewall is forwarding logs.**

```shell
> show logging-status
```

For successful forwarding, the output indicates that the log forwarding agent is active.

- For a Panorama virtual appliance, the agent is **Panorama**.
- For an M-500 appliance or M-100 appliance, the agent is **a LogCollector**.
- For the Logging Service, the agent is **Log CollectionService**. And the

```
'Log Collection log forwarding agent' is active and connected to <IP_address>.
```

**STEP 4 | View the average logging rate. The displayed rate will be the average logs/second for the last five minutes.**

- If Log Collectors receive the logs, access the Panorama web interface, select **Panorama** > **Managed Collectors** and click the **Statistics** link in the far-right column.
- If a Panorama virtual appliance in Legacy mode receives the logs, access the Panorama CLI and run the following command: **debug log-collector log-collection-stats show incoming-logs**
This command also works on an M-Series appliance.
Modify Log Forwarding and Buffering Defaults

You can define the log forwarding mode that the firewalls use to send logs to Panorama and, when configured in a high availability (HA) configuration, specify which Panorama peer can receive logs. To access these options, select **Panorama > Setup > Management**, edit the Logging and Reporting Settings, and select **Log Export and Reporting**.

- Define the log forwarding mode on the firewall: The firewalls can forward logs to Panorama (pertains to both the M-Series appliance and the Panorama virtual appliance) in either Buffered Log Forwarding mode or in the Live Mode Log Forwarding mode.

<table>
<thead>
<tr>
<th>Logging Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(Best Practice) Buffered Log Forwarding from Device</strong></td>
<td>Allows each managed firewall to buffer logs and send the logs at 30-second intervals to Panorama (not user configurable). Buffered log forwarding is very valuable when the firewall loses connectivity to Panorama. The firewall buffers log entries to its local hard disk and keeps a pointer to record the last log entry that was sent to Panorama. When connectivity is restored the firewall resumes forwarding logs from where it left off. The disk space available for buffering depends on the log storage quota for the firewall model and the volume of logs that are pending 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>
<tr>
<td><strong>Live Mode Log Forwarding from Device</strong></td>
<td>In live mode, the managed firewall sends every log transaction to Panorama at the same time as it records it on the firewall.</td>
</tr>
</tbody>
</table>

- Define log forwarding preference on a Panorama virtual appliance in Legacy mode that is deployed in a high availability (HA) configuration:
  - When logging to a virtual disk, enable logging to the local disk on the primary Panorama peer only. By default, both Panorama peers in the HA configuration receive logs.

  *For the 5200 and 7000 series firewalls, only the active peer receive logs.*

  - When logging to an NFS (ESXi server only), 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 in Legacy mode that is logging to a virtual disk and is deployed in an HA configuration.</td>
<td>Allows you to configure only the primary Panorama peer to save logs to the local disk.</td>
</tr>
<tr>
<td>Default: Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get Only New Logs on Convert to Primary</td>
<td>Panorama virtual appliance in Legacy mode that is mounted to a Network File System (NFS) datastore, runs on a VMware ESXi server, and is deployed in an HA configuration</td>
<td>With NFS logging, when you have a pair of Panorama servers configured in a high availability configuration, only the primary Panorama peer mounts the NFS datastore. Therefore, the firewalls can only send logs to the primary Panorama peer, which can write to the NFS datastore. When an HA failover occurs, the Get Only New Logs on Convert to Primary option allows an administrator to configure the managed firewalls to send only newly generated logs to Panorama. This event is triggered when the priority of the active-secondary Panorama is promoted to primary and it can begin logging to the NFS. This behavior is typically enabled to prevent the firewalls from sending a large volume of buffered logs when connectivity to Panorama is restored after a significant period of time.</td>
</tr>
<tr>
<td>Default: Disabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configure Log Forwarding from Panorama to External Destinations

Panorama enables you to forward logs to external services, including syslog, email, SNMP trap, and HTTP-based services. Using an external service enables you to receive alerts for important events, archive monitored information on systems with dedicated long-term storage, and integrate with third-party security monitoring tools. In addition to forwarding firewall logs, you can forward the logs that the Panorama management server and Log Collectors generate. The Panorama management server or Log Collector that forwards the logs converts them to a format that is appropriate for the destination (syslog message, email notification, SNMP trap, or HTTP payload).

If your Panorama management server is a Panorama virtual appliance in Legacy mode, it converts and forwards logs to external services without using Log Collectors.

You can also forward logs directly from firewalls to external services: see Log Forwarding Options.

On a Panorama virtual appliance running Panorama 5.1 or earlier releases, you can use Secure Copy (SCP) commands from the CLI to export the entire log database to an SCP server and import it to another Panorama virtual appliance. A Panorama virtual appliance running Panorama 6.0 or later releases, and M-Series appliances running any release, do not support these options because the log database on those models is too large for an export or import to be practical.

To forward logs to external services, start by configuring the firewalls to forward logs to Panorama. Then you must configure the server profiles that define how Panorama and Log Collectors connect to the services. Lastly, you assign the server profiles to the log settings of Panorama and to Collector Groups.

**STEP 1 |** Configure the firewalls to forward logs to Panorama.
Configure Log Forwarding to Panorama.

**STEP 2 |** Configure a server profile for each external service that will receive log information.

1. Select Panorama > Server Profiles and select the type of server that will receive the log data: **SNMP Trap**, **Syslog**, **Email**, or **HTTP**.
2. Configure the server profile:
   - **Configure an SNMP Trap server profile.** For details on how SNMP works for Panorama and Log Collectors, refer to SNMP Support.
   - **Configure a Syslog server profile.** If the syslog server requires client authentication, use the **Panorama > Certificate Management > Certificates** page to create a certificate for securing syslog communication over SSL.
   - **Configure an Email server profile.**
   - **Configure an HTTP server profile.**

**STEP 3 |** Configure destinations for:

- Logs that the Panorama management server and Log Collectors generate.
- Firewall logs that a Panorama virtual appliance in Legacy mode collects.

1. Select Panorama > Log Settings.
2. **Add** one or more **match list profiles** for each log type.
The profiles specify log query filters, forwarding destinations, and automatic actions such as tagging.
For each match list profile:
1. Enter a **Name** to identify the profile.
2. Select the **Log Type**.
3. In the **Filter** drop-down, select **Filter Builder**. Specify the following and then **Add** each query:
   - **Connector** logic (and/or)
   - **Log Attribute**
   - **Operator** to define inclusion or exclusion logic
   - **Attribute Value** for the query to match
4. **Add** the server profiles you configured for each external service.
5. Click **OK** to save the profile.

**STEP 4** | Configure destinations for firewall logs that Log Collectors receive.

*Each Collector Group can forward logs to different destinations. If the Log Collectors are local to a high availability (HA) pair of Panorama management servers, you must log into each HA peer to configure log forwarding for its Collector Group.*

1. Select **Panorama** > **Collector Groups** and edit the Collector Group that receives the firewall logs.
2. (Optional, SNMP trap forwarding only) Select **Monitoring** and configure the SNMP settings.
3. Select **Collector Log Forwarding** and see step **Add one or more match list profiles for each log type**.
4. Click **OK** to save your changes to the Collector Group.

**STEP 5** | (Syslog forwarding only) If the syslog server requires client authentication and the firewalls forward logs to Dedicated Log Collectors, assign a certificate that secures syslog communication over SSL.

Perform the following steps for each Dedicated Log Collector:
1. Select **Panorama** > **Managed Collectors** and edit the Log Collector.
2. Select the **Certificate for Secure Syslog** and click **OK**.

**STEP 6** | (SNMP trap forwarding only) Enable your SNMP manager to interpret traps.

Load the **Supported MIBs** and, if necessary, compile them. For the specific steps, refer to the documentation of your SNMP manager.

**STEP 7** | Commit and verify your configuration changes.

1. Select **Commit** > **Commit and Push** to commit your changes to Panorama and push the changes to device groups, templates, and Collector Groups.
2. Verify that the external services are receiving the log information:
   - **Email server**—Verify that the specified recipients are receiving logs as email notifications.
   - **Syslog server**—Refer to the documentation for your syslog server to verify it’s receiving logs as syslog messages.
   - **SNMP manager**—Refer to the documentation for your SNMP trap server to verify it’s receiving logs as SNMP traps.
   - **HTTP server**—Verify that the HTTP-based server is receiving logs in the correct payload format.
Log Collection Deployments

The following topics describe how to configure log collection in the most typical deployments. Before starting, Plan Your Panorama Deployment according to your current and future logging needs.

The deployments in these topics all describe Panorama in a high availability (HA) configuration. Palo Alto Networks recommends HA because it enables automatic recovery (in case of server failure) of components that are not saved as part of configuration backups. In HA deployments, the Panorama management server only supports an active/passive configuration.

- Deploy Panorama with Dedicated Log Collectors
- Deploy Panorama M-Series Appliances with Local Log Collectors
- Deploy Panorama Virtual Appliances with Local Log Collectors
- Deploy Panorama Virtual Appliances in Legacy Mode with Local Log Collection

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 or M-500 appliances in Panorama mode that are deployed in an active/passive high availability (HA) configuration. Alternatively, you can use an HA pair of Panorama virtual appliances. The firewalls send logs to Dedicated Log Collectors (M-Series appliances in Log Collector mode). This is the recommended configuration if the firewalls generate over 10,000 logs/second.

If you will assign more than one Log Collector to a Collector Group, see Caveats for a Collector Group with Multiple Log Collectors to understand the requirements, risks, and recommended mitigations.
Perform the following steps to deploy Panorama with Dedicated Log Collectors. Skip any steps you have already performed (for example, the initial setup).
STEP 1 | Perform the initial setup of the Panorama management server (virtual appliances or M-Series appliances) and the Dedicated Log Collectors.

For each M-Series appliance:

1. Rack mount the M-Series appliance. Refer to the M-100 or M-500 Hardware Reference Guide for instructions.
2. Perform Initial Configuration of the M-Series Appliance.

*Palo Alto Networks recommends reserving the management (MGT) interface for administrative access to Panorama and dedicating separate M-Series Appliance Interfaces to other Panorama services.*

3. Configure each array. This task is required to make the RAID disks available for logging. Optionally, you can add disks to Increase Storage on the M-Series Appliance.
4. Register Panorama and Install Licenses.
5. Install Content and Software Updates for Panorama.

For each virtual appliance (if any):

1. Install the Panorama Virtual Appliance.
2. Perform Initial Configuration of the Panorama Virtual Appliance.
3. Register Panorama and Install Licenses.
4. Install Content and Software Updates for Panorama.

For the Panorama management server (virtual appliance or M-Series appliance), you must also Set Up HA on Panorama.

STEP 2 | Switch from Panorama mode to Log Collector mode on each M-Series appliance that will be a Dedicated Log Collector.

*Switching the mode of an M-Series appliance deletes any existing log data and deletes all configurations except the management access settings. After the switch, the M-Series appliance retains CLI access but loses web interface access.*

1. Connect to the M-Series appliance in one of the following ways:
   - Attach a serial cable from your computer to the Console port on the M-Series appliance. Then use terminal emulation software (9600-8-N-1) to connect.
   - Use terminal emulation software such as PuTTY to open an SSH session to the IP address that you specified for the MGT interface of the M-Series appliance during initial configuration.
2. Log in to the CLI when prompted. Use the default admin account and the password that you specified during initial configuration.
3. Switch to Log Collector mode by entering the following command:
   > request system system-mode logger
4. Enter Y to confirm the mode change. The M-Series appliance reboots. If the reboot process terminates your terminal emulation software session, reconnect to the M-Series appliance to see the Panorama login prompt.

*If you see a CMS Login prompt, this means the Log Collector has not finished rebooting. Press Enter at the prompt without typing a username or password.*

5. Log back in to the CLI.
6. Verify that the switch to Log Collector mode succeeded:
STEP 3 | Enable connectivity between each Log Collector and the Panorama management server. This step is required before you can enable logging disks on the Log Collectors.

Enter the following commands at the CLI of each Log Collector. `<IPaddress1>` is for the MGT interface of the active Panorama and `<IPaddress2>` is for the MGT interface of the passive Panorama.

> configure
# set deviceconfig system panorama-server `<IPaddress1>` panorama-server-2 `<IPaddress2>`
# commit
# exit

STEP 4 | Record the serial number of each Log Collector.

You need the serial numbers to add the Log Collectors as managed collectors on the Panorama management server.

1. At the CLI of each Log Collector, enter the following command to display its serial number.

> show system info | match serial

2. Record the serial number.

STEP 5 | Add each Log Collector as a managed collector.

Use the web interface of the primary Panorama management server peer to Configure a Managed Collector:

1. Select Panorama > Managed Collectors and Add the managed collector.
2. In the General tab, enter the serial number (Collector S/N) you recorded for the Log Collector.
3. Enter the IP address or FQDN of the active and passive Panorama HA peers in the Panorama Server IP field and Panorama Server IP 2 field respectively. These fields are required.
4. Select Interfaces, click Management, and configure one or both of the following field sets for the MGT interface based on the IP protocols of your network.
   - IPv4—IP Address, Netmask, and Default Gateway
   - IPv6—IPv6 Address/Prefix Length and Default IPv6 Gateway
5. (Optional) Select SNMP if you will use an SNMP manager to monitor Log Collector statistics.
   - Using SNMP requires additional steps besides configuring the Log Collector (see Monitor Panorama and Log Collector Statistics Using SNMP).
6. Click OK to save your changes.
7. Select Commit > Commit to Panorama and Commit your changes.
   - This step is required before you can enable logging disks on the Log Collectors.
8. Verify that the Panorama > Managed Collectors page lists the Log Collector you added. The Connected column displays a check mark to indicate that the Log Collector is connected to
At this point, the Configuration Status column displays Out of Sync and the Run Time Status column displays disconnected. The status will change to In Sync and connected after you configure a Collector Group (Step 9).

**STEP 6** | Enable the logging disks on each Log Collector.

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

1. Select Panorama > Managed Collectors and edit the Log Collector.
2. Select Disks, Add each disk pair, and click OK.
3. Select Commit > Commit to Panorama and Commit your changes.

**STEP 7** | (Recommended) Configure the Ethernet1, Ethernet2, Ethernet3, Ethernet4, and Ethernet5 interfaces if the Log Collector will use them for Device Log Collection (receiving logs from firewalls) and Collector Group Communication.

By default, the Log Collector uses the MGT interface for log collection and Collector Group communication. Assigning other interfaces to these functions enables you to reserve the MGT interface for management traffic. In an environment with heavy log traffic, consider using the 10Gbps interfaces (Ethernet4 and Ethernet5) on the M-500 appliance for log collection and Collector Group communication. To load balance the logging traffic across interfaces, you can enable Device Log Collection on multiple interfaces.

Use the web interface of the primary Panorama management server peer to perform these steps for each Log Collector:

1. Select Panorama > Managed Collectors, edit the Log Collector, and select Interfaces.
2. Perform the following steps for each interface:
   1. Click the name of the interface to edit it.
   2. Select <interface-name> to enable the interface.
   3. Complete one or both of the following field sets based on the IP protocols of your network:
      - IPv4—IP Address, Netmask, and Default Gateway
      - IPv6—IPv6 Address/Prefix Length and Default IPv6 Gateway
   4. Select the Device Management Services that the interface supports:
      - Device Log Collection—You can assign one or more interfaces.
      - Collector Group Communication—You can assign only one interface.
   5. Click OK to save your changes to the interface.
3. Click OK to save your changes to the Log Collector.
4. Select Commit > Commit to Panorama and Commit your changes to the Panorama configuration.

**STEP 8** | Add a Firewall as a Managed Device.

Use the web interface of the primary Panorama management server peer to perform this task for each firewall that will forward logs to Log Collectors.

**STEP 9** | Configure the Collector Group.

If each Collector Group will have one Log Collector, repeat this step for each Collector Group before continuing.

If you will assign all the Log Collectors to one Collector Group, perform this step only once.
Use the web interface of the primary Panorama management server peer to Configure a Collector Group:

1. Select Panorama > Collector Groups and Add the Collector Group.
2. Enter a Name to identify the Collector Group.
3. Add one or more Log Collectors to the Collector Group Members list.

- In any single Collector Group, all the Log Collectors must run on the same Panorama model: all M-500 appliances, all M-100 appliances, or all Panorama virtual appliances.

4. (Best Practice) Enable log redundancy across collectors if you add multiple Log Collectors to a single Collector group. This option requires each Log Collector to have the same number of logging disks.
5. (Optional) Select Monitoring and configure the settings if you will use SNMP to monitor Log Collector statistics and traps.
6. Select Device Log Forwarding and configure the Log Forwarding Preferences list. This list defines which firewalls forward logs to which Log Collectors. Assign firewalls according to the number of Log Collectors in this Collector Group:
   - Single—Assign the firewalls that will forward logs to that Log Collector, as illustrated in Single Dedicated Log Collector Per Collector Group.
   - Multiple—Assign each firewall to both Log Collectors for redundancy. When you configure the preferences, make Log Collector 1 the first priority for half the firewalls and make Log Collector 2 the first priority for the other half, as illustrated in Multiple Dedicated Log Collectors Per Collector Group.
7. Click OK to save your changes to the Collector Group.
8. Select Commit > Commit and Push and then Commit and Push your changes to Panorama and to the Collector Groups you added.
9. Select Panorama > Managed Collectors to verify that the Log Collector configuration is synchronized with Panorama.
   - The Configuration Status column should display In Sync and the Run Time Status column should display connected.

STEP 10 | Configure log forwarding from firewalls to Panorama.

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

1. Configure Log Forwarding to Panorama.
2. Verify Log Forwarding to Panorama.
3. (Optional) Configure Log Forwarding from Panorama to External Destinations.

Deploy Panorama M-Series Appliances with Local Log Collectors

The following figures illustrate Panorama in a centralized log collection deployment. In these examples, the Panorama management server comprises two M-Series appliances in Panorama mode that are deployed in an active/passive high availability (HA) configuration. The firewalls send logs to the predefined (default) local Log Collector on each Panorama M-Series appliance. This is the recommended deployment if the firewalls generate up to 10,000 logs/second.

- If you will assign more than one Log Collector to a Collector Group, see Caveats for a Collector Group with Multiple Log Collectors to understand the requirements, risks, and recommended mitigations.

After implementing this deployment, if the logging rate increases beyond 10,000 logs per second, Palo Alto Networks recommends that you add Dedicated Log Collectors (M-Series appliances in Log Collector mode) as described in Deploy Panorama with Dedicated
Log Collectors. Such an expansion might require reassigning firewalls from the local Log Collectors to Dedicated Log Collectors.

**Figure 18: Single Local Log Collector Per Collector Group**

**Figure 19: Multiple Local Log Collectors Per Collector Group**

Perform the following steps to deploy Panorama with local Log Collectors. Skip any steps you have already performed (for example, the initial setup).

**STEP 1** | Perform the initial setup of each M-Series appliance.

1. Rack mount the M-Series appliance. Refer to the M-100 or M-500 Hardware Reference Guide for instructions.
2. **Perform Initial Configuration of the M-Series Appliance.**

   *Palo Alto Networks recommends reserving the management (MGT) interface for administrative access to Panorama and dedicating separate M-Series Appliance Interfaces to other Panorama services.*

3. **Configure each array.** This task is required to make the RAID disks available for logging. Optionally, you can add disks to *Increase Storage on the M-Series Appliance.*

4. **Register Panorama and Install Licenses.**

5. **Install Content and Software Updates for Panorama.**

6. **Set Up HA on Panorama.**

---

### STEP 2 | Perform the following steps to prepare Panorama for log collection.

1. Connect to the primary Panorama in one of the following ways:
   - Attach a serial cable from your computer to the Console port on the primary Panorama. Then use terminal emulation software (9600-8-N-1) to connect.
   - Use terminal emulation software such as PuTTY to open an SSH session to the IP address that you specified for the MGT interface of the primary Panorama during initial configuration.

2. Log in to the CLI when prompted. Use the default admin account and the password that you specified during initial configuration.

3. Enable the primary Panorama to connect to the secondary Panorama by entering the following command, where `<IPaddress2>` represents the MGT interface of the secondary Panorama:

   ```
   > configure
   # set deviceconfig system panorama-server <IPaddress2>
   # commit
   ```

4. Log in to the CLI of the secondary Panorama.

5. Enable the secondary Panorama to connect to the primary Panorama by entering the following command, where `<IPaddress1>` represents the MGT interface of the primary Panorama:

   ```
   > configure
   # set deviceconfig system panorama-server <IPaddress1>
   # commit
   # exit
   ```

6. In the CLI of the secondary Panorama, enter the following command to display the serial number, and then record it:

   ```
   > show system info | match serial
   ```

   You need the serial number to add the Log Collector of the secondary Panorama as a managed collector to the primary Panorama.

### STEP 3 | Edit the Log Collector that is local to the primary Panorama.

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

1. Select **Panorama** > **Managed Collectors** and select the default (local) Log Collector.
2. Select **Disks** and **Add** each logging disk pair.
3. Click **OK** to save your changes.

### STEP 4 | Configure the Log Collector that is local to the secondary Panorama.
Panorama treats this Log Collector as remote because it’s not local to the primary Panorama. Therefore you must manually add it on the primary Panorama.

Use the web interface of the primary Panorama to Configure a Managed Collector:

1. Select **Panorama > Managed Collectors** and **Add** the Log Collector.
2. Enter the serial number (**Collector S/N**) you recorded for the Log Collector of the secondary Panorama.
3. Enter the IP address or FQDN of the primary and secondary Panorama HA peers in the **Panorama Server IP** field and **Panorama Server IP 2** field respectively. These fields are required.
4. Select **Interfaces** and configure each interface that the Log Collector will use. The **Management** interface is required. Perform the following steps for each interface:
   1. Click the interface name.
   2. Configure one or both of the following field sets based on the IP protocols of your network.
      - **IPv4**—IP Address, Netmask, and Default Gateway
      - **IPv6**—IPv6 Address/Prefix Length and Default IPv6 Gateway
     3. **(Management interface only)** Select **SNMP** if you will use an SNMP manager to monitor Log Collector statistics.

        Using SNMP requires additional steps besides configuring the Log Collector (see **Monitor Panorama and Log Collector Statistics Using SNMP**).
    4. Click **OK** to save your changes to the interface.
    5. Click **OK** to save your changes to the Log Collector.
6. Select **Commit > Commit to Panorama** and **Commit** your changes.

   This step is required before you can enable logging disks.
7. Edit the Log Collector by clicking its name.
8. Select **Disks**, **Add** each RAID disk pair, and click **OK**.
9. Select **Commit > Commit to Panorama** and **Commit** your changes.

**STEP 5 | Add a Firewall as a Managed Device.**

Use the web interface of the primary Panorama to perform this task for each firewall that will forward logs to the Log Collectors.

**STEP 6 | Edit the default Collector Group that is predefined on the primary Panorama.**

Use the web interface of the primary Panorama to **Configure a Collector Group**:

1. Select **Panorama > Collector Groups** and edit the **default** Collector Group.
2. **Add** the local Log Collector of the secondary Panorama to the Collector Group Members list if you are adding multiple Log Collectors to a single Collector group. By default, the list displays the local Log Collector of the primary Panorama because it is pre-assigned to the default Collector Group.

   **In any single Collector Group, all the Log Collectors must run on the same Panorama model:** all M-500 appliances, all M-100 appliances, or all Panorama virtual appliances.

3. **(Best Practice) Enable log redundancy across collectors** if you add multiple Log Collectors to a single Collector group. This option requires each Log Collector to have the same number of logging disks.
4. **(Optional) Select Monitoring** and configure the settings if you will use SNMP to monitor Log Collector statistics and traps.
5. Select **Device Log Forwarding** and configure the Log Forwarding Preferences list. This list defines which firewalls forward logs to which Log Collectors. Assign firewalls according to the number of Log Collectors in this Collector Group:
• **Single**—Assign the firewalls that will forward logs to the local Log Collector of the primary Panorama, as illustrated in Single Local Log Collector Per Collector Group.
• **Multiple**—Assign each firewall to both Log Collectors for redundancy. When you configure the preferences, make Log Collector 1 the first priority for half the firewalls and make Log Collector 2 the first priority for the other half, as illustrated in Multiple Local Log Collectors Per Collector Group.

6. Click OK to save your changes.

**STEP 7 |** Configure a Collector Group that contains the Log Collector of the secondary Panorama.

Required if each Collector Group has only one Log Collector.

Use the web interface of the primary Panorama to Configure a Collector Group:

1. Select Panorama > Collector Groups and Add the Collector Group.
2. Enter a Name to identify the Collector Group.
3. Add the local Log Collector of the secondary Panorama to the Collector Group Members list.
4. (Optional) Select Monitoring and configure the settings if you will use an SNMP manager to monitor Log Collector statistics and traps.
5. Select Device Log Forwarding and Add an entry to the Log Forwarding Preferences list:
   1. Modify the Devices list, select the firewalls that will forward logs to the local Log Collector of the secondary Panorama (see Single Local Log Collector Per Collector Group), and click OK.
   2. Add the local Log Collector of the secondary Panorama to the Collectors list and click OK.
6. Click OK to save your changes.

**STEP 8 |** Commit and push your changes to the Panorama configuration and the Collector Groups.

In the web interface of the primary Panorama, select Commit > Commit and Push and then Commit and Push your changes to Panorama and the Collector Groups you added.

**STEP 9 |** Manually fail over so that the secondary Panorama becomes active.

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

1. Select Panorama > High Availability.
2. Click Suspend local Panorama in the Operational Commands section.

**STEP 10 |** On the secondary Panorama, configure the network settings of the Log Collector that is local to the primary Panorama.

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

1. In the Panorama web interface, select Panorama > Managed Collectors and select the Log Collector that is local to the primary Panorama.
2. Enter the IP address or FQDN of the secondary Panorama in the Panorama Server IP field and the IP address or FQDN of the primary Panorama in the Panorama Server IP 2 field. These fields are required.
3. Select Interfaces, click Management, and complete one or both of the following field sets (based on the IP protocols of your network) with the MGT interface values of the primary Panorama:
   - **IPv4**—IP Address, Netmask, and Default Gateway
   - **IPv6**—IPv6 Address/PREFIX Length and Default IPv6 Gateway
4. Click OK to save your changes.
5. Select Commit > Commit and Push and then Commit and Push your changes to Panorama and the Collector Groups you added.
STEP 11 | Manually fail back so that the primary Panorama becomes active.  

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

1. Select Panorama > High Availability.
2. Click Suspend local Panorama in the Operational Commands section.

STEP 12 | Configure log forwarding from firewalls to Panorama.

Use the web interface of the primary Panorama to:

1. Configure Log Forwarding to Panorama.
2. Verify Log Forwarding to Panorama.
3. (Optional) Configure Log Forwarding from Panorama to External Destinations.

You can assign separate external server profiles to each Panorama HA peer. For example, you might want each peer to forward logs to a different syslog server. To make each Panorama peer forward logs to different external services, log in to the web interface of each peer, select Panorama > Collector Groups, select the Collector Group, select Collector Log Forwarding, assign the server profiles, and click OK.

Deploy Panorama Virtual Appliances with Local Log Collectors

You can configure firewalls to send logs to a Log Collector that runs locally on a Panorama virtual appliance in Panorama mode. In a high availability (HA) configuration, each Panorama HA peer can have a local Log Collector. You can assign the local Log Collectors on the HA peers to the same Collector Group or to separate Collector Groups, as illustrated in the following figures. Deploying the Panorama virtual appliance with local Log Collectors suits firewall management within a VMware virtual infrastructure in which Panorama processes up to 10,000 logs per second.

The Panorama virtual appliance cannot be a Dedicated Log Collector. However, if the logging rate increases beyond 10,000 logs per second, you can use the virtual appliance to manage Dedicated Log Collectors as described in Deploy Panorama with Dedicated Log Collectors. Such an expansion might require reassigning firewalls from the local Log Collectors to Dedicated Log Collectors.

If you will assign more than one Log Collector to a Collector Group, see Caveats for a Collector Group with Multiple Log Collectors to understand the requirements, risks, and recommended mitigations.
Figure 20: Single Log Collector Per Collector Group

Figure 21: Multiple Log Collectors Per Collector Group
Perform the following steps to deploy Panorama with local Log Collectors. Skip any steps you have already performed (such as the initial setup).

**STEP 1 |** Perform the initial setup of each Panorama virtual appliance.

1. **Install Panorama on an ESXi Server.** You must configure the following resources to ensure the virtual appliance starts in Panorama mode:
   - System disk with exactly 81GB of storage.
   - **CPUs and memory** that are sufficient for the quantity of logs that Panorama will receive and store.
   - Virtual logging disk with 2–24TB of storage.

   *Panorama automatically divides the new disk into 2TB partitions, each of which will function as a separate virtual disk.*

2. **Perform Initial Configuration of the Panorama Virtual Appliance.**
3. **Register Panorama and Install Licenses.**
4. **Install Content and Software Updates for Panorama.**

**STEP 2 |** Set up the Panorama virtual appliances in an HA configuration.

1. **Set Up HA on Panorama.**
2. **Test Panorama HA Failover.**

**STEP 3 |** Add a Log Collector that is local to the primary Panorama.

On the primary Panorama:

1. Record the Panorama serial number.
   1. Access the Panorama web interface.
   2. Select **Dashboard** and record the **Serial #** in the General Information section.
2. Add the Log Collector as a managed collector.
   1. Select **Panorama** > **Managed Collectors** and **Add** a new Log Collector.
   2. In the **General** settings, enter the serial number (**Collector S/N**) you recorded for Panorama.
   3. Click **OK** to save your changes.
   4. Select **Commit** > **Commit to Panorama**.

   This step is required before you can add the virtual logging disks.

3. Add the virtual logging disks.
   1. Select **Panorama** > **Managed Collectors** and edit the Log Collector by clicking its name.
   2. Select **Disks** and **Add** the virtual logging disks.
   3. Click **OK** to save your changes.
   4. Select **Commit** > **Commit to Panorama**.

**STEP 4 |** Add a Log Collector that is local to the secondary Panorama.

*Panorama treats this Log Collector as remote because it does not run locally on the primary Panorama.*

1. Record the serial number of the secondary Panorama.
   1. Access the web interface of the secondary Panorama.
   2. Select **Dashboard** and record the **Serial #** in the General Information section.
2. Access the web interface of the primary Panorama.
3. Select Panorama > Managed Collectors and Add the Log Collector.
4. In the General settings, enter the serial number (Collector S/N) you recorded for the secondary Panorama.
5. Enter the IP address or FQDN of the primary and secondary Panorama HA peers in the Panorama Server IP field and Panorama Server IP 2 field respectively.
6. Click OK to save your changes to the Log Collector.
7. Select Commit > Commit to Panorama and Commit your changes.

   This step is required before you can add the virtual logging disks.
8. Edit the Log Collector by clicking its name.

   The Log Collector name has the same value as the hostname of the secondary Panorama.
9. Select Disks, Add the virtual logging disks, and click OK.
10. Select Commit > Commit to Panorama and Commit your changes.

STEP 5 | Add a Firewall as a Managed Device.

Use the primary Panorama to perform this task for each firewall that will forward logs to the Log Collectors.

STEP 6 | Configure the Collector Group.

Perform this step once if you will assign both Log Collectors to the same Collector Group. Otherwise, configure a Collector Group for each Log Collector.

On the primary Panorama:
1. Select Panorama > Collector Groups and Add a Collector Group.
2. Add one or both Log Collectors as Collector Group Members.

   In any single Collector Group, all the Log Collectors must run on the same Panorama model: all M-500 appliances, all M-100 appliances, or all Panorama virtual appliances.
3. (Best Practice) Enable log redundancy across collectors if you add multiple Log Collectors to a single Collector group. This option requires each Log Collector to have the same number of virtual logging disks.

   Enabling redundancy doubles the amount of logs and log processing traffic in a Collector Group. If necessary, Expand Log Storage Capacity on the Panorama Virtual Appliance.
4. Select Device Log Forwarding and configure the Log Forwarding Preferences list. This list defines which firewalls forward logs to which Log Collectors. Assign firewalls according to the number of Log Collectors in this Collector Group:
   - Single—Assign the firewalls that will forward logs to the Log Collector that is local to the primary Panorama, as illustrated in Figure 20: Single Log Collector Per Collector Group.
   - Multiple—Assign each firewall to both Log Collectors for redundancy. When you configure the preference list, 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 21: Multiple Log Collectors Per Collector Group.
5. Click OK to save your changes.
6. Select Commit > Commit and Push and then Commit and Push your changes to Panorama and the Collector Groups you added.

STEP 7 | Trigger failover on the primary Panorama so that the secondary Panorama becomes active.

On the primary Panorama:
1. Select Panorama > High Availability.
2. Click Suspend local Panorama in the Operational Commands section.

**STEP 8** | Configure the connection from the secondary Panorama to the Log Collector that is local to the primary Panorama.

On the secondary Panorama:

1. In the Panorama web interface, select Panorama > Managed Collectors and select the Log Collector that is local to the primary Panorama.
2. Enter the IP address or FQDN of the secondary Panorama in the Panorama Server IP field and the IP address or FQDN of the primary Panorama in the Panorama Server IP 2 field.
3. Click OK to save your changes.
4. Select Commit > Commit and Push and then Commit and Push your changes to Panorama and the Collector Groups.

**STEP 9** | Trigger fail-back on the secondary Panorama so that the primary Panorama becomes active.

On the secondary Panorama:

1. Select Panorama > High Availability.
2. Click Suspend local Panorama in the Operational Commands section.

**STEP 10** | Configure log forwarding from the firewalls to Panorama.

On the primary Panorama to:

1. Configure Log Forwarding to Panorama from firewalls.
2. Verify Log Forwarding to Panorama.

**Deploy Panorama Virtual Appliances in Legacy Mode 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 in Legacy mode that are deployed in an active/passive high availability (HA) configuration. This configuration suits firewall management within a VMware virtual infrastructure in which Panorama processes up to 10,000 logs/second. The firewalls send logs to the NFS datastore (ESXi server only) or virtual disk on the Panorama management server. By default, the active and passive peers both receive logs, though you can Modify Log Forwarding and Buffering Defaults so that only the active peer does. For the 5200 and 7000 series firewalls, only the active peer receive logs. By default, the Panorama virtual appliance in Legacy mode uses approximately 11GB on its internal disk partition for log storage, though you can Expand Log Storage Capacity on the Panorama Virtual Appliance if necessary.

- If the logging rate increases beyond 10,000 logs per second, it is recommended that you Deploy Panorama with Dedicated Log Collectors.
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).

**STEP 1 |** Perform the initial setup of each Panorama virtual appliance.

1. **Install the Panorama Virtual Appliance.** To ensure the virtual appliance starts in Panorama mode, do not add a virtual logging disk during installation.

   By default, Panorama uses an 11GB partition on its system disk for log storage. If you want more storage, you can add a dedicated virtual logging disk of up to 8TB after the installation.

2. **Perform Initial Configuration of the Panorama Virtual Appliance.**
3. **Register Panorama and Install Licenses.**
4. **Install Content and Software Updates for Panorama.**

**STEP 2 |** Set up the Panorama virtual appliances in an HA configuration.

1. **Set Up HA on Panorama.**
2. **Test Panorama HA Failover.**

**STEP 3 |** Perform the following steps to prepare Panorama for log collection.

1. **Add a Firewall as a Managed Device** for each one that will forward logs to Panorama.
2. **Configure Log Forwarding to Panorama.**

**STEP 4 |** Commit your changes.

Select **Commit > Commit to Panorama** and **Commit** your changes.
Manage WildFire Appliances

You can manage up to 200 standalone WildFire appliances and WildFire appliance cluster nodes centrally using a Panorama M-Series or virtual appliance. Compared to managing WildFire appliances and appliance clusters individually using the local CLI, using Panorama provides centralized management and monitoring of multiple appliances and appliance clusters. Centralized management enables you to push common configurations, configuration updates, and software upgrades to all or a subset of the managed WildFire appliances, which makes it easy to ensure that WildFire appliances and appliance clusters have consistent configurations.

When you use Panorama to manage WildFire appliance clusters, Panorama must run version 8.0.1 or later. WildFire appliances and WildFire appliance clusters that you manage with Panorama also must run PAN-OS 8.0.1 or later.

> Add Standalone WildFire Appliances to Manage with Panorama
> Configure Basic WildFire Appliance Settings on Panorama
> Remove a WildFire Appliance from Panorama Management
Add Standalone WildFire Appliances to Manage with Panorama

You can manage up to 200 WildFire appliances with a Panorama M-Series or virtual appliance. The 200 WildFire appliance limit is the combined total of standalone appliances and WildFire appliance cluster nodes (if you also Configure a Cluster and Add Nodes on Panorama).

Ensure that Panorama runs at least version 8.0.1, and that any WildFire appliance you add to Panorama also runs at least version 8.0.1.

**STEP 1 |** Using the local CLI, verify that each WildFire appliance that you want to manage with Panorama runs PAN-OS 8.0.1 or later.

```
admin@qa16> show system info | match version
sw-version: 8.0.1-c45
wf-content-version: 702-283
logdb-version: 8.0.15
```

**STEP 2 |** On each Panorama appliance you want to use to manage WildFire appliances, verify that Panorama runs version 8.0.1 or later:

Dashboard > General Information > Software Version displays the running software version.

**STEP 3 |** If you aren’t sure if a WildFire appliance belongs to a WildFire appliance cluster or is a standalone appliance on the local WildFire appliance CLI, check the **Node mode** to ensure that the status is **stand_alone** and check the **Application status** to ensure that the **global-db-service** and **global-queue-service** indicate **ReadyStandalone**.

```
admin@WF-500> show cluster membership
Service Summary:  wfpc signature
Cluster name:      
Address:          10.10.10.100
Host name:        WF-500
Node name:        wfpc-012345678901-internal
Serial number:    012345678901
Node mode:        stand_alone
Server role:      True
HA priority:      
Last changed:     Mon, 06 Mar 2017 16:34:25 -0800
Services:         wfcore signature wfpc infra
Monitor status:   Serf Health Status: passing
                  Agent alive and reachable
Application status:
  global-db-service: ReadyStandalone
  wildfire-apps-service: Ready
  global-queue-service: ReadyStandalone
  wildfire-management-service: Done
  siggen-db: ReadyMaster
Diag report:      10.10.10.100: reported leader '10.10.10.100', age 0.
                  10.10.10.100: local node passed sanity check.
```
STEP 4 | If the WildFire appliances you want to manage with Panorama are new, check Get Started with WildFire to ensure that you complete basic steps such as confirming your WildFire license is active, enabling logging, connecting firewalls to WildFire appliances, and configuring basic WildFire features.

STEP 5 | On the local CLI of each WildFire appliance the Panorama server will manage, configure the IP address of the Panorama server.

Before you register standalone WildFire appliances to a Panorama appliance, you must first configure the Panorama IP address or FQDN on each WildFire appliance. This is how each WildFire appliance knows which Panorama appliance manages it.

1. Configure the IP address or FQDN of the primary Panorama appliance's management interface:

   ```
   admin@WF-500# set deviceconfig system panorama-server <ip-address | FQDN>
   ```

2. If you use a backup Panorama appliance for high availability (recommended), configure the IP address or FQDN of the backup Panorama appliance's management interface:

   ```
   admin@WF-500# set deviceconfig system panorama-server-2 <ip-address | FQDN>
   ```

STEP 6 | Register WildFire appliances on the primary Panorama appliance.

1. From the Panorama web interface, Panorama > Managed WildFire Appliances and Add Appliance.
2. Enter the serial number of each WildFire appliance on a separate line. If you do not have a list of serial numbers, on each WildFire appliance, run:

   ```
   admin@WF-500> show system info | match serial
   serial: 012345678901
   ```

   Several local CLI commands display the WildFire appliance serial number, including show cluster membership.

3. Click OK.

   If it is available, information about configuration that is already committed on the WildFire appliances displays, such as IP address and software version.

STEP 7 | (Optional) Import WildFire appliance configurations into the Panorama appliance.

1. Select the appliances that have configurations you want to import from the list of managed WildFire appliances.
2. Import Config.
3. Select Yes.

   Importing configurations updates the displayed information and makes the imported configurations part of the Panorama appliance candidate configuration.

4. Commit to Panorama to make the imported WildFire appliance configurations part of the Panorama running configuration.

STEP 8 | Configure or confirm the configuration of the WildFire appliance interfaces.

Each WildFire appliance has four interfaces: Management (Ethernet0), Analysis Network Environment (Ethernet1), Ethernet2, and Ethernet3.

1. Select Panorama > Managed WildFire Appliances and select a WildFire appliance.
2. Select Interfaces.
3. Select an interface to configure or edit it. You can enable the interface, set the speed and duplex, the IP address and netmask, the default gateway, the MTU, the DNS server, the link state, and the Management Services for each interface. You can also Add permitted IP addresses so that an interface accepts traffic only from specified addresses.

The Analysis Network Environment, Ethernet2, and Ethernet3 interfaces support only Ping as a Management Services option.

The Management interface supports Ping, SSH, and SNMP as Management Services options. In addition, the Management interface supports proxy server configuration in case a direct connection to the internet is not possible.

4. Click OK after you configure or confirm the settings.

**STEP 9** | Commit the configuration on the Panorama appliance and push it to the appliance or to multiple appliances.

1. **Commit and Push.**
2. If there are configurations on the Panorama appliance that you do not want to push, Edit Selections to choose the appliances to which you push configurations. The pushed configuration overwrites the running configuration on the WildFire appliance.

**STEP 10** | Verify the configuration.

1. Select Panorama > Managed WildFire Appliances.
2. Check the following fields:
   - **Connected**—State is Connected.
   - **Role**—Each WildFire appliance's role is Standalone.
   - **Config Status**—Status is In Sync.
   - **Last Commit State**—Commit succeeded.
Configure Basic WildFire Appliance Settings on Panorama

Configuring basic settings such as content update and WildFire cloud servers, WildFire cloud services, logging, authentication, and so on, is similar to how you Configure General Cluster Settings on Panorama. Instead of selecting a cluster and configuring settings on the cluster, select a WildFire appliance and configure the individual settings for that appliance. Select and configure each WildFire appliance that you add to Panorama.

Configure the WildFire Appliance describes how to integrate a WildFire appliance into a network and perform basic setup with the CLI, but the concepts are the same as performing basic setup using Panorama.

Many settings are pre-populated with either defaults, information from previously existing settings on the WildFire appliance, or the settings you configured when adding the WildFire appliance to Panorama.
Remove a WildFire Appliance from Panorama Management

You can remove WildFire standalone appliances from Panorama management. When you remove a standalone WildFire appliance from Panorama management, you no longer enjoy the benefits of centralized management and must manage the appliance using its local CLI and scripts.

**STEP 1** | Select Panorama > Managed WildFire Appliances.

**STEP 2** | Select the WildFire appliance or appliances you want to remove from Panorama management by selecting the checkbox next to each appliance or by clicking in an appliance's row.

**STEP 3** | Remove the selected WildFire appliances from Panorama management.
Manage Licenses and Updates

You can use the Panorama™ management server to centrally manage licenses, software updates, and content updates on firewalls and Dedicated 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 or update. This capability facilitates deployment by eliminating the need to repeat the same tasks on each firewall or Dedicated Log Collector. It is particularly useful for managing firewalls that don’t have direct Internet access or for managing Dedicated Log Collectors, which don’t have a web interface.

Before deploying updates, see Panorama, Log Collector, Firewall, and WildFire Version Compatibility for important details about update version compatibility.

You must activate a support subscription directly on each firewall; you cannot use Panorama to deploy support subscriptions.

To activate licenses or install updates on the Panorama management server, see Register Panorama and Install Licenses and Install Content and Software Updates for Panorama.

- Manage Licenses on Firewalls Using Panorama
- Deploy Updates to Firewalls, Log Collectors and WildFire Appliances Using Panorama
Manage Licenses on Firewalls Using Panorama

The following steps describe how to retrieve new licenses using an authentication (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 a.m. and 2 a.m.; you cannot change this schedule.

You cannot use Panorama to activate the support license for firewalls. You must access the firewalls individually to activate their support licenses.

To activate licenses for Panorama, see Register Panorama and Install Licenses.

• Activate newly purchased licenses.
  1. Select Panorama > Device Deployment > Licenses and Activate.
  2. Enter the Auth Code that Palo Alto Networks® provided for each firewall that has a new license.
  3. Activate the license.
  4. (WildFire® subscriptions only) Perform a commit on each firewall that has a new WildFire subscription to complete the activation:
     • Commit any pending changes. You must access each firewall web interface to do this.
     • If no configuration changes are pending, make a minor change and Commit it. For example, update a rule description and commit the change. If the firewalls belong to the same device group, you can push the rule change from Panorama to initiate a commit on all those firewalls instead of accessing each firewall separately.

Check that the WildFire Analysis profile rules include the advanced file types that the WildFire subscription supports.

• Update the license status of firewalls.
  1. Select Panorama > Device Deployment > Licenses.
     Each entry on the page indicates whether the license is active or inactive and displays the expiration date for active licenses.
  2. If you previously activated auth codes for the support subscription directly on the firewalls, click Refresh and select the firewalls from the list. Panorama retrieves the license, deploys it to the firewalls and updates the licensing status on the Panorama web interface.
Deploy Updates to Firewalls, Log Collectors, and WildFire Appliances Using Panorama

You can use Panorama™ to qualify software and content updates by deploying them to a subset of firewalls, Dedicated Log Collectors, or WildFire® appliances and appliance clusters before installing the updates on the rest of your managed appliances. If you want to schedule periodic content updates, Panorama requires a direct Internet connection. To deploy software or content updates on demand (unscheduled), the procedure differs based on whether Panorama is connected to the internet. Panorama displays a warning if you manually deploy a content update when a scheduled update process has started or will start within five minutes.

When deploying updates, Panorama notifies the managed appliances (firewalls, Log Collectors, and WildFire appliances) that updates are available and the appliances then retrieve the update packages from Panorama. By default, managed appliances retrieve updates over the management (MGT) interface on Panorama. However, if you want to reduce the traffic load on the MGT interface by using another interface for appliances to retrieve updates, you can Configure Panorama to Use Multiple Interfaces.

By default, you can download up to two software or content updates of each type to Panorama. When you start any download beyond that maximum, Panorama deletes the oldest update of the selected type. To change the maximum, see Manage Panorama Storage for Software and Content Updates.

- Supported Updates
- Schedule a Content Update Using Panorama
- Upgrade Log Collectors When Panorama Is Internet-Connected
- Upgrade Log Collectors When Panorama Is Not Internet-Connected
- Upgrade Firewalls When Panorama Is Internet-Connected
- Upgrade Firewalls When Panorama Is Not Internet-Connected

Supported Updates

The software and content updates you can install vary based on which subscriptions are active on each firewall, Log Collector, and WildFire® appliance and appliance cluster:

<table>
<thead>
<tr>
<th>Appliance Type</th>
<th>Software Updates</th>
<th>Content Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Collector</td>
<td>Panorama™</td>
<td>Applications (Log Collectors don’t need Threats signatures)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Antivirus</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BrightCloud URL filtering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WildFire</td>
</tr>
<tr>
<td>Firewall</td>
<td>PAN-OS®</td>
<td>Applications</td>
</tr>
<tr>
<td></td>
<td>GlobalProtect™ agent/app</td>
<td>Applications and Threats</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Antivirus</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BrightCloud URL filtering</td>
</tr>
</tbody>
</table>
Schedule a Content Update Using Panorama

Panorama™ requires a direct internet connection for scheduling Supported Updates on firewalls, Log Collectors, and WildFire® appliances and appliance clusters. Otherwise, you can perform only on-demand updates. (To schedule Antivirus, WildFire, or BrightCloud URL updates for Log Collectors, the Log Collectors must be running Panorama 7.0.3 or a later release.) Each firewall, Log Collector, or WildFire appliance or appliance cluster receiving an update generates a log to indicate that the installation succeeded (a Config log) or failed (a System log). To schedule updates on the Panorama management server, see Install Updates for Panorama with an Internet Connection.

Before deploying updates, see Panorama, Log Collector, Firewall, and WildFire Version Compatibility for important details about content release version compatibility. Refer to the Release Notes for the minimum content release version you must install for a Panorama release.

Panorama can download only one update at a time for updates of the same type so if you schedule multiple updates of the same type to download during the same time interval, only the first download will succeed. To ensure that multiple updates of the same type succeed, stagger the updates.

If your firewalls connect directly to the Palo Alto Networks® Update Server, you can also use Panorama templates (Device > Dynamic Updates) to push content update schedules to the firewalls. If you want to delay the installation of updates for a period after they are released, you must deploy schedules using templates. In rare instances, a content update includes errors; specifying a delay increases the likelihood that Palo Alto Networks will identify and remove such an update from the Update Server before your firewalls install it.

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

**STEP 1** | Select Panorama > Device Deployment > Dynamic Updates, click Schedules, and Add a schedule.

**STEP 2** | Specify a Name (to identify the schedule), the update Type, and the update frequency (Recurrence). The frequency options depend on the update Type.

PAN-OS® uses the Panorama timezone for update scheduling.

If you set the Type to App and Threat, Log Collectors install and need only the Applications content, not the Threats content. Firewalls use both Applications and Threats content. For details, see Panorama, Log Collector, Firewall, and WildFire Version Compatibility.

The WildFire Private (WF-Private) type is available only if you set the WildFire Private Cloud field (Panorama > Setup > WildFire) to a WildFire appliance, not to the WildFire cloud.

**STEP 3** | Select one of the following schedule actions and then select the firewalls or Log Collectors:
• **Download And Install** *(Best Practice)*—Select Devices (firewalls), Log Collectors, or WildFire Appliances and Clusters.
• **Download Only**—Panorama downloads the update but does not install it.

**STEP 4** | Click **OK**.

**STEP 5** | Select **Commit > Commit to Panorama** and then **Commit** your changes.

### Upgrade Log Collectors When Panorama Is Internet-Connected

For a list of software and content updates you can install on Log Collectors, see Supported Updates.

**STEP 1** | Before you upgrade Log Collectors, ensure that you are running the appropriate Panorama™ software release on the Panorama management server.

_Palo Alto Networks® highly recommends that Panorama and Log Collectors run the same Panorama software release and that Panorama, Log Collectors, and all managed firewalls run the same content release version._

Panorama must be running the same (or later) software release as Log Collectors but must have the same or an earlier content release version:

- **Software release version**—If your Panorama management server is not already running the same or a later software release than the release to which you intend to update Log Collectors, then you must install the same or a later Panorama release on Panorama (see **Install Content and Software Updates for Panorama**) before you update any Log Collectors.
- **Content release version**—For content release versions, you should ensure that all Log Collectors are running the latest content release version or, at minimum, running a later version than is running on Panorama; if not, then first update managed firewalls (using Panorama) and then update Log Collectors before you update the content release version on the Panorama management server.

To check software and content versions:

- **Panorama management server**—To determine what software and content versions are running on the Panorama management server, log in to the Panorama web interface and go to General Information settings *(Dashboard)*.
- **Log Collectors**—To determine what software and content versions are running on Log Collectors, log in to the CLI of each Log Collector and run the _show system info_ command.

**STEP 2** | Install the latest content updates.

*Refer to the Release Notes for the minimum content release versions required for a Panorama software release.*

1. **Check Now** *(Panorama > Device Deployment > Dynamic Updates)* for the latest updates. If an update is available, the Action column displays a **Download** link.
2. If not already installed, **Download** the appropriate content updates. After a successful download, the link in the Action column changes from **Download** to **Install**.
3. Install the content update (Applications or Applications and Threats update before any others): Click **Install**, select the Log Collectors, and click **OK**.

_Regardless whether your subscription includes both Applications and Threats content, Panorama installs and needs only the Applications content. For details, see Panorama, Log Collector, Firewall, and WildFire Version Compatibility._
4. Repeat step c for any other updates (Antivirus, WildFire®, or URL Filtering) as needed, one at a time, and in any sequence.

**STEP 3** | Determine the software upgrade path to PAN-OS 8.0 for the Log Collectors that you intend to upgrade to Panorama 8.0. Refer to the New Features Guide for the upgrade path to a PAN-OS 8.0 release.

Check which Software Version is running on each Log Collector you intend to upgrade (Panorama > Managed Collectors) and take note of each release you need to download in your path to Panorama 8.0.

*If upgrading more than one Log Collector, streamline the process by determining the upgrade paths for all Log Collectors you intend to upgrade before you start downloading images.*

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

**STEP 4** | For all Log Collectors you intend to update, use the upgrade path(s) identified in Step 3 to upgrade Log Collectors to your target Panorama release.

1. On Panorama, Check Now (Panorama > Device Deployment > Software) for the latest updates. If an update is available, the Action column displays a Download link.

2. For each release in your upgrade path, Download the model-specific file for the release version to which you are upgrading. For example, to upgrade an M-Series appliance to Panorama 8.0.8, download the Panorama_m-8.0.8 image.

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

   *You can quickly locate Panorama images by selecting Panorama M Images (for M-Series appliances) from the Filter By drop-down.*

3. Click Install for the first (or next) version in your upgrade path and select the appropriate Log Collectors.

4. Select one of the following depending on the version you are installing within your upgrade path (Step 3):
   - Upload only to device (do not install).
   - Reboot device after install.

   *As a best practice, when upgrading to Panorama 8.0.3 or a later release), reboot the appliance after you install the Panorama 8.0.2 base image and before you download and install the maintenance release.*

5. Click OK to start the installation (or upload).

6. Repeat steps c through e until Log Collectors are running the desired release.

**STEP 5** | Verify the software and content update versions that are installed on the Log Collector.

Log in to the Log Collector CLI and enter the show system info operational command. The output will resemble the following:

```
sw-version: 8.0.0
app-version: 649-3758
app-release-date: 2016/12/21 15:46:03
av-version: 2581-3020
av-release-date: 2016/12/21 14:31:27
```
STEP 6 | Migrate Panorama Logs to the New Log Format.

When you upgrade to a Panorama 8.0 release, Panorama Log Collectors use a new log storage format. Because Panorama can no longer generate reports or ACC data from logs in the pre-8.0-release log format, you must migrate the existing logs as soon as you upgrade Panorama and its Log Collectors from a PAN-OS 7.1 or earlier release to a PAN-OS 8.0 or later release. Log migration is a one-time task; you do not need to migrate them again after you upgrade to PAN-OS 8.0.

Upgrade Log Collectors When Panorama Is Not Internet-Connected

For a list of software and content updates you can install on Log Collectors, see Supported Updates.

STEP 1 | Before you upgrade Log Collectors, ensure that you are running the appropriate Panorama™ software release on the Panorama management server.

Palo Alto Networks® highly recommends that Panorama and Log Collectors run the same Panorama software release and that Panorama, Log Collectors, and all managed firewalls run the same content release version. For important software and content compatibility details, see Panorama, Log Collector, Firewall, and WildFire Version Compatibility.

Panorama must be running the same (or later) software release as Log Collectors but must have the same or an earlier content release version:

- **Software release version**— If your Panorama management server is not already running the same or a later software release than the release to which you intend to update Log Collectors, then you must install the same or a later Panorama release on Panorama (see Install Content and Software Updates for Panorama) before you update any Log Collectors.

- **Content release version**— For content release versions, you should ensure that all Log Collectors are running the latest content release version or, at minimum, running a later version than you will install or that is running on Panorama; if not, then first update managed firewalls (using Panorama) and then update Log Collectors before you update the content release version on the Panorama management server (see Install Content and Software Updates for Panorama).

To check the software and content versions:

- **Panorama management server**— Log in to the Panorama web interface and go to General Information settings (Dashboard).

- **Log Collectors**— Log in to the CLI of each Log Collector and run the `show system info` command.

STEP 2 | Determine which content updates you need to install on Log Collectors. Refer to the Release Notes for the minimum content release version you must install for a Panorama release.

You must install content updates before software updates.

1. Run the `show system info` CLI command to view the current update versions.
2. For each content update, determine whether you need updates and take note of which content updates you need to download in Step 4.

Ensure that Panorama is running the same but not a later content release version than is running on managed firewalls and Log Collectors.

3. (As needed) Before you update content versions on Log Collectors, first upgrade managed firewalls to the same or later content release versions.
STEP 3 | Determine the software upgrade path for the Log Collectors that you intend to update to Panorama 8.0. Refer to the New Features Guide for the upgrade path to PAN-OS® 8.0.

Log in to Panorama, select (Panorama > Managed Collectors) and note the current Software Version for the Log Collectors you intend to upgrade.

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

STEP 4 | Download the content and software updates to a host that can connect and upload the files to Panorama either over SCP or HTTPS.

1. Use a host with internet access to log in to the Palo Alto Networks Customer Support web site.
2. Download content updates:
   1. Click Dynamic Updates in the Resources section.
   2. Download the desired content updates and save the files to the host. Perform this step for each content type you will update.
3. Download software updates:
   1. Return to the main page of the Palo Alto Networks Customer Support website and click Software Updates in the Resources section.
   2. Review the Download column to determine the version to install. The update package filenames for M-Series appliances begin with "Panorama_m" followed by the release number. For example, to upgrade an M-Series appliance to Panorama 8.0.8, download the Panorama_m-8.0.8 image.

   You can quickly locate Panorama images by selecting Panorama M Images (for M-Series appliances) from the Filter By drop-down.

   4. Click the appropriate filename and save the file to the host.

STEP 5 | Install content updates on Log Collectors.

If you need to install content updates, you must do so before you install software updates. Additionally, install content updates on firewalls first and then on Log Collectors before you update the content release version on Panorama.

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

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

1. In Panorama, select Panorama > Device Deployment > Dynamic Updates.
2. Click Upload, select the update Type, Browse to the appropriate content update file on the host, and click OK.
3. Click Install From File, select the update Type, and select the File Name of the update you just uploaded.
4. Select the Log Collectors.
5. Click OK to start the installation.
6. Repeat these steps for each content update.

STEP 6 | Install software updates.
1. Select **Panorama > Device Deployment > Software**.
2. Click **Upload, Browse** to the appropriate software update file on the host, and click **OK**.
3. Click **Install** in the Action column for the release you just uploaded.
4. Select the Log Collectors on which to install the update.
5. Select one of the following based on the software version you are installing within the upgrade path (Step 3):
   - Upload only to device (do not install).
   - Reboot device after install.
6. Click **OK** to start the installation.

**STEP 7 | Verify the software and content versions that are installed on each Log Collector.**

Log in to the Log Collector CLI and enter the `show system info` operational command. The output will resemble the following:

```
sw-version: 8.0.2
app-version: 649-3758
app-release-date: 2016/12/21 15:46:03
av-version: 2581-3020
av-release-date: 2016/12/21 14:31:27
```

**STEP 8 | Migrate Panorama Logs to the New Log Format.**

When you upgrade to a Panorama 8.0 or later release, Panorama Log Collectors use a new log storage format. Because Panorama can no longer generate reports or ACC data from logs in the pre-8.0-release log format, you must migrate the existing logs as soon as you upgrade Panorama and its Log Collectors from a PAN-OS 7.1 or earlier release to a PAN-OS 8.0 (or later) release. Log migration is a one-time task; you do not need to migrate them again after you upgrade to PAN-OS 8.0.

**Upgrade Firewalls When Panorama Is Internet-Connected**

Before deploying updates to firewalls, you must upgrade Panorama™ and then upgrade Log Collectors. For a list of software and content updates you can install on firewalls, see Supported Updates.

*You cannot deploy GlobalProtect™ data file updates on demand; you can only schedule the updates using the firewall web interface or a Panorama template.*

**Upgrade Firewalls When Panorama Is Not Internet-Connected**

For a list of software and content updates you can install on firewalls, see Supported Updates.

**STEP 1 | Before you upgrade managed firewalls, ensure that you are running the appropriate Panorama™ software release on the Panorama management server and Log Collectors.**

*Palo Alto Networks® highly recommends that Panorama and Log Collectors run the same Panorama software release and that Panorama, Log Collectors, and all managed firewalls run the same content release version.*

*For important software and content compatibility details, see Panorama, Log Collector, Firewall, and WildFire Version Compatibility.*

Panorama must be running the same (or later) software release as the firewalls but must have the same or an earlier content release version:
• **Software release version**—If your Panorama management server or Log Collectors are not already running the same or a later software release than the release to which you intend to update firewalls, then you must install the same or a later Panorama release on Panorama and then on Log Collectors (see **Install Content and Software Updates for Panorama**) before you update any firewalls.

• **Content release version**—For content release versions, you should ensure that all firewalls are running the latest content release version or, at minimum, are running a later version than is running on Panorama and Log Collectors; if not, then update managed firewalls and then **Upgrade Log Collectors When Panorama Is Not Internet-Connected** before you update the content release version on the Panorama management server (see **Install Content and Software Updates for Panorama**).

To check the software and content versions:

• **Panorama management server**—Log in to the Panorama web interface and go to General Information settings (**Dashboard**).

• **Log Collectors**—Log in to the CLI of each Log Collector and run the **show system info** command.

**STEP 2 |** Save a backup of the current configuration file on each managed firewall you plan to upgrade.

*Although the firewall automatically creates a configuration backup, it is a best practice to create and externally store a backup before you upgrade.*

1. **Export Panorama and devices config bundle (Panorama > Setup > Operations)** to generate and export the latest configuration backup of Panorama and of each managed appliance.

2. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the upgrade.

**STEP 3 |** Determine which content updates you need to install. Refer to **Release Notes** for the minimum content release version you must install for a PAN-OS® release.

*Palo Alto Networks highly recommends that Panorama, Log Collectors, and all managed firewalls run the same content release version.*

For each content update, determine whether you need updates and take note of which content updates you need to download in **Step 5**.

*Ensure that Panorama is running the same but not a later content release version than is running on managed firewalls and Log Collectors.*

**STEP 4 |** Determine the software upgrade path for the firewalls that you intend to update to PAN-OS 8.0. Refer to the **New Features Guide** for the upgrade path to PAN-OS 8.0.

Log in to Panorama, select **Panorama > Managed Devices**, and note the current Software Version for the firewalls you intend to upgrade.

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

**STEP 5 |** Download the content and software updates to a host that can connect and upload the files to Panorama either over SCP or HTTPS.

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

1. Use a host with internet access to log in to the Palo Alto Networks Customer Support web site.
2. Download content updates:
   1. Click Dynamic Updates in the Resources section.
   2. Download the latest content release version (or, at a minimum, the same or a later version than you will install or is running on the Panorama management server) and save the file to the host; repeat for each content type you need to update.
3. Download software updates:
   1. Return to the main page of the Palo Alto Networks Customer Support web site and click Software Updates in the Resources section.
   2. Review the Download column to determine the version(s) you need to install. The filename of the update packages indicates the model. For example, to upgrade a PA-200, PA-3050, and PA-5060 firewall to PAN-OS 8.0.8, download the `PanOS_200-8.0.8`, `PanOS_3000-8.0.8`, and `PanOS_5000-8.0.8` images.
      
      You can quickly locate specific PAN-OS images by selecting PAN-OS for the PA-<series/model> from the Filter By drop-down.
   3. Click the appropriate filename and save the file to the host.

**STEP 6 | Install content updates on managed firewalls.**

You must install content updates before software updates.

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

1. Select Panorama > Device Deployment > Dynamic Updates.
2. Click Upload, select the update Type, Browse to the appropriate content update file, and click OK.
3. Click Install From File, select the update Type, and select the File Name of the content update you just uploaded.
4. Select the firewalls on which to install the update.
5. Click OK to start the installation.
6. Repeat these steps for each content update.

**STEP 7 | (Firewalls serving as GlobalProtect™ portals only) Upload and activate a GlobalProtect agent/app software update on firewalls.**

You activate the update on firewalls so that users can download it to their endpoints (client systems).

1. Use a host with internet access to log in to the Palo Alto Networks Customer Support website.
2. Download the appropriate GlobalProtect agent/app software update.
4. Click Upload, Browse to the appropriate GlobalProtect agent/app software update on the host to which you downloaded the file, and click OK.
5. Click Activate From File and select the File Name of the GlobalProtect agent/app update you just uploaded.
You can activate only one version of agent/app software at a time. If you activate a new version but some agents require a previous version, you will have to reactivate the earlier version again for those agents to download the previous update.

6. Select the firewalls on which to activate the update.
7. Click OK to activate.

STEP 8 | Upload PAN-OS software updates.
1. Select Panorama > Device Deployment > Software.
2. Click Upload, Browse to the appropriate software update file on the host, and click OK.

STEP 9 | Install PAN-OS software updates.

To avoid downtime when updating the software on high availability (HA) firewalls, update one HA peer at a time.

For active/active firewalls, it doesn’t matter which peer you update first.

For active/passive firewalls, you must update the passive peer first, suspend the active peer (fail over), update the active peer, and then return the active peer to a functional state (fail back).

1. Perform the steps that apply to your firewall configuration to install the PAN-OS software update you just uploaded.

- **Non-HA firewalls**—Click Install in the Action column, select all the firewalls you are upgrading, select Reboot device after install, and click OK.
- **Active/active HA firewalls**:
  1. Confirm that the preemption setting is disabled on the first peer that you intend to upgrade (Device > High Availability > Election Settings). If enabled, then edit Election Settings and disable (clear) the Preemptive setting and Commit your change. You need only disable this setting on one firewall in each HA pair but ensure that the commit is successful before you proceed.
  2. Click Install, disable (clear) Group HA Peers, select either HA peer, select Reboot device after install, and click OK. Wait for the firewall to finish rebooting before you proceed.
  3. Click Install, disable (clear) Group HA Peers, select the HA peer that you didn’t update in the previous step, Reboot device after install, and click OK.
- **Active/passive HA firewalls**—In this example, the active firewall is named fw1 and the passive firewall is named fw2:
  1. Confirm that the preemption setting is disabled on the first peer that you intend to upgrade (Device > High Availability > Election Settings). If enabled, then edit Election Settings and disable (clear) the Preemptive setting and Commit your change. You need only disable this setting on one firewall in each HA pair but ensure that the commit is successful before you proceed.
  2. Click Install in the Action column for the appropriate update, disable (clear) Group HA Peers, select fw2, Reboot device after install, and click OK. Wait for fw2 to finish rebooting before you proceed.
  3. After fw2 finishes rebooting, verify on fw1 (Dashboard > High Availability) that fw2 is still the passive peer (the Local firewall state is active and the Peer—fw2—is passive).
  4. Access fw1 and Suspend local device (Device > High Availability > Operational Commands).
  5. Access fw2 (Dashboard > High Availability widget) and verify that the Local firewall state is active and the Peer is suspended.
6. Access Panorama, select Panorama > Device Deployment > Software, click Install in the Action column for the appropriate release, disable (clear) Group HA Peers, select fw1, Reboot device after install, and click OK. Wait for fw1 to finish rebooting before you proceed.

7. Access fw1 (Device > High Availability > Operational Commands) and click Make local device functional. Then wait two minutes before you proceed.

8. On fw1 (Dashboard > High Availability widget), verify that the Local firewall state is passive and the Peer (fw2) is active.

2. After you complete the above steps for a PAN-OS release update, repeat Step 8 and Step 9 to upload the next PAN-OS release in your upgrade path as needed until all firewalls are running the target PAN-OS 8.0 release.

STEP 10 | Verify the software and content versions that are installed on each managed firewall.

1. Select Panorama > Managed Devices.

2. Locate the firewall and review the values in the Software Version, Apps and Threat, Antivirus, URL Filtering, and GlobalProtect Client columns.

STEP 11 | If you disabled preemption on one of your HA firewalls before you upgraded, then edit the Election Settings (Device > High Availability) and re-enable the Preemptive setting for that firewall.
Monitor Network Activity

The Panorama™ management server provides a comprehensive, graphical view of network traffic. Using the visibility tools on Panorama—the Application Command Center (ACC), logs, and 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
- Ingest Traps ESM Logs on Panorama
- 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? • How has user activity changed over the current week as compared to last week or last month?</td>
</tr>
<tr>
<td>• What are the top URL categories being viewed in the last hour?</td>
<td></td>
</tr>
<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>
</tbody>
</table>
## ACC

<table>
<thead>
<tr>
<th>Monitor &gt; AppScope</th>
</tr>
</thead>
<tbody>
<tr>
<td>• What content or files are being blocked and are there specific users who trigger this File Blocking/Data Filtering rule?</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>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACC</th>
</tr>
</thead>
<tbody>
<tr>
<td>• What are the threats on the network, and how are these incoming and outgoing traffic threats distributed geographically?</td>
</tr>
</tbody>
</table>

You can then use the information to maintain or enforce changes to the traffic patterns on your network. See **Use Case: Monitor Applications Using Panorama** for a glimpse into how the visibility tools on Panorama can influence how you shape the acceptable use policies for your network.

Here are a few tips to help you navigate the ACC:

- **Switch from a Panorama view to a Device view**—Use the Context drop-down to access the web interface of any managed firewall. For details, see **Context Switch—Firewall or Panorama**.

- **Change Device Group and Data Source**—The default **Data Source** used to display the statistics on the charts in the ACC is **Panorama** local data, and the default **Device Group** setting is **All**. Using the local data on Panorama provides a quick load time for the charts. You can, however, change the data source to **Remote Device Data** if all the managed firewalls are on PAN-OS 7.0 or a later release. If the managed firewalls have a mix of PAN-OS 7.0 and earlier releases, you can only view Panorama data. When configured to use Remote Device Data, Panorama will poll all the managed firewalls and present an aggregated view of the data. The onscreen display indicates the total number of firewalls being polled and the number of firewalls that have responded to the query for information.

- **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 User-ID™ mapping information.

Based on the log forwarding configuration on the managed firewalls, the **Monitor > Logs** tab can include logs for traffic flows, threats, URL filtering, data filtering, host information profile (HIP) matches, and WildFire™ submissions. You can review the logs to verify a wealth of information on a given session or transaction. Some examples of this information are the user who initiated the session, the action (allow or deny) that the firewall performed on the session, and the source and destination ports, zones, and addresses. The System and Config logs can indicate a configuration change or an alarm that the firewall triggered when a configured threshold was exceeded.

**If Panorama will manage firewalls running software versions earlier than PAN-OS 7.0, specify a WildFire server from which Panorama can gather analysis information for WildFire samples that those firewalls submit. Panorama uses the information to complete WildFire Submissions logs that are missing field values introduced in PAN-OS 7.0. Firewalls running earlier releases won’t populate those fields. To specify the server, select Panorama > Setup > WildFire, edit the General Settings, and enter the WildFire Private Cloud name. The default is wildfire-public-cloud, which is the WildFire cloud hosted in the United States.**

### Generate, Schedule, and Email Reports

You can configure reports to run immediately or schedule them to run at specific intervals. You can save and export the reports or email them to specific recipients. Emailing is particularly useful if you want to share reports with administrators who do not have access to Panorama. Panorama supports the same report types as the Palo Alto Networks firewall.

**It is recommended that you install matching software releases on Panorama and the firewalls for which you will generate reports. For example, if the Panorama management server runs Panorama 8.0, install PAN-OS 8.0 on its managed firewalls before generating the reports. This practice avoids issues that might occur if you create reports that include fields supported in the Panorama release but not supported in an earlier PAN-OS release on the firewalls.**

**STEP 1 |** Configure Panorama to receive and store user and user group information that it receives from firewalls.

Required to generate reports based on usernames and groups instead of just IP addresses.

1. If you want Panorama to include user group information in reports, upgrade the managed firewalls to PAN-OS 8.0 or a later release. Panorama cannot synchronize group information from firewalls running earlier releases.
2. Select Panorama > Setup > Management, edit the Panorama Settings, and Enable reporting and filtering on groups.
3. Configure device groups if you haven't already. For each device group:
   - Select a Master Device, which is the firewall that provides user and user group information to Panorama.
   - Enable Panorama to Store users and groups from Master Device.

**STEP 2 | Generate reports.**

The steps to generate a report depend on the type.

- Custom report:
  1. Select Monitor > Manage Custom Reports and Add the report.
  2. Enter a Name to identify the report.
  3. Select a Database for the report.
     
     You can base the report on Summary Databases or Detailed Logs databases.
     
     To base the report on logs stored on the Panorama management server and Log Collectors, select Panorama Data (recommended for faster performance).
     
     To base the reports on logs stored on the managed firewalls, select Remote Device Data. This option is for cases where the firewalls might have logs that were not yet forwarded to Panorama. However, because Panorama must query the firewalls directly, this option is slower.
  4. Select Scheduled.
  5. Define your log filtering criteria by selecting the Time Frame, Sort By order, Group By preference, and the columns (log attributes) that the report will display.
  6. (Optional) Use the Query Builder to further refine the log filtering criteria based on log attributes.
  7. To test the report settings, select Run Now. If necessary, modify the settings to change the information that the report displays.
  8. Click OK to save the custom report.

- PDF Summary Report:
  1. Select Monitor > PDF Reports > Manage PDF Summary and add the report.
  2. Enter a Name to identify the report.
  3. 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.
  4. Click OK to save the settings.

**STEP 3 | Configure a Report Group.**

It can include predefined reports, PDF Summary reports, and custom reports. Panorama compiles all the included reports into a single PDF.

1. Select Monitor > PDF Reports > Report Groups and Add a report group.
2. Enter a Name to identify the report group.
3. (Optional) Select Title Page and add a Title for the PDF output.
5. Add the selected reports to the report group.
6. Click OK to save the settings.

**STEP 4 | Configure an Email server profile.**

The profile defines how the firewall connects to the server and sends email.

1. Select Panorama > Server Profiles > Email and Add a server profile.
2. Enter a Name to identify the profile.
3. Add up to four SMTP servers and Add the following information for each one:
   - Name—A name to identify the SMTP server (1 to 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 5 | Schedule the report for email delivery.**
1. Select Monitor > PDF Reports > Email Scheduler and Add an email scheduler profile.
2. Enter a Name to identify the profile.
3. Select the Report Group, the Email server profile you just created (Email Profile), and the Recurrence for the report (default is Disable).
4. Send test email to verify that the email settings are accurate.
5. Click OK to save your changes.
6. Select Commit > Commit to Panorama and Commit your changes.
Ingest Traps ESM Logs on Panorama

Visibility is a critical first step in preventing and reducing the impact of an attack. To help you meet this challenge, Panorama provides an integrated view of firewall logs (events on the network) and Traps™ ESM Server logs (security events on the endpoints) so that you can trace any suspicious or malicious activity.

For awareness and context on the events observed on the network and on your endpoints, forward security events that the Traps agents report to the ESM Server on to Panorama. Panorama can serve as a Syslog receiver that ingests these logs from the Traps ESM components using Syslog over TCP, UDP, or SSL. Then, Panorama can correlate discrete security events that occur on the endpoints with what’s happening on the network and generate match evidence. This evidence gives you more context on the chronology and flow of events to investigate issues and fix security gaps in your network.

**STEP 1** | Define the log ingestion profile on Panorama and attach it to a Collector Group.

1. Select Panorama > Log Ingestion Profile, and click Add.
2. Enter a Name for the profile.
3. Click Add and enter the details for the ESM Server. You can add up to four ESM Servers to a profile.
   1. Enter a Source Name.
   2. Specify the Port on which Panorama will be listening for syslog messages. The range is 23000 to 23999.
   3. Select the Transport layer protocol—TCP, UDP, or SSL.
   4. Select Traps_ESM for External Log type and 3.4.0 from the Version drop-down.
      As Traps log formats are updated, the updated log definitions will be available through content updates on Panorama.
4. Select Panorama > Collector Groups > Log Ingestion and Add the log ingestion profile so that the Collector Group can receive logs from the ESM Server(s) listed in the profile.

If you are enabling SSL for secure syslog communication between Panorama and the ESM Server(s), you must attach a certificate to the Managed Collectors that belong to the Collector Group (Panorama > Managed Collectors > General, and select the certificate to use for Inbound Certificate for Secure Syslog).

5. Commit changes to Panorama and the Collector Group.

**STEP 2** | Configure Panorama as a Syslog receiver on the ESM Server.

1. From the ESM Console, select Settings > ESM > Syslog, and Enable Syslog.
2. Enter Panorama hostname or IP address as the Syslog Server and the Syslog Port on which Panorama is listening.
3. Select the Transport layer protocol: TCP, TCP with SSL, or UDP. If you select TCP with SSL, the ESM Server requires a server certificate to enable client authentication.

   From Panorama, you must export the root CA certificate for the Inbound Certificate for Secure Syslog, and import the certificate in to the trusted root certificate store of the host on which you have installed the ESM Server.
4. In the Logging Events area, select one or more of the events. At a minimum, you must enable sending of security events for prevention, notification, and provisional incidents that the Traps agents report. For details on the other forwarding settings, refer to the Traps 3.4 Administrator's Guide.
STEP 3 | View ESM logs and correlated events.

1. Select Monitor > External Logs > Traps ESM to view the logs ingested in to Panorama.

![Figure 24: ESM Logs and Correlated Events](image)

2. Select Monitor > Automated Correlation Engine > Correlated Events, and filter on the Wildfire and Traps ESM Correlated C2 correlation object name to find correlated events. Panorama generates correlated events when a host on your network exhibits command and control activity that matches the behavior observed for a malicious file in the WildFire virtual environment. This correlated event alerts you to suspicious activity that a Traps agent and the firewall have observed from one or more infected hosts on your network.
Use Case: Monitor Applications Using Panorama

This example takes you through the process of assessing the efficiency of your current policies and determining where you need to adjust them to fortify the acceptable use policies for your network.

When you log in to Panorama, the Top Applications widget on the Dashboard gives a preview of the most used applications over the last hour. To display the widget, select Widgets > Application > Top Applications in the toolbar. You can either glance over the list of top applications and mouse over each application block for which you want to review the details, or you can select the ACC tab to view the same information as an ordered list. The following image is a view of the Top Applications widget on the Dashboard.

![Top Applications Widget](image)

**Figure 25: Top Applications Widget**

The data source for this display is the application statistics database; it does not use the Traffic logs and is generated whether or not you have enabled logging for security rules. This view into the traffic on your network depicts everything that is allowed on your network and is flowing through unblocked by any policy rules that you have defined.

In the ACC tab, you can select and toggle the Data Source to be local on Panorama or you can query the managed firewalls (Remote Device Data) for the data; Panorama automatically aggregates and displays the information. For a speedier flow, consider using Panorama as the data source (with log forwarding to Panorama enabled) because the time to load data from the managed firewalls varies by the time period for which you choose to view data and the volume of traffic that is generated on your network. If your managed firewalls have a combination of PAN-OS 7.0 and earlier versions, Remote Device Data is not available.

The Dashboard example in Figure 25: Top Applications Widget shows BitTorrent as a popular application. If you click the BitTorrent application block, Panorama opens the ACC > Network Activity tab with BitTorrent applied as a global filter and shows information on the application, users who accessed the application, and the details on the risk level and characteristics of the application.
In the User Activity widget, you can see how many users are using BitTorrent and the volume of traffic being generated. If you have enabled User-ID, you can view the names of the users who are generating this traffic, and drill in to review all the sessions, content or threats associated with each user.

In the Threat Activity tab, view the Compromised Hosts widget to see what correlation objects were matched on, and view the match evidence associated with the user and application. You can also view the threat name, category and ID in the Threat Activity widget.

With BitTorrent set as a global filter, use the Destination IP Activity and the Destination Regions widgets to verify where the traffic was destined. You can also view the ingress and egress zones and the security rule that is letting this connection through.

For more detailed information, jump into the Traffic logs for a filtered view and review each log entry for ports used, packets sent, bytes sent and received. Adjust the columns to view more information or less information based on your needs.

The Monitor > App-Scope > Traffic Map tab displays a geographical map of the traffic flow and provides a view of incoming versus outgoing traffic. You can also use the Monitor > App-Scope > Change Monitor tab to view changes in traffic patterns. For example, compare the top applications used over this hour to the last week or month to determine if there is a pattern or trend.

With all the information you have now uncovered, you can evaluate what changes to make to your policy configurations. Here are some suggestions to consider:

- Be restrictive and create a pre-rule on Panorama to block all BitTorrent traffic. Then use Panorama device groups to create and push this policy rule to one or more firewalls.
• Enforce bandwidth use limits and create a QoS profile and policy rule that de-prioritizes non-business traffic. Use Panorama device groups and templates to configure QoS and then push rules to one or more firewalls.
• Reduce risk to your network assets and create an application filter that blocks all file sharing applications that are peer-to-peer technology with a risk factor of 4 or 5. Make sure to verify that the BitTorrent application is included in that application filter, and will therefore be blocked.
• Schedule a custom report group that pulls together the activity for the specific user and that of top applications used on your network to observe that pattern for another week or two before taking action.

Besides checking for a specific application, you can also check for any unknown applications in the list of top applications. These are applications that did not match a defined App-ID™ signature and display as unknown-udp and unknown-tcp. To delve into these unknown applications, click on the name to drill down to the details for the unclassified traffic.

Use the same process to investigate the top source IP addresses of the hosts that initiated the unknown traffic along with the IP address of the destination host to which the session was established. For unknown traffic, the traffic logs, by default, perform a packet capture (pcap) when an unknown application is detected. The green arrow in the left column represents the packet capture snippet of the application data. Clicking on the green arrow displays the pcap in the browser.

Having the IP addresses of the servers (destination IP), the destination port, and the packet captures, you will be better positioned to identify the application and make a decision on how you would like to take action on your network. For example, you can create a custom application that identifies this traffic instead of labeling it as unknown TCP or UDP traffic. Refer to the article Identifying Unknown Applications for more information on identifying unknown application and Custom Application Signatures for information on developing custom signatures to discern the application.
Use Case: Respond to an Incident Using Panorama

Network threats can originate from different vectors, including malware and spyware infections due to drive-by downloads, phishing attacks, unpatched servers, and random or targeted denial of service (DoS) attacks, to name a few methods of attack. The ability to react to a network attack or infection requires processes and systems that alert the administrator to an attack and provide the necessary forensics evidence to track the source and methods used to launch the attack.

The advantage that Panorama provides is a centralized and consolidated view of the patterns and logs collected from the managed firewalls across your network. You can use the information from the automated correlation engine alone or in conjunction with the reports and logs generated from a Security Information Event Manager (SIEM), to investigate how an attack was triggered and how to prevent future attacks and loss of damage to your network.

The questions that this use case probes are:

- How are you notified of an incident?
- How do you corroborate that the incident is not a false positive?
- What is your immediate course of action?
- How do you use the available information to reconstruct the sequence of events that preceded or followed the triggering event?
- What are the changes you need to consider for securing your network?

This use case traces a specific incident and shows how the visibility tools on Panorama can help you respond to the report.

- Incident Notification
- Review the Widgets in the ACC
- Review Threat Logs
- Review WildFire Logs
- Review Data Filtering Logs
- Update Security Rules

Incident Notification

There are several ways that you could be alerted to an incident depending on how you’ve configured the Palo Alto Networks firewalls and which third-party tools are available for further analysis. You might receive an email notification that was triggered by a log entry recorded to Panorama or to your syslog server, or you might be informed through a specialized report generated on your SIEM solution, or a third-party paid service or agency might notify you. For this example, let’s say that you receive an email notification from Panorama. The email informs you of an event that was triggered by an alert for a Zero Access 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.

Review the Widgets in the ACC

In the ACC > Threat Activity tab, check the Compromised Hosts widget and Threat Activity widget for any critical or high severity threats. In the Compromised Hosts widget, look into the Matching Objects and click a Match Count value to view the match evidence for the associated incident.
Review Threat Logs

To begin investigating the alert, use the threat ID to search the Threat logs on Panorama (Monitor > Logs > Threat). From the Threat logs, you can find the IP address of the victim, export the packet capture (PCAP) by clicking the download icon in the log entry, and use a network analyzer tool such as WireShark to review the packet details. In the HTTP case, look for a malformed or bogus HTTP REFERER in the protocol, suspicious host, URL strings, the user agent, the IP address and port in order to validate the incident. Data from these pcaps is also useful in searching for similar data patterns and creating custom signatures or modifying security policy to better address the threat in the future.

As a result of this manual review, if you feel confident about the signature, consider transitioning the signature from an alert action to a block action for a more aggressive approach. In some cases, you may choose to add the attacker IP to an IP block list to prevent further traffic from that IP address from reaching the internal network.

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.

If you see this issue, enable the DNS sinkholing action in the Anti-Spyware profile in security rules to identify the infected hosts on your network. DNS sinkholing allows you to control outbound connections to malicious domains and redirect DNS queries to an internal IP address that is unused; the sinkhole that does not put out a response. When a compromised host initiates a connection to a malicious domain, instead of going out to the internet, the firewall redirects the request to the IP address you defined and it is sinkholed. Now, reviewing the traffic logs for all hosts that connected to the sinkhole allows you locate all compromised hosts and take remedial action to prevent the spread.

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 though the WildFire Submissions logs. The WildFire Submissions logs contain information on files uploaded to the WildFire service for analysis. Because spyware typically embeds itself covertly, reviewing the WildFire Submissions logs tells you whether the victim recently downloaded a suspicious file. The WildFire forensics report displays information on the URL from which the file or .exe was obtained, and the behavior of the content. It informs you if the file is malicious, if it modified registry keys, read/wrote into files, created new files, opened network communication channels, caused application crashes, spawned processes, downloaded files, or exhibited other malicious behavior. Use this information to determine whether to block the application that
caused the infection (web-browsing, SMTP, FTP), make more stringent URL Filtering rules, or restrict some applications/actions (for example, file downloads to specific user groups).

**Access to the WildFire logs from Panorama requires the following:** a WildFire subscription, a File Blocking profile that is attached to a Security rule, and Threat log forwarding to Panorama.

If Panorama will manage firewalls running software versions earlier than PAN-OS 7.0, specify a WildFire server from which Panorama can gather analysis information for WildFire samples that those firewalls submit. Panorama uses the information to complete WildFire Submissions logs that are missing field values introduced in PAN-OS 7.0. Firewalls running earlier releases won't populate those fields. To specify the server, select Panorama > Setup > WildFire, edit the General Settings, and enter the WildFire Private Cloud name. The default is wildfire-public-cloud, which is the WildFire cloud hosted in the United States.

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 firewall context and configure the firewall for Botnet reports that identify potential botnet-infected hosts on the network.
To provide redundancy in case of a system or network failure, you can deploy two Panorama™ management servers in a high availability (HA) configuration. Panorama supports an HA configuration in which one peer is the active-primary and the other is the passive-secondary. If a failure occurs on the primary peer, it automatically fails over and the secondary peer becomes active.

> 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**—The peers must be the same model and mode: both M-500 appliances in Panorama mode, M-100 appliances in Panorama mode, virtual appliances in Panorama mode, or virtual appliances in Legacy mode. (M-Series appliances in Log Collector mode do not support HA.)
- **The same Panorama OS version**—Must run the same Panorama version to synchronize configuration information and maintain parity for a seamless failover.
- **The same set of licenses**—Must have the same firewall management capacity license.
- (Panorama virtual appliance only) **Unique serial number**—Must have unique serial numbers; if the serial number is the same for both Panorama instances, they will be in suspended mode until you resolve the issue.

Figure 27: Panorama HA Organization

The Panorama servers in the HA configuration are peers and you can use either (active or passive) to centrally manage the firewalls, Log Collectors, and WildFire appliances and appliance clusters, with a few
exceptions (see Synchronization Between Panorama HA Peers). The HA peers use the management (MGT) interface to synchronize the configuration elements pushed to the managed firewalls, Log Collectors, and WildFire appliances and appliance clusters to maintain state information. Typically, Panorama HA peers are geographically located in different sites, so you need to make sure that the MGT interface IP address assigned to each peer is routable through your network. HA connectivity uses TCP port 28 with encryption enabled. If encryption is not enabled, ports 28769 and 28260 are used for HA connectivity and to synchronize configuration between the HA peers. We recommend less than 500ms latency between the peers. To determine the latency, use Ping during a period of normal traffic.
Priority and Failover on Panorama in HA

Each Panorama peer in the HA pair is assigned a priority value. The priority value of the primary or secondary peer determines which will be eligible for being the main point of administration and log management. The peer set as primary assumes the active state, and the secondary becomes passive. The active peer handles all the configuration changes and pushes them to the managed firewalls; the passive peer cannot make any configuration changes or push configuration to the managed firewalls. However, either peer can be used to run reports or to perform log queries.

The passive peer is synchronized and ready to transition to the active state if a path, link, system, or network failure occur on the active Panorama.

When a failover occurs, only the state (active or passive) of the Panorama peer changes; the priority (primary and secondary) does not. For example, when the primary peer fails, its status changes from active-primary to passive-primary.

A peer in the active-secondary state can perform all functions with two exceptions:

- It cannot manage firewall or Log Collector deployment functions such as license updates or software upgrades.
- It cannot log to an NFS until you manually change its priority to primary. Only the Panorama virtual appliance in Legacy mode supports NFS.

The following table lists the capabilities of Panorama based on its state and priority settings:

<table>
<thead>
<tr>
<th>Capability</th>
<th>active-primary</th>
<th>passive-primary</th>
<th>active-secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch device context</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Perform distributed reporting</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Manage shared policy</td>
<td>✔️</td>
<td>☑️</td>
<td>✔️</td>
</tr>
<tr>
<td>Log to local disk</td>
<td>✔️</td>
<td>☑️</td>
<td>✔️</td>
</tr>
<tr>
<td>Log to an NFS partition (Panorama virtual appliance only)</td>
<td>✔️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Deploy software and licenses</td>
<td>✔️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Export Panorama configuration</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

Figure 28: Panorama HA Capabilities

For more information, see Panorama HA Prerequisites or Set Up HA on Panorama.
Failover Triggers

When a failure occurs on the active Panorama and the passive Panorama takes over the task of managing the firewalls, the event is called a failover. A failover is triggered when a monitored metric on the active Panorama fails. This failure transitions the state on the primary Panorama from active-primary to passive-primary, and the secondary Panorama becomes active-secondary.

The conditions that trigger a failover are:

- The Panorama peers cannot communicate with each other and the active peer does not respond to health and status polls; the metric used is **HA Heartbeat Polling and Hello Messages**.
  
  When the Panorama peers cannot communicate with each other, the active one monitors whether the peers are still connected before a failover is triggered. This check helps in avoiding a failover and causing a split-brain scenario, where both Panorama peers are in an active state.

- One or more of the destinations (IP addresses) specified on the active peer cannot be reached; the metric used is **HA Path Monitoring**.

In addition to the failover triggers listed above, a failover also occurs when the administrator places the Panorama peer in a suspended state or when preemption occurs. Preemption is a preference for the primary Panorama to resume the active role after recovering from a failure (or user-initiated suspension). By default, preemption is enabled and when the primary Panorama recovers from a failure and becomes available, the secondary Panorama relinquishes control and returns to the passive state. When preemption occurs, the event is logged in the System log.

If you are logging to an NFS datastore, do not disable preemption because it allows the primary peer (that is mounted to the NFS) to resume the active role and write to the NFS datastore. For all other deployments, preemption is only required if you want to make sure that a specific Panorama is the preferred active peer.

HA Heartbeat Polling and Hello Messages

The HA peers use hello messages and heartbeats to verify that the peer is responsive and operational. Hello messages are sent from one peer to the other at the configured Hello Interval to verify the state of the other. The heartbeat is an ICMP ping to the HA peer, and the peer responds to the ping to establish that the peers are connected and responsive. By default, the interval is 1,000 milliseconds for the heartbeat and 8,000ms for hello messages.

HA Path Monitoring

Path monitoring checks the network connectivity and link state for an IP address or group of IP addresses (path group). The active peer uses ICMP pings to verify that one or more destination IP addresses can be reached. For example, you can monitor the availability of interconnected networking devices like a router or a switch, connectivity to a server, or some other vital device that is in the flow of traffic. Make sure that the node/device configured for monitoring is not likely to be unresponsive, especially when it comes under load, as this could cause a path monitoring failure and trigger a failover.

The default ping interval is 5,000ms. An IP address is considered unreachable when three consecutive pings (the default value) fail, and a peer failure is triggered when any or all of the IP addresses monitored become unreachable. By default, if any one of the IP addresses becomes unreachable, the HA state transitions to non-functional.
Logging Considerations in Panorama HA

Setting up Panorama in an HA configuration provides redundancy for log collection. Because the managed firewalls are connected to both Panorama peers over SSL, when a state change occurs, each Panorama sends a message to the managed firewalls. The firewalls are notified of the Panorama HA state and can forward logs accordingly.

By default, when the managed firewalls cannot connect to Panorama, they buffer the logs; when the connection is restored, they resume sending logs from where it was last left off.

The logging options on the hardware-based Panorama and on the Panorama virtual appliance differ:

- Logging Failover on a Panorama Virtual Appliance in Legacy Mode
- Logging Failover on an M-Series Appliance or Panorama Virtual Appliance in Panorama Mode

Logging Failover on a Panorama Virtual Appliance in Legacy Mode

The Panorama virtual appliance in Legacy mode provides the following log failover options:

<table>
<thead>
<tr>
<th>Log Storage Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual disk</td>
<td>By default, the managed firewalls send logs as independent streams to each Panorama HA peer. By default, if a peer becomes unavailable, the managed firewalls buffer the logs and when the peer reconnects it resumes sending logs from where it had left off (subject to disk storage capacity and duration of the disconnection). The maximum log storage capacity depends on the virtual platform (VMware ESXi or vCloud Air); see Panorama Models for details. You can choose whether to forward logs only to the active peer (see Modify Log Forwarding and Buffering Defaults). However, Panorama does not support log aggregation across the HA pair. Therefore, if you log to a virtual disk, for monitoring and reporting you must query the Panorama peer that collects the logs from the managed firewalls.</td>
</tr>
<tr>
<td>Network File System (NFS)</td>
<td>You can mount NFS storage only to a Panorama virtual appliance that runs on a VMware ESXi server. Only the active-primary Panorama mounts to the NFS-based log partition and can receive logs. On failover, the primary device goes into a passive-primary state. In this scenario, until preemption occurs, the active-secondary Panorama manages the firewalls, but it does not receive the logs and it cannot write to the NFS. To allow the active-secondary peer to log to the NFS, you must manually switch it to primary so that it can mount to the NFS partition. For instructions, see Switch Priority after Panorama Failover to Resume NFS Logging.</td>
</tr>
</tbody>
</table>
Logging Failover on an M-Series Appliance or Panorama Virtual Appliance in Panorama Mode

If you forward firewall logs to the local Log Collectors on an HA pair of M-500 appliances, M-100 appliances, or Panorama virtual appliances in Panorama mode, you specify which firewalls send logs to which Log Collectors when you Configure a Collector Group. You can configure a separate Collector Group for the Log Collector of each Panorama peer or configure a single Collector Group to contain the Log Collectors of both peers. In a Collector Group that contains both local Log Collectors, the log forwarding preference list determines which Log Collector receives logs from firewalls. For the PA-7000 Series and PA-5200 Series firewalls, you have the option to send logs to all the Log Collectors in the Collector Group, in which case Panorama uses round-robin load balancing to select which Log Collector receives the logs at any given moment.

In a Collector Group that contains both Log Collectors, you can also enable redundancy so that each log will have two copies and each copy will reside on a different Log Collector. This redundancy ensures that, if any one Log Collector becomes unavailable, no logs are lost: you can see all the logs forwarded to the Collector Group and run reports for all the log information. Log redundancy is available only if each Log Collector in the Collector Group has the same number of disks.

All the Log Collectors for any particular Collector Group must be the same model: all M-100 appliances: all M-500 appliances, or all Panorama virtual appliances in Panorama mode.

Because enabling redundancy creates more logs, this configuration requires more storage capacity. 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. (When a Collector Group runs out of space, it deletes older logs.)
Synchronization Between Panorama HA Peers

The Panorama HA peers synchronize the running configuration each time you commit changes on the active Panorama peer. The candidate configuration is synchronized between the peers each time you save the configuration on the active peer or just before a failover occurs.

Settings that are common across the pair, such as shared objects and policy rules, device group objects and rules, template configuration, certificates and SSL/TLS service profiles, and administrative access configuration, are synchronized between the Panorama HA peers.

The settings that are not synchronized are those that are unique to each peer, such as the following:

- Panorama HA configuration—Priority setting, peer IP address, path monitoring groups and IP addresses
- Panorama configuration—Management interface IP address, FQDN settings, login banner, NTP server, time zone, geographic location, DNS server, permitted IP addresses for accessing Panorama, SNMP system settings, and dynamic content update schedules
- Scheduled configuration exports
- NFS partition configuration and all disk quota allocation for logging. This applies only to a Panorama virtual appliance in Legacy mode that runs on a VMware ESXi server.
- Disk quota allocation for the different types of logs and databases on the Panorama local storage (SSD)

If you use a master key to encrypt the private keys and certificates on Panorama, you must use the same master key on both HA peers. If the master keys differ, Panorama cannot synchronize the HA peers.

For more information, see Panorama HA Prerequisites or Set Up HA on Panorama.
Manage a Panorama HA Pair

- Set Up HA on Panorama
- Set Up Authentication Using Custom Certificates Between HA Peers
- Test Panorama HA Failover
- Switch Priority after Panorama Failover to Resume NFS Logging
- Restore the Primary Panorama to the Active State

To install software or content updates, see Install Updates for Panorama in an HA Configuration.

Set Up HA on Panorama

Review the Panorama HA Prerequisites before performing the following steps:

STEP 1 | Set up connectivity between the MGT ports on the HA peers.

The Panorama peers communicate with each other using the MGT port. Make sure that the IP addresses you assign to the MGT port on the Panorama servers in the HA pair are routable and that the peers can communicate with each other across your network. To set up the MGT port, see Perform Initial Configuration of the Panorama Virtual Appliance or Perform Initial Configuration of the M-Series Appliance.

Pick a Panorama peer in the pair and complete the remaining tasks.

STEP 2 | Enable HA and (optionally) enable encryption for the HA connection.

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 Panorama.
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:
   1. Select Panorama > Certificate Management > Certificates.
   2. Select Export HA key. Save the HA key to a network location that the peer Panorama can access.
   3. On the peer Panorama, navigate to Panorama > Certificate Management > Certificates, select Import HA key, browse to the location where you saved the key, and import it.

STEP 3 | Set the HA priority.

1. In Panorama > High Availability, edit the Election Settings section.
2. Define the Device Priority as Primary or Secondary. Make sure to set one peer as primary and the other as secondary.

   If both peers have the same priority setting, the peer with the higher serial number will be placed in a suspended state.

3. Define the Preemptive behavior. By default preemption is enabled. The preemption selection—enabled or disabled—must be the same on both peers.
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 | Commit your configuration changes.
Select Commit > Commit to Panorama and Commit your changes.

STEP 7 | Configure the other Panorama peer.
Repeat Step 2 through Step 6 on the other peer in the HA pair.

STEP 8 | Synchronize the Panorama peers.
1. Access the Dashboard on the active Panorama and select Widgets > System > High Availability to display the HA widget.
2. Sync to peer, click Yes, and wait for the Running Config to display Synchronized.
3. Access the Dashboard on the passive Panorama and select Widgets > System > High Availability to display the HA widget.
4. Verify that the Running Config displays Synchronized.

Set Up Authentication Using Custom Certificates Between HA Peers

You can Set Up Authentication Using Custom Certificates for securing the HA connection between Panorama HA peers.

STEP 1 | Generate a certificate authority (CA) certificate on Panorama.
1. Select Panorama > Certificate Management > Certificates.
2. Create a self-signed root CA certificate or import a certificate from your enterprise CA.
STEP 2 | Configure a certificate profile that includes the root CA and intermediate CA.
2. Configure a certificate profile.

STEP 3 | Configure an SSL/TLS service profile.
2. Configure an SSL/TLS profile to define the certificate and protocol that Panorama and its manage devices use for SSL/TLS services.

STEP 4 | Configure Secure Server Communication on Panorama.
1. Select Panorama > Setup > Management and Edit the Panorama Settings.
2. Verify that the Custom Certificate Only check box is not selected. This allows you to continue managing all devices while migrating to custom certificates.
   
   When the Custom Certificate Only check box is selected, Panorama does not authenticate and cannot manage devices using predefined certificates.
3. Select the SSL/TLS service profile from the SSL/TLS Service Profile drop-down. This SSL/TLS service profile applies to all SSL connections between Panorama, firewalls, Log Collectors, and Panorama’s HA peers.
4. Select the certificate profile from the Certificate Profile drop-down.
5. (Optional) Configure an authorization list.
   
   1. Click Add under Authorization List.
   2. Select the Subject or Subject Alt Name as the Identifier type.
   3. Enter the Common Name
6. In Disconnect Wait Time (min), enter the number of minutes Panorama should before breaking and reestablishing the connection with its managed devices. This field is blank by default and the range is 0 to 44,640 minutes.
   
   The disconnect wait time does not begin counting down until you commit the new configuration.
   
1. Click OK.
2. Commit your changes.

STEP 5 | Upgrade the client-side Panorama to 8.0.
Upgrade Panorama.

STEP 6 | Configure Secure Client Communication.
1. Select Panorama > High Availability and Edit the HA settings.
3. Click OK.
4. Commit your changes.

Test Panorama HA Failover

To test that your HA configuration works properly, trigger a manual failover and verify that the peer transitions states successfully.

STEP 1 | Log in to the active Panorama peer.
You can verify the state of the Panorama server in the bottom right corner of the web interface.
STEP 2 | Suspend the active Panorama peer.

Select Panorama > High Availability, and then click the Suspend local Panorama link in the Operational Commands section.

STEP 3 | Verify that the passive Panorama peer has taken over as active.

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.

STEP 4 | Restore the suspended peer to a functional state. Wait for a couple minutes, and then verify that preemption has occurred, if preemptive is enabled.

On the Panorama you previously suspended:

1. Select Panorama > High Availability and, in the Operational Commands section, click Make local Panorama functional.
2. In the High Availability widget on the Dashboard, confirm that this (Local) Panorama has taken over as the active peer and that the other peer is now in a passive state.

Switch Priority after Panorama Failover to Resume NFS Logging

The Panorama virtual appliance in Legacy mode running on an ESXi server can use an NFS datastore for logging. In an HA configuration, only the primary Panorama peer is mounted to the NFS-based log partition and can write to the NFS. When a failover occurs and the passive Panorama becomes active, its state becomes active-secondary. Although a secondary Panorama peer can actively manage the firewalls, it cannot receive logs or write to the NFS because it does not own the NFS partition. When the firewalls cannot forward logs to the primary Panorama peer, each firewall writes the logs to its local disk. The firewalls maintain a pointer for the last set of log entries that they forwarded to Panorama so that when the passive-primary Panorama becomes available again, they can resume forwarding logs to it.

Use the instructions in this section to manually switch priority on the active-secondary Panorama peer so that it can begin logging to the NFS partition. The typical scenarios in which you might need to trigger this change are as follows:

- Preemption is disabled. By default, preemption is enabled on Panorama and the primary peer resumes as active when it becomes available again. When preemption is disabled, you need to switch the priority on the secondary peer to primary so that it can mount the NFS partition, receive logs from the managed firewalls, and write to the NFS partition.
- The active Panorama fails and cannot recover from the failure in the short term. If you do not switch the priority, when the maximum log storage capacity on the firewall is reached, the oldest logs will be overwritten to enable it to continue logging to its local disk. This situation can lead to loss of logs.

STEP 1 | Log in to the currently passive-primary Panorama, select Panorama > Setup > Operations and, in the Device Operations section, click Shutdown Panorama.

STEP 2 | Log in to the active-secondary Panorama, select Panorama > High Availability, edit the Election Settings, and set the Priority to Primary.

STEP 3 | Click OK to save your changes.

STEP 4 | Select Commit > Commit to Panorama and Commit your changes.

Do not reboot when prompted.
STEP 5 | Log in to the Panorama CLI and enter the following command to change the ownership of the
NFS partition to this peer: `request high-availability convert-to-primary`

STEP 6 | Select Panorama > Setup > Operations and, in the Device Operations section, click Reboot
Panorama.

STEP 7 | Power on the Panorama peer that you powered off in step 1. This peer will now be in a
passive-secondary state.

Restore the Primary Panorama to the Active State

By default, the preemptive capability on Panorama allows the primary Panorama to resume functioning as
the active peer as soon as it becomes available. However, if preemption is disabled, the only way to force
the primary Panorama to become active after recovering from a failure, a non-functional, or a suspended
state, is by suspending the secondary Panorama peer.

Before the active-secondary Panorama goes into a suspended state, it transfers the candidate configuration
to the passive Panorama so that all your uncommitted configuration changes are saved and can be accessed
on the other peer.

STEP 1 | Suspend Panorama.

1. Log in to the Panorama peer that you want to place in a suspended state.
2. Select Panorama > High Availability, and click the Suspend local Panorama link in the Operational
Commands section.

STEP 2 | Verify that the status indicates that the Panorama was suspended at user request.

On the Dashboard, High Availability widget, verify that the Local state is suspended.

A failover is triggered when you suspend a peer, and the other Panorama takes over as the active peer.

STEP 3 | Restore the suspended Panorama to a functional state.

1. In the Panorama > High Availability tab, Operational Commands section, click the Make local
Panorama functional link.
2. On the Dashboard, High Availability widget, confirm that the Panorama has transitioned to either the
active or passive state.
Administrator Panorama

This section describes how to administer and maintain the Panorama™ management server. It includes the following topics:

- Preview, Validate, or Commit Configuration Changes
- Manage Panorama and Firewall Configuration Backups
- Compare Changes in Panorama Configurations
- Manage Locks for Restricting Configuration Changes
- Add Custom Logos to Panorama
- Use the Panorama Task Manager
- Manage Storage Quotas and Expiration Periods for Logs and Reports
- Monitor Panorama
- Reboot or Shut Down Panorama
- Configure Panorama Password Profiles and Complexity

For instructions on completing initial setup, including defining network access settings, licensing, upgrading the Panorama software version, and setting up administrative access to Panorama, see Set Up Panorama.
Preview, Validate, or Commit Configuration Changes

You can perform Panorama Commit, Validation, and Preview Operations on pending changes to the Panorama configuration and then push those changes to the devices that Panorama manages, including firewalls, Log Collectors, and WildFire appliances and appliance clusters. You can filter the pending changes by administrator or location and then commit, push, validate, or preview only those changes. The locations can be specific device groups, templates, Collector Groups, Log Collectors, shared settings, or the Panorama management server.

Because Panorama pushes its running configuration, you cannot push changes to devices until you first commit them to Panorama. If the changes are not ready to activate on devices, you can select Commit > Commit to Panorama to commit the changes to the Panorama configuration without pushing them to devices. Later, when the changes are ready to activate on devices, you can select Commit > Push to Devices. If the changes are ready to activate on both Panorama and the devices, select Commit > Commit and Push as described in the following procedure.

**STEP 1 |** Configure the scope of configuration changes that you will commit, validate, or preview.

1. Click Commit at the top of the web interface.
2. Select one of the following options:
   - **Commit All Changes** (default)—Applies the commit to all changes for which you have administrative privileges. You cannot manually filter the commit scope when you select this option. Instead, the administrator role assigned to the account you used to log in determines the commit scope.
   - **Commit Changes Made By**—Enables you to filter the commit scope by administrator or location. The administrative role assigned to the account you used to log in determines which changes you can filter.

   To commit the changes of other administrators, the account you used to log in must be assigned the Superuser role or an Admin Role profile with the Commit For Other Admins privilege enabled.

3. (Optional) To filter the commit scope by administrator, select Commit Changes Made By, click the adjacent link, select the administrators, and click OK.
4. (Optional) To filter by location, select Commit Changes Made By and clear any changes that you want to exclude from the Commit Scope.

   If dependencies between the configuration changes you included and excluded cause a validation error, perform the commit with all the changes included. For example, when you commit changes to a device group, you must include the changes of all administrators who added, deleted, or repositioned rules for the same rulebase in that device group.

**STEP 2 |** Preview the changes that the commit will activate.

When you preview changes after you delete and then re-add the same device to a policy rule, Panorama displays that same device as both deleted in the running configuration and as added in the candidate configuration. Additionally, the order of devices in the device target list in the running configuration may then be different from the candidate configuration and display as a change when you preview changes even when there aren’t any configuration changes.
This can be useful if, for example, you don’t remember all your changes and you’re not sure you want to activate all of them.

Panorama compares the configurations you selected in the Commit Scope to the running configuration. The preview window displays the configurations side-by-side and uses color coding to indicate which changes are additions (green), modifications (yellow), or deletions (red).

**Preview Changes** and select the **Lines of Context**, which is the number of lines from the compared configuration files to display before and after the highlighted differences. These lines help you correlate the preview output to settings in the web interface. Close the preview window when you finish reviewing the changes.

Because the preview results display in a new window, your browser must allow pop-up windows. If the preview window does not open, refer to your browser documentation for the steps to unblock pop-up windows.

**STEP 3 | Preview the individual settings for which you are committing changes.**

This can be useful if you want to know details about the changes, such as the types of settings and who changed them.

1. Click **Change Summary**.
2. **(Optional)** Group By a column name (such as the Type of setting).
3. Close the Change Summary dialog when you finish reviewing the changes.

**STEP 4 | Validate the changes before committing to ensure the commit will succeed.**

1. **Validate Changes**.
   - The results display all the errors and warnings that an actual commit would display.
   - Resolve any errors that the validation results identify.

**STEP 5 | (Optional) Modify the Push Scope.**

By default, the Push Scope includes all locations with changes that require a Panorama commit.

If you select Commit > Push to Devices, the push scope includes all locations associated with devices that are out of sync with the Panorama running configuration.

1. **Edit Selections** and select:
   - **Device Groups**—Select device groups or individual firewalls or virtual systems.
   - **Templates**—Select templates, template stacks, or individual firewalls.
   - **Collector Groups**—Select Collector Groups.
2. Click **OK** to save your changes to the Push Scope.

**STEP 6 | Validate the changes you will push to device groups or templates.**

1. **Validate Device Group Push** or **Validate Template Push**.
   - The results display all the errors and warnings that an actual push operation would display.
   - Resolve any errors that the validation results identify.

**STEP 7 | Commit your changes to Panorama and push the changes to devices.**

**Commit and Push** the configuration changes.
Use the Panorama Task Manager to see details about commits that are pending (optionally, you can cancel these), in progress, completed, or failed.
Manage Panorama and Firewall Configuration Backups

The running configuration on Panorama comprises all the settings that you have committed and that are therefore active. The candidate configuration is a copy of the running configuration plus any inactive changes that you made since the last commit. Saving backup versions of the running or candidate configuration enables you to later restore those versions. For example, if a commit validation shows that the current candidate configuration has more errors than you want to fix, you can restore a previous candidate configuration. You can also revert to the current running configuration without saving a backup first.

See Panorama Commit, Validation, and Preview Operations for more information on committing configuration changes to Panorama and pushing the changes to managed devices.

After a commit on a local firewall that runs PAN-OS 5.0 or later, a backup is sent of its running configuration to Panorama. Any commits performed on the local firewall will trigger the backup, including commits that an administrator performs locally on the firewall or automatic commits that PAN-OS initiates (such as an FQDN refresh). By default, Panorama stores up to 100 backups for each firewall, though this is configurable. To store Panorama and firewall configuration backups on an external host, you can schedule exports from Panorama or export on demand. You can also import configurations from firewalls into Panorama device groups and templates to Transition a Firewall to Panorama Management.

- Schedule Export of Configuration Files
- Save and Export Panorama and Firewall Configurations
- Revert Panorama Configuration Changes
- Configure the Maximum Number of Configuration Backups on Panorama
- Load a Configuration Backup on a Managed Firewall

Schedule Export of Configuration Files

Panorama saves a backup of its running configuration as well as the running configurations of all managed firewalls. The backups are in XML format with file names that are based on serial numbers (of Panorama or the firewalls). Use these instructions to schedule daily exports of the backups to a remote host. Panorama exports the backups as a single gzip file. You require superuser privileges to schedule the export.

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.

To export backups on demand, see Save and Export Panorama and Firewall Configurations.

**STEP 1** | Select Panorama > Scheduled Config Export and click Add.

**STEP 2** | Enter a Name and Description for the scheduled file export and Enable it.

**STEP 3** | Using the 24-hour clock format, enter a daily Scheduled Export Start Time or select one from the drop-down.

**STEP 4** | Set the export Protocol to Secure Copy (SCP) or File Transfer Protocol (FTP).
STEP 5 | Enter the details for accessing the server, including: Hostname or IP address, Port, Path for uploading the file, Username, and Password.

If you are exporting to a BSD server, you will need to modify the SSHD password prompt to <username>@<hostname> <password>:

STEP 6 | (SCP only) Click Test SCP server connection. To enable the secure transfer of data, you must verify and accept the host key of the SCP server. Panorama doesn't establish the connection until you accept the host key. If Panorama has an HA configuration, perform this step on each HA peer so that each one accepts the host key of the SCP server. If Panorama can successfully connect to the SCP server, it creates and uploads the test file named ssh-export-test.txt.

STEP 7 | Click OK to save your changes.

STEP 8 | Select Commit > Commit to Panorama and Commit your changes.

Save and Export Panorama and Firewall Configurations

Saving a backup of the candidate configuration to persistent storage on Panorama enables you to later restore that backup (see Revert Panorama Configuration Changes). This is useful for preserving changes that would otherwise be lost if a system event or administrator action causes Panorama to reboot. After rebooting, Panorama automatically reverts to the current version of the running configuration, which Panorama stores in a file named running-config.xml. Saving backups is also useful if you want to revert to a Panorama configuration that is earlier than the current running configuration. Panorama does not automatically save the candidate configuration to persistent storage. You must manually save the candidate configuration as a default snapshot file (.snapshot.xml) or as a custom-named snapshot file. Panorama stores the snapshot file locally but you can export it to an external host.

You don't have to save a configuration backup to revert the changes made since the last commit or reboot; just select Config > Revert Changes (see Revert Panorama Configuration Changes).

Palo Alto Networks recommends that you back up any important configurations to an external host.

STEP 1 | Save changes to the candidate configuration.

- To overwrite the default snapshot file (.snapshot.xml) with all the changes that all administrators made, perform one of the following steps:
  - Select Panorama > Setup > Operations and Save candidate Panorama configuration.
  - Log in to Panorama with an administrative account that is assigned the Superuser role or an Admin Role profile with the Save For Other Admins privilege enabled. Then select Config > Save Changes at the top of the web interface, select Save All Changes and Save.
- To create a snapshot that includes all the changes that all administrators made but without overwriting the default snapshot file:
  1. Select Panorama > Setup > Operations and Save named Panorama configuration snapshot.
  2. Specify the Name of a new or existing configuration file.
  3. Click OK and Close.
- To save only specific changes to the candidate configuration without overwriting any part of the default snapshot file:
1. Log in to Panorama with an administrative account that has the role privileges required to save the desired changes.
2. Select Config > Save Changes at the top of the web interface.
3. Select Save Changes Made By.
4. To filter the Save Scope by administrator, click <administrator-name>, select the administrators, and click OK.
5. To filter the Save Scope by location, clear any locations that you want to exclude. The locations can be specific device groups, templates, Collector Groups, Log Collectors, shared settings, or the Panorama management server.
6. Click Save, specify the Name of a new or existing configuration file, and click OK.

**STEP 2 | Export a candidate or running configuration to a host external to Panorama or to a firewall.**

You can schedule daily exports to an SCP or FTP server (see Schedule Export of Configuration Files) or export configurations on demand. To export on demand, select Panorama > Setup > Operations and select one of the following options:

- **Export named Panorama configuration snapshot**—Export the current running configuration, a named candidate configuration snapshot, or a previously imported configuration (candidate or running). Panorama exports the configuration as an XML file with the Name you specify.
- **Export Panorama configuration version**—Select a Version of the running configuration to export as an XML file.
- **Export Panorama and devices config bundle**—Generate and export the latest version of the running configuration backup of Panorama and 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 export or push device config bundle to perform one of the following actions:
  - **Push & Commit** the configuration bundle to the firewall to remove 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.

*The full procedure to Transition a Firewall to Panorama Management requires additional steps.*

**Revert Panorama Configuration Changes**

Revert operations replace settings in the current candidate configuration with settings from another configuration. Reverting changes is useful when you want to undo changes to multiple settings as a single operation instead of manually reconfiguring each setting.

You can revert pending changes that were made to the Panorama configuration since the last commit. Panorama provides the option to filter the pending changes by administrator or location. The locations can be specific device groups, templates, Collector Groups, Log Collectors, shared settings, or the Panorama management server. If you saved a snapshot file for a candidate configuration that is earlier than the current running configuration (see Save and Export Panorama and Firewall Configurations), you can also revert to that snapshot. Reverting to a snapshot enables you to restore a candidate configuration that existed before the last commit. Panorama automatically saves a new version of the running configuration whenever you commit changes, and you can restore any of those versions.
• Revert to the current Panorama running configuration (file named running-config.xml).
  This operation undoes changes you made to the candidate configuration since the last commit.
  • To revert all the changes that all administrators made, perform one of the following steps:
    • Select Panorama > Setup > Operations, Revert to running Panorama configuration, and click Yes to confirm the operation.
    • Log in to Panorama with an administrative account that is assigned the Superuser role or an Admin Role profile with the Commit For Other Admins privilege enabled. Then select Config > Revert Changes at the top of the web interface, select Revert All Changes and Revert.
  • To revert only specific changes to the candidate configuration:
    1. Log in to Panorama with an administrative account that has the role privileges required to revert the desired changes.

      The privileges that control commit operations also control revert operations.

      2. Select Config > Revert Changes at the top of the web interface.
      3. Select Revert Changes Made By.
      4. To filter the Revert Scope by administrator, click `<administrator-name>`, select the administrators, and click OK.
      5. To filter the Revert Scope by location, clear any locations that you want to exclude.
      6. Revert the changes.

• Revert to the default snapshot (.snapshot.xml) of the Panorama candidate configuration.
  1. Select Panorama > Setup > Operations and Revert to last saved Panorama configuration.
  2. Click Yes to confirm the operation.
  3. (Optional) To overwrite the running configuration with the snapshot, select Commit > Commit to Panorama and Commit your changes.

• Revert to a previous version of the running configuration that is stored on Panorama.
  2. Select a configuration Version and click OK.
  3. (Optional) To overwrite the running configuration with the version you just restored, select Commit > Commit to Panorama and Commit your changes.

• Revert to one of the following:
  • Custom-named version of the Panorama running configuration that you previously imported
  • Custom-named Panorama candidate configuration snapshot (instead of the default snapshot)
  1. Select Panorama > Setup > Operations and Load named Panorama configuration snapshot.
  2. Select the snapshot Name and click OK.
  3. (Optional) To overwrite the running configuration with the snapshot, select Commit > Commit to Panorama and Commit your changes.

• Restore a Panorama running or candidate configuration that you previously exported to an external host.
  1. Select Panorama > Setup > Operations, Import named Panorama configuration snapshot, Browse to the configuration file on the external host, and click OK.
  2. Load named Panorama configuration snapshot, select the Name of the configuration file you just imported, and click OK.
3. (Optional) To overwrite the running configuration with the snapshot you just imported, select Commit > Commit to Panorama and Commit your changes.

Configure the Maximum Number of Configuration Backups on Panorama

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

**STEP 2** | Select Log Export and Reporting and enter the Number of Versions for Config Backups (default is 100; range is 1 to 1,048,576).

**STEP 3** | Click OK to save your changes.

**STEP 4** | Select Commit > Commit to Panorama and Commit your changes.

Load a Configuration Backup on a Managed Firewall

Use Panorama to load a configuration backup on a managed firewall. You can choose to revert to a previously saved or committed configuration on the firewall. Panorama pushes the selected version to the managed firewall, thereby overwriting the current candidate configuration on the firewall.

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

**STEP 2** | Select Manage in the Backups column.

**STEP 3** | Select from the Saved Configurations or Committed Configurations.

- Click a version number to view the contents of that version.
- Load a configuration version.

**STEP 4** | Select Commit > Commit to Panorama and Commit your changes.
Compare Changes in Panorama Configurations

To compare configuration changes on Panorama, you can select any two sets of configuration files: the candidate configuration, the running configuration, or any other configuration version that has been previously saved or committed on Panorama. The side-by-side comparison enables you to:

- Preview the configuration changes before committing them to Panorama. You can, for example, preview the changes between the candidate configuration and the running configuration. As a best practice, select the older version on the left pane and the newer version on the right pane, to easily compare and identify modifications.
- Perform a configuration audit to review and compare the changes between two sets of configuration files.
- Compare changes in Panorama configurations.
  1. Select Panorama > Config Audit.
  2. In each drop-down, select a configuration for the comparison.
  3. Select the number of lines that you want to include for Context and click Go.

  Panorama uses color shading to highlight items you added (green), modified (yellow), or deleted (red).

- Configure the number of versions Panorama stores for configuration audits.
  1. Select Panorama > Setup > Management and edit the Logging and Reporting Settings.
  2. Enter the Number of Versions for Config Audit (range is 1–1,048,576; default is 100).
  3. Click OK to save your changes.
  4. Select Commit > Commit to Panorama and Commit your changes.

- View and compare Panorama configuration files before committing.
  1. Select Commit > Commit to Panorama and Preview Changes.
  2. Select the number of Lines of Context you want to see, and click OK.
Manage Locks for Restricting Configuration Changes

Locking the candidate or running configuration prevents other administrators from changing the configuration until you manually remove the lock or Panorama removes it automatically (after a commit). Locks ensure that administrators don’t make conflicting changes to the same settings or interdependent settings during concurrent login sessions.

If you are changing settings that are unrelated to the settings other administrators are changing in concurrent sessions, you don’t need configuration locks to prevent commit conflicts. Panorama queues commit operations and performs them in the order that administrators initiate the commits. For details, see Panorama Commit, Validation, and Preview Operations.

A template or device group configuration push will fail if a firewall assigned to the template or device group has a commit or config lock that an administrator set locally on that firewall.

- View details about current locks.
  For example, you can check whether other administrators have set locks and read comments they entered to explain the locks.

  Click the locked padlock (🔒) at the top of the web interface. The adjacent number indicates the number of current locks.

- Lock a configuration.
  Read-only administrators who cannot modify firewall or Panorama configurations cannot set locks.
  1. Click the padlock icon at the top of the web interface.

     The icon varies based on whether existing locks are (🔒) or are not (🔓) set.

  2. Take a Lock and select the lock Type:

     • **Config**—Blocks other administrators from changing the candidate configuration.

        A custom role administrator who cannot commit changes can set a Config lock and save the changes to the candidate configuration. However, because that administrator cannot commit the changes, Panorama does not automatically release the lock after a commit; the administrator must manually remove the Config lock after making the required changes.

     • **Commit**—Blocks other administrators from changing the running configuration.

  3. Select the Location to determine the scope of the lock:

     • **Shared**—Restricts changes to the entire Panorama configuration, including all device groups and templates.

     • **Template**—Restricts changes to the firewalls included in the selected template. (You can’t take a lock for a template stack, only for individual templates within the stack.)

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

  4. (Optional) As a best practice, enter a **Comment** to describe your reason for setting the lock.

  5. Click **OK** and **Close**.
• Unlock a configuration.

Only a superuser or the administrator who locked the configuration can manually unlock it. However, Panorama automatically removes a lock after completing the commit operation that the administrator who set the lock initiated.

1. Click the locked padlock (🔒) at the top of the web interface.
2. Select the lock entry in the list.
3. Click Remove Lock, OK, and Close.

• Configure Panorama to automatically lock the running configuration when you change the candidate configuration. This setting applies to all Panorama administrators.

1. Select Panorama > Setup > Management and edit the General Settings.
2. Select Automatically Acquire Commit Lock and click OK.
3. Select Commit > Commit to Panorama and Commit your changes.
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.

**STEP 1** | Select **Panorama > Setup > Operations**.

**STEP 2** | In the Miscellaneous section, click **Custom Logos**.

**STEP 3** | 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.

**STEP 4** | Click **Open** to add the image. To preview the image, click the preview logo icon.

**STEP 5** | *(Optional)* To clear the green background header on the Panorama web interface, select the check box for **Remove Panorama background header**.

**STEP 6** | Click **Close** to save your changes.

**STEP 7** | Select **Commit > Commit to Panorama** and **Commit** your changes.
Use the Panorama Task Manager

Click **Tasks** (Tasks) at the bottom of the web interface to open the Task Manager, which displays details about all the operations that administrators initiated (for example, manual commits) or that Panorama or a managed firewall initiated (for example, scheduled report generation) since the last Panorama or firewall reboot. You can use the Task Manager to troubleshoot failed operations, investigate warnings associated with completed commits, or cancel pending commits.

**STEP 1** | Click **Tasks**.

**STEP 2** | **Show** the **Running** (in progress) tasks or **All** tasks (the default), optionally filter by type (**Reports**; **Log Requests**; or commit, download, and installation **Jobs**), and select **Panorama** (default) or the firewall for which you want to see the tasks.

**STEP 3** | Perform any of the following actions:

- **Display or hide task details**—By default, the Task Manager displays the Type, Status, Start Time, and Messages for each task. To see the End Time and Job ID for a task, you must manually display those columns. To display or hide a column, open the drop-down in any column header, select **Columns**, and select or clear the columns as desired.
- **Investigate warnings or failures**—Read the entries in the Messages column for task details. If the column says **Too many messages**, click the entry in the Type column to see more information.
- **Display a commit description**—If an administrator entered a description for a commit, click **Commit Description** in the Messages column to display it.
- **Check the position of a commit in the queue**—The Messages column indicates the queue position of commits that are in progress.
- **Cancel pending commits**—Clear **Commit Queue** to cancel all pending commits (available only to predefined administrative roles). To cancel an individual commit, click **x** in the Action column (the commit remains in the queue until Panorama dequeues it). You cannot cancel commits that are in progress.
Manage Storage Quotas and Expiration Periods for Logs and Reports

- Log and Report Storage
- Log and Report Expiration Periods
- Configure Storage Quotas and Expiration Periods for Logs and Reports
- Configure the Run Time for Panorama Reports

Log and Report Storage

You can edit the default storage quotas for each log type. When a log quota reaches the maximum size, Panorama starts overwriting the oldest log entries with the new log entries. The storage capacity for reports is not configurable. The Log storage locations and report storage capacities vary by Panorama model:

- **Panorama virtual appliance in Panorama mode**—The storage space for reports is 200MB. The appliance uses its virtual system disk to store the System and Config logs that Panorama and Log Collectors generate. The virtual system disk also stores the Application Statistics (App Stats) logs that Panorama automatically receives at 15-minute intervals from all managed firewalls. Panorama stores all other log types to its virtual logging disks (1 to 12).

- **Panorama virtual appliance in Legacy mode**—The storage space for reports is 200MB for Panorama 8.0 or earlier releases and 500MB for Panorama 8.0.1 and later releases. Panorama writes all logs to its assigned storage space, which can be any of one the following:
  - **Virtual system disk**—By default, approximately 11GB is allocated for log storage on the virtual system disk that you created when installing Panorama. If you add a virtual logging disk or NFS partition, Panorama still uses the system disk to store the System and Config logs that Panorama and Log Collectors generate and to store the App Stats logs collected from firewalls.
  - **Dedicated virtual logging disk**—Stores all log types except those that reside on the system disk.
  - **NFS partition**—This option is available only to Panorama running on a VMware ESXi server. The NFS partition stores all log types except those that reside on the system disk.

- **M-500 or M-100 appliance**—The storage space for reports is 500MB for Panorama 6.1 or later releases and 200MB for earlier releases. The M-Series appliances use their internal SSD to store the Config logs and System logs that Panorama and Log Collectors generate and to store the App Stats logs collected from firewalls. Panorama saves all other log types to its RAID-enabled disks. The RAID disks are either local to the M-Series appliance in Panorama mode or are in a Dedicated Log Collector (M-Series appliance in Log Collector mode). You edit the log storage quotas on the RAID disks when you Configure a Collector Group.

For details on the log storage options and capacities, see Panorama Models. You can Expand Log Storage Capacity on the Panorama Virtual Appliance by adding virtual logging disks or NFS storage. You can Increase Storage on the M-Series Appliance by adding RAID drives or by upgrading from 1TB drives to 2TB drives.

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 expired reports at the same it generates new reports (see Configure the Run Time for Panorama Reports).

• **Each log type**—Panorama evaluates logs as it receives them, and deletes logs that exceed the configured expiration period.

  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 in Legacy mode receives from firewalls.
- App Stats logs that Panorama receives from firewalls.
- System and Config logs that Panorama and Log Collectors generate locally.

The Panorama management server stores these logs locally.

  If you reduce a storage quota such that the current logs exceed it, after you commit the change, Panorama removes the oldest logs to fit the quota.

1. Select **Panorama > Setup > Management** and edit the Logging and Reporting Settings.
2. In the **Log Storage** settings, enter the storage **Quota (%)** for each log type.

   When you change a percentage value, the page refreshes to display the corresponding absolute value (Quota GB/MB column) based on the total allotted storage on Panorama.

3. Enter the **Max Days** (expiration period) for each log type (range is 1 to 2,000).

   By default, the fields are blank, which means the logs never expire.

   Restore Defaults if you want to reset the quotas and expiration periods to the factory defaults.

**STEP 2** | Configure the expiration period for reports that Panorama generates.

1. Select **Log Export and Reporting** and enter the **Report Expiration Period** in days (range is 1 to 2,000).

   By default, the field is blank, which means reports never expire.

2. Click **OK** to save your changes.

**STEP 3** | Configure the storage quotas and expiration periods for logs of all types (except App Stats logs) that an M-500 appliance, M-100 appliance, or Panorama virtual appliance in Panorama mode receives from firewalls.

The local or Dedicated Log Collectors store these logs.

  You configure these storage quotas at the Collector Group level, not for individual Log Collectors.

1. Select **Panorama > Collector Groups** and edit the Collector Group.
2. In the **General** settings, click the **Log Storage** value.
A value doesn’t display unless you assigned Log Collectors to the Collector Group. If the field displays 0MB after you assign Log Collectors, verify that you enabled the disk pairs when configuring the Log Collector and that you committed the changes (Panorama > Managed Collectors > Disks).

3. Enter the storage Quota(%) for each log type.

When you change a percentage value, the page refreshes to display the corresponding absolute value (Quota GB/MB column) based on the total storage allotted to the Collector Group.

4. Enter the Max Days (expiration period) for each log type (range is 1 to 2,000).

By default, the fields are blank, which means the logs never expire.

   Restore Defaults if you want to reset the quotas and expiration periods to the factory defaults.

5. Click OK to save your changes.

STEP 4 | Commit the changes to Panorama and push the changes to the Collector Group.

2. Select Collector Groups, select the Collector Group you modified, and click OK.
3. Commit and Push your changes.

STEP 5 | Verify that Panorama applied the storage quota changes.

1. Select Panorama > Setup > Management and, in the Logging and Reporting Settings, verify that the Log Storage values are correct for the logs that the Panorama management server stores.
2. Select Panorama > Collector Groups, select the Collector Group you modified, and verify that the Log Storage values in the General tab are correct for the logs that the Log Collectors store.

   You can also verify the Collector Group storage quotas by logging in to a Log Collector CLI and entering the operational command show log-diskquota-pct.

Configure the Run Time for Panorama Reports

   Panorama generates reports daily at the time you specify. Panorama deletes any expired reports after generating the new reports.

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

STEP 2 | Select Log Export and Reporting and set the Report Runtime to an hour in the 24-hour clock schedule (default is 02:00; range is 00:00 [midnight] to 23:00).

STEP 3 | Select Commit > Commit to Panorama and Commit your changes.
Monitor Panorama

To monitor Panorama and its managed collectors, you can periodically view their System and Config logs (filter logs by type), configure an 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 records every configuration change in 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 and Config logs or filter the logs based on attributes such as the receive time or severity level (System logs only). The following table summarizes the severity levels for System logs:

<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 configuration push.</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>

Panorama stores the System and Config logs locally; the exact location and storage capacity varies by Panorama model (see Log and Report Storage). Upon reaching the capacity limit, Panorama deletes the oldest logs to create space for new logs. If you need to store the logs for longer periods than what the local storage allows, you can Configure Log Forwarding from Panorama to External Destinations.

For information on using Panorama to monitor firewall logs, see Monitor Network Activity.

Monitor Panorama and Log Collector Statistics Using SNMP

You can configure an SNMP manager to request information from a Panorama management server and configure Panorama to respond. For example, the SNMP manager can request the high availability (HA) mode, Panorama state, and Panorama version. If the Panorama management server has a local Log
Collector, then Panorama can also provide logging statistics: average logs per second, storage duration, retention periods, log disk usage, log forwarding status from individual firewalls to Panorama and external servers, and the status of firewall-to-Log Collector connections. 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 to respond to requests for the same logging statistics as the Panorama management server. This information is useful when evaluating whether you need to expand log storage capacity.

You can’t configure an SNMP manager to control Panorama or Log Collectors (using SET messages); an SNMP manager can only collect statistics (using GET messages).

For details on how Panorama implements SNMP, see SNMP Support.

**STEP 1** | Configure the SNMP Manager to get statistics from Panorama and the Log Collectors.

The following steps are an overview of the tasks you perform on the SNMP manager. For the specific steps, refer to the documentation of your SNMP manager.

1. To enable the SNMP manager to interpret statistics, load the Supported MIBs and, if necessary, compile them.
2. For each Panorama appliance that the SNMP manager will monitor, define its connection settings (IP address and port) and authentication settings (SNMPv2c community string or SNMPv3 username and password). All Panorama appliances use port 161.

   The SNMP manager can use the same or different connection and authentication settings for multiple Panorama management servers and Log Collectors. The settings must match those you define when you configure SNMP on Panorama (see Step Configure the Panorama management server to respond to statistics requests from an SNMP manager. and Step Configure the Dedicated Log Collectors (if any) to respond to SNMP requests.). For example, if you use SNMPv2c, the community string you define when configuring Panorama must match the community string you define in the SNMP manager for Panorama.

3. 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.

4. Configure the SNMP manager to monitor the desired OIDs.

**STEP 2** | Enable SNMP traffic on the management (MGT) interface of the Panorama management server.

1. Select Panorama > Setup > Management and edit the Management Interface Settings.
2. In the Services section, select the SNMP check box and click OK.

**STEP 3** | Enable SNMP traffic on the management (MGT) interface of any M-Series appliances in Log Collector mode:

1. Select Panorama > Managed Collectors and select the Log Collector.
2. Select the Management tab, select the SNMP check box, and click OK.

**STEP 4** | Configure the Panorama management server to respond to statistics requests from an SNMP manager.

1. Select Panorama > Setup > Operations and, in the Miscellaneous section, click SNMP Setup.
2. Select the SNMP Version and configure the authentication values as follows. For version details, see SNMP Support.
• **V2c**—Enter the **SNMP Community String**, which identifies a community of SNMP managers and monitored devices (Panorama, in this case), and serves as a password to authenticate the community members to each other.

  *Don’t use the default community string **public**; it is well known and therefore not secure.*

• **V3**—Create at least one SNMP view group and one user. User accounts and views provide authentication, privacy, and access control when SNMP managers get statistics.

  **Views**—Each view is a paired OID and bitwise mask: the OID specifies a MIB, and the mask (in hexadecimal format) specifies which objects are accessible inside (include matching) or outside (exclude matching) that MIB. Click **Add** in the first list and enter a **Name** for the group of views. For each view in the group, click **Add** and configure the view **Name**, **OID**, matching **Option** (include or exclude), and **Mask**.

  **Users**—Click **Add** in the second list, enter a username in the Users column, select the **View** group from the drop-down, enter the authentication password (**Auth Password**) used to authenticate to the SNMP manager, and enter the privacy password (**Priv Password**) used to encrypt SNMP messages to the SNMP manager.

3. Click **OK** to save the settings.

**STEP 5 |** Configure the Dedicated Log Collectors (if any) to respond to SNMP requests.

For each Collector Group:

1. Select **Panorama > Collector Groups** and select the Collector Group.
2. Select the **Monitoring** tab, configure the same settings as in Step 4, and click **OK**.

**STEP 6 |** Commit the changes to Panorama and push the changes to Collector Groups.

1. Select **Commit > Commit and Push** and **Edit Selections** in the Push Scope.
2. Select **Collector Groups** you, select the Collector Groups you edited, and click **OK**.
3. **Commit and Push** your changes.

**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.

**STEP 1** | Select Panorama > Setup > Operations.

**STEP 2** | In the Device Operations section, select Reboot Panorama or Shutdown Panorama.
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.

**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.

**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:

   1. **Required Password Change Period**—Frequency, in days, at which the passwords must be changed.
   2. **Expiration Warning Period**—Number of days before expiration that the administrator will receive a password reminder.
   3. **Post Expiration Grace Period**—Number of days that the administrator can still log in to the system after the password expires.
   4. **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 issues for the Panorama™ management server and Dedicated Log Collectors:

- Troubleshoot Panorama System Issues
- Troubleshoot Log Storage and Connection Issues
- Replace an RMA Firewall
- Troubleshoot Commit Failures
- Troubleshoot Registration or Serial Number Errors
- Troubleshoot Reporting Errors
- View Task Success or Failure Status
Troubleshoot Panorama System Issues

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

Generate Diagnostic Files for Panorama

Diagnostic files aid in monitoring system activity and in discerning potential causes for issues on Panorama. To assist Palo Alto Networks Technical Support in troubleshooting an issue, the support representative might request a tech support file. The following procedure describes how to download a tech support file and upload it to your support case.

**STEP 1** | Select Panorama > Support and click Generate Tech Support File.

**STEP 2** | Download and save the file to your computer.

**STEP 3** | Upload the file to your case on the Palo Alto Networks Customer Support web site.

Diagnose Panorama Suspended State

If Panorama is in a suspended state, check for the following conditions:

- **Serial numbers**—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.
- **Mode**—If you deploy the Panorama virtual appliance in a high availability (HA) configuration, verify that both HA peers are in the same mode: Panorama mode or Legacy mode.
- **HA priority**—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.
- **Panorama software version**—Verify that both Panorama HA peers are running the same Panorama software 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

You can Install Content and Software Updates for Panorama and Deploy Updates to Firewalls, Log Collectors and WildFire Appliances Using Panorama. You cannot configure the amount of space available on Panorama to store updates. When the allotted storage capacity reaches 90%, Panorama alerts you to
free up space (delete stored updates) for new downloads or uploads. The maximum number of updates is a
global setting that applies to all the updates that Panorama stores. You must access the CLI to configure this
setting. The default value is two updates of each type.

- Modify the maximum number of updates of each type.

  Access the Panorama CLI and enter the following, where `<number>` can be between 2 and 64:

  ```
  > set max-num-images count <number>
  ```

- View the number of updates that Panorama currently stores.

  Enter:

  ```
  > show max-num-images
  ```

- Use the web interface to delete updates to free up space on Panorama.

  1. Select the type of update to delete:
     - Firewall or Log Collector updates:
       - PAN-OS/Panorama software images—Select Panorama > Device Deployment > Software.
       - GlobalProtect™ agent/app software updates—Select Panorama > Device Deployment > GlobalProtect Client.
       - Content updates—Select Panorama > Device Deployment > Dynamic Updates.
       - Panorama software images—Select Panorama > Software.
       - Panorama content updates—Select Panorama > Dynamic Updates.
     2. Click the X icon in the far right column for the image or update.

- Use the CLI to delete updates to free up space on Panorama.

  Delete software images by version:

  ```
  > delete software version <version_number>
  ```

  Delete content updates:

  ```
  > delete content update <filename>
  ```

**Recover from Split Brain in Panorama HA Deployments**

When Panorama is configured in a high availability (HA) setup, the managed firewalls are connected to
both the active and passive Panorama HA peers. When the connection between the active and the passive
Panorama peers fails, before the passive Panorama takes over as the active peer it checks whether any
firewall is connected to both the active and the passive peer. If even one firewall is connected to both
peers, the failover is not triggered.

In the rare event that a failover is triggered when a set of firewalls are connected to the active peer and a
set of firewalls are connected to the passive peer, but none of the firewalls are connected to both peers, it
is called a split brain. When a split brain occurs, the following conditions occur:

- Neither Panorama peer is aware of the state nor the HA role of the other peer.
• Both Panorama peers become active and manage a unique set of firewalls.

To resolve a split brain, debug your network issues and restore connectivity between the Panorama HA peers.

However, if you need to make configuration changes to your firewalls without restoring the connection between the peers, here are a couple of options:

• Manually add the same configuration changes on both Panorama peers. This ensures that when the link is reestablished the configuration is synchronized.

• If you need to add/change the configuration at only one Panorama location, make the changes and synchronize the configuration (make sure that you initiate the synchronization from the peer on which you made the changes) when the link between the Panorama peers is re-established. To synchronize the peers, select the Dashboard tab and click the Sync to peer link in the High Availability widget.

• If you need to add/change the configuration for only the connected firewalls at each location, you can make configuration changes independently on each Panorama peer. Because the peers are disconnected, there is no replication and each peer now has a completely different configuration file (they are out of sync). Therefore, to ensure that the configuration changes on each peer are not lost when the connection is restored, you cannot allow the configuration to be automatically re-synchronized. To solve this problem, export the configuration from each Panorama peer and manually merge the changes using an external diff and merge tool. After the changes are integrated, you can import the unified configuration file on the primary Panorama and then synchronize the imported configuration file with the peer.
Troubleshoot Log Storage and Connection Issues

- Verify Panorama Port Usage
- Resolve Zero Log Storage for a Collector Group
- Replace a Failed Disk on an M-Series Appliance
- Replace the Virtual Disk on an ESXi Server
- Replace the Virtual Disk on vCloud Air
- Migrate Logs to a New M-Series Appliance in Log Collector Mode
- Migrate Logs to a New M-Series Appliance in Panorama Mode
- Migrate Logs to a New M-Series Appliance Model in Panorama Mode in High Availability
- Migrate Logs to the Same M-Series Appliance Model in Panorama Mode in High Availability
- Migrate Log Collectors after Failure/RMA of Non-HA Panorama
- Regenerate Metadata for M-Series Appliance RAID Pairs

Verify Panorama Port Usage

To ensure that Panorama can communicate with managed firewalls, Log Collectors, and WildFire appliances and appliance clusters, and its high availability (HA) peer, use the following table to verify the ports that you must open on your network. Panorama uses TCP protocol for port communications.

By default, Panorama uses the management (MGT) interface to manage devices (firewalls, Log Collectors, and WildFire appliances and appliance clusters), collect logs, communicate with Collector Groups, and deploy software and content updates to devices. However, you can optionally assign the log collection and Collector Group communication functions to the Eth1 or Eth2 interfaces on an M-500 or M-100 appliance running Panorama 6.1 through 7.1. If the appliance runs Panorama 8.0 or a later release, you can assign any function to the Eth1, Eth2, or Eth3 interfaces on the M-100 appliance and to the Eth1, Eth2, Eth3, Eth4, or Eth5 interfaces on the M-500 appliance. 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 Systems &amp; Direction of Connection Establishment</th>
<th>Ports Used in Panorama 5.x</th>
<th>Ports Used in Panorama 6.x to 7.x</th>
<th>Ports Used in Panorama 8.x and later</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panorama and Panorama (HA) Direction: Each peer initiates its own connection to the other</td>
<td>28</td>
<td>28</td>
<td>28</td>
<td>For HA connectivity and synchronization if encryption is enabled.</td>
</tr>
<tr>
<td>Panorama and Panorama (HA) Direction: Each peer initiates its own connection to the other</td>
<td>28769 and 28260 (5.1)</td>
<td>28260 and 28769</td>
<td>28260 and 28769</td>
<td>For HA connectivity and synchronization if encryption is not enabled.</td>
</tr>
<tr>
<td>Panorama and Panorama (HA) Direction: Each peer initiates its own connection to the other</td>
<td>28769 and 28260 (5.1)</td>
<td>28260 and 28769</td>
<td>28260 and 28769</td>
<td>For HA connectivity and synchronization if encryption is not enabled.</td>
</tr>
<tr>
<td>Communicating Systems &amp; Direction of Connection Establishment</td>
<td>Ports Used in Panorama 5.x</td>
<td>Ports Used in Panorama 6.x to 7.x</td>
<td>Ports Used in Panorama 8.x and later</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>----------------------------------</td>
<td>-------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Panorama and managed firewalls</td>
<td>3978</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>
<td></td>
</tr>
<tr>
<td>Panorama and Log Collector</td>
<td>3978</td>
<td>3978</td>
<td>3978</td>
<td>For management and log collection/reporting. Used for communication between the local Log Collector on a Panorama in Panorama mode, and for communicating with Log Collectors in a distributed log collection deployment.</td>
</tr>
<tr>
<td>Direction: Initiated by the Log Collector</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Panorama and managed devices (firewalls, Log Collectors, and WildFire appliances and appliance clusters)</td>
<td>3978</td>
<td>3978</td>
<td>28443</td>
<td>Devices running PAN-OS 8.x or later releases use port 28443 to retrieve software and content update files from Panorama. Devices running 7.x or earlier releases do not retrieve update files from Panorama; Panorama pushes the update files to the devices over port 3978. Support for Panorama management of WildFire appliances and appliance clusters requires PAN-OS 8.0.1 or later installed on the managed WildFire appliances. We recommend that Panorama runs 8.0.1 or later to manage WildFire appliances and appliance clusters.</td>
</tr>
<tr>
<td>Direction:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Initiated by managed devices running PAN-OS 8.x or later releases.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Initiated by Panorama for devices running PAN-OS 7.x or earlier releases.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log Collector to Log Collector</td>
<td>49190</td>
<td>28270</td>
<td>28270</td>
<td>For distributing blocks and all binary data between Log Collectors.</td>
</tr>
<tr>
<td>Direction: Each Log Collector initiates a connection to the</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communicating Systems &amp; Direction of Connection Establishment</td>
<td>Ports Used in Panorama 5.x</td>
<td>Ports Used in Panorama 6.x to 7.x</td>
<td>Ports Used in Panorama 8.x and later</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>---------------------------</td>
<td>---------------------------------</td>
<td>-----------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>other Log Collectors in the Collector Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Panorama to Logging Service</td>
<td>NA</td>
<td>NA</td>
<td>444</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Version 8.0.5 and later</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For setting up a secure communication channel with the Logging Service.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The managed firewalls use port 3978 to communicate with the Logging Service.</td>
<td></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 in the Log Collectors. To enable the disk pairs, perform the following steps for each Log Collector in the Collector Group.

**STEP 1** | Add the RAID disk pairs.
1. Select **Panorama > Managed Collectors** and click the Collector Name.
2. Select **Disks, Add** each RAID disk pair, and click **OK**.

**STEP 2** | Commit the changes to Panorama and push the changes to the Collector Group.
1. Select **Commit > Commit and Push** and **Edit Selections** in the Push Scope.
2. Select **Collector Groups**, select the Collector Group you modified, and click **OK**.
3. **Commit and Push** your changes.

**STEP 3** | Verify the state of the Log Collectors and disk pairs.
1. Select **Panorama > Managed Collectors** and verify that the configuration of each Log Collector is synchronized with Panorama.
   
   The Configuration Status column should display **In Sync** and the Run Time Status column should display **connected**.
2. Click **Statistics** in the last column for each Log Collector and verify that the disk pairs are **Enabled** and **Available**.

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

If a disk fails on the M-Series appliance, you must replace the disk and reconfigure it in a RAID 1 array. For details, refer to the **M-100 or M-500 appliance Hardware Reference Guide**.

**Replace the Virtual Disk on an ESXi Server**

You cannot resize a virtual disk after adding it to the Panorama virtual appliance running on a VMware ESXi server. Because the Panorama virtual appliance in Legacy mode allows only one log storage location, you must replace the virtual disk as follows to modify the log storage capacity. In Panorama mode, you can simply add another disk (up to the maximum of 12) to **Expand Log Storage Capacity on the Panorama Virtual Appliance**.
On the Panorama virtual appliance in Legacy mode, you will lose the logs on the existing disk when you replace it. For the options to preserve existing logs, see Preserve Existing Logs When Adding Storage on Panorama Virtual Appliance in Legacy Mode.

STEP 1 | Remove the old virtual disk.
1. Access the VMware vSphere Client and select the Virtual Machines tab.
2. Right-click the Panorama virtual appliance and select Power > Power Off.
3. Right-click the Panorama virtual appliance and select Edit Settings.
4. Select the virtual disk in the Hardware tab and click Remove.
5. Select one of the Removal Options and click OK.

STEP 2 | Add the new virtual disk.
1. Add a Virtual Disk to Panorama on an ESXi Server.
   Panorama running on ESXi 5.5 and later versions supports a virtual disk of up to 8TB. Panorama running on an earlier ESXi version supports a virtual disk of up to 2TB.
2. In the vSphere Client, right-click the Panorama virtual appliance and select Power > Power On.
   The reboot process might take several minutes and the message cache data unavailable will display.

STEP 3 | Verify that the modified log storage capacity is correct.
1. Log in to the Panorama virtual appliance.
2. Select Panorama > Setup > Management and verify that the Logging and Reporting Settings section, Log Storage field, displays the modified log storage capacity accurately.

Replace the Virtual Disk on vCloud Air

You cannot resize a virtual disk after adding it to the Panorama virtual appliance running on VMware vCloud Air. Because the Panorama virtual appliance in Legacy mode allows only one log storage location, you must replace the virtual disk as follows to modify the log storage capacity. In Panorama mode, you can simply Add a Virtual Disk to Panorama on vCloud Air (up to the maximum of 12).

On the Panorama virtual appliance in Legacy mode, you will lose the logs on the existing disk when you replace it. For the options to preserve existing logs, see Preserve Existing Logs When Adding Storage on Panorama Virtual Appliance in Legacy Mode.

STEP 1 | Remove the old virtual disk.
1. Access the vCloud Air web console and select your Virtual Private Cloud OnDemand region.
2. Select the Panorama virtual appliance in the Virtual Machines tab.
3. Select Actions > Edit Resources.
4. Click x for the virtual disk you are removing.

STEP 2 | Add the new virtual disk.
1. Add another disk.
2. Set the Storage to up to 8TB and set the storage tier to Standard or SSD-Accelerated.
3. Save your changes.

STEP 3 | Reboot Panorama.
1. Log in to the Panorama virtual appliance.
2. Select Panorama > Setup > Operations and Reboot Panorama.
STEP 4 | Verify that the modified log storage capacity is correct.

1. Log in to the Panorama virtual appliance after it reboots.
2. Select Panorama > Setup > Management and verify that the Logging and Reporting Settings section, Log Storage field, displays the modified log storage capacity accurately.

Migrate Logs to a New M-Series Appliance in Log Collector Mode

If you need to replace an M-500 or M-100 appliance in Log Collector mode (Dedicated Log Collector), you can migrate the logs it collected from firewalls by moving its RAID disks to a new M-Series appliance. This procedure enables you to recover logs after a system failure on the M-Series appliance or to migrate logs as part of a hardware upgrade (from an M-100 appliance to an M-500 appliance).

STEP 1 | Perform initial setup of the new M-Series appliance that will be a Dedicated Log Collector.

1. Rack mount the M-Series appliance. Refer to the M-100 or M-500 Appliance Hardware Reference Guide for instructions.
2. Perform Initial Configuration of the M-Series Appliance.

   When configuring interfaces, configure only the Management (MGT) interface.

   Switching to Log Collector mode (later in this procedure) removes the configurations for any other interfaces. If the Log Collector will use interfaces other than MGT, add them when configuring the Log Collector (see Step 2).

3. Register Panorama.
4. Purchase and activate the Panorama support license or transfer licenses as follows only if the new M-Series appliance is the same hardware model as the old M-Series appliance. If the new M-Series appliance is a different model than the old M-Series appliance, you must purchase new licenses.
   1. Log in to the Palo Alto Networks Customer Support web site.
   2. Select the Assets tab and click the Spares link.
   3. Click the Serial Number of the new M-Series appliance.
   4. Click Transfer Licenses.
   5. Select the old M-Series appliance and click Submit.
5. Activate a firewall management license. If you are migrating from an M-100 appliance to an M-500 appliance, enter the auth-code associated with the migration license.
6. Install Content and Software Updates for Panorama. For important details about software versions, see Panorama, Log Collector, Firewall, and WildFire Version Compatibility.
7. Switch from Panorama mode to Log Collector mode:
   1. Access the Log Collector CLI and switch to Log Collector mode:

      > request system system-mode logger

   2. Enter y to confirm the mode change. The M-Series appliance reboots. If the reboot process terminates your terminal emulation software session, reconnect to the M-Series appliance to display the Panorama login prompt.

      If you see a CMS Login prompt, press Enter without typing a username or password.

   8. Use the Log Collector CLI to enable connectivity between the Log Collector and Panorama management server. <IPaddress1> is for the MGT interface of the primary Panorama and <IPaddress2> is for the MGT interface of the secondary Panorama.

      > configure
STEP 2 | On the Panorama management server, add the new Log Collector as a managed collector.

For all steps with commands that require a serial number, you must type the entire serial number; pressing the Tab key won't complete a partial serial number.

1. Configure the Log Collector as a managed collector using the Panorama web interface or using the following CLI commands:

```bash
> configure
# set log-collector <LC_serial_number> deviceconfig system hostname <LC_hostname>
# exit
```

If the old Log Collector used interfaces other than the MGT interface for log collection and Collector Group communication, you must define those interfaces on the new Log Collector when you configure it as a managed collector (Panorama > Managed Collectors > Interfaces).

2. Verify that the Log Collector is connected to Panorama and that the status of its disk pairs is present/available.

```bash
> show log-collector serial-number <log-collector_SN>
```

The disk pairs will display as disabled at this stage of the restoration process.

3. Commit your changes to Panorama. Don't commit the changes to the Collector Group just yet.

```bash
> configure
# commit
# exit
```

STEP 3 | Remove the RAID disks from the old Log Collector.

1. Power off the old Log Collector by pressing the Power button until the system shuts down.
2. Remove the disk pairs. For details, refer to the disk replacement procedure in the M-100 or M-500 Appliance Hardware Reference Guide.

STEP 4 | 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. To expedite the process, you can launch multiple CLI sessions and run the metadata regeneration command in each session to complete the process simultaneously for every pair. For details, see Regenerate Metadata for M-Series Appliance RAID Pairs.

1. Insert the disks into the new Log Collector. For details, refer to the disk replacement procedure in the M-100 or M-500 Appliance Hardware Reference Guide.

The disk carriers of the M-100 appliance are incompatible with those of the M-500 appliance. Therefore, when migrating between these hardware models, you must...
unscrew each disk from its old carrier and insert the disk in the new carrier before inserting the disk in the new appliance.

You must maintain the disk pair association. Although you can place a disk pair from slot A1/A2 on the old appliance into slot B1/B2 on the new appliance, you must keep the disks together in the same slot; otherwise, Panorama might not restore the data successfully.

2. Enable the disk pairs by running the following CLI command for each pair:

   > request system raid add <slot> force no-format

   For example:

   > request system raid add A1 force no-format
   > request system raid add A2 force no-format

   The **force** and **no-format** arguments are required. The **force** argument associates the disk pair with the new Log Collector. The **no-format** argument prevents reformatting of the drives and retains the logs stored on the disks.

3. Generate the metadata for each disk pair.

   > request metadata-regenerate slot <slot_number>

   For example:

   > request metadata-regenerate slot 1

### STEP 5 | Add a Log Collector with no disks to a Collector Group.

*From this point, only commits that are required to complete the migration process on Panorama and the Log Collectors. Hold off making any other changes.*

1. Access the Panorama CLI.
2. Overwrite Panorama restriction to allow Log Collector with no disk to be added to a Collector Group:

   request log-migration-set-start

### STEP 6 | Migrate the logs.

*You must use the Panorama CLI for this step, not the web interface.*

You must assign the new Log Collector to the Collector Group that contains the old Log Collector.

1. Assign the new Log Collector to the Collector Group and commit your changes to Panorama.

   > configure
   # set log-collector-group <collector_group_name> logfwd-setting collectors <new_LC_serial_number>
   # commit
   # exit

2. For each disk pair, migrate the logs from the old Log Collector to the new Log Collector and attach the disk pair to the new Log Collector.
STEP 7 | Reconfigure the Collector Group.

1. Use the web interface to assign the new Log Collector to the firewalls that forward logs (Panorama > Collector Groups > Device Log Forwarding). Give the new Log Collector the same priority in the firewall preference lists as the old Log Collector.

   You cannot use the CLI to change the priority assignments of firewall preference lists.

2. Delete the old Log Collector from the Collector Group.

   ```
   > configure
   # delete log-collector-group <group_name> logfwd-setting collectors <old_LC_serial_number>
   ```

   For example:

   ```
   # delete log-collector-group DC-Collector-Group logfwd-setting collectors 003001000010
   ```

3. Delete the old Log Collector from the Panorama configuration and commit your changes to Panorama.

   ```
   # delete log-collector <old_LC_serial_number>
   # commit
   # exit
   ```

4. Commit the Collector Group changes so that the managed firewalls can send logs to the new Log Collector.

   ```
   > commit-all log-collector-config log-collector-group <collector_group_name>
   ```

   For example:

   ```
   > commit-all log-collector-config log-collector-group DC-Collector-Group
   ```

STEP 8 | Generate new keys on the new Dedicated Log Collector.

This command is required in order to add the new Log Collector to the Collector Group and should only be run for the Collector Group of the Log Collector being replaced. This step deletes the existing RSA keys and allows Panorama to create new RSA keys.

1. Access the Panorama CLI.
2. Delete all RSA keys on new Log Collector:

```
request logdb update-collector-group-after-replace collector-group <collector-group-name>
```

The process can take up to 10 minutes to completed.

**STEP 9** Confirm that SearchEngine Status is Active for all Log Collectors in the Collector Group.

- **Do not continue until SearchEngine Status is Active for all Log Collectors in the Collector Group. This will result in purging of logs from the Log Collector being replaced.**

1. Access the Panorama CLI.
2. Show the Log Collector details by running the following commands either:
   - On Panorama for all Log Collectors:
     ```
     show log-collector all
     ```
   - Alternatively, you can run the following command on each Dedicated Log Collector:
     ```
     show log-collector detail
     ```
3. Confirm that SearchEngine Status is Active.

```
Redistribution status: none

Last commit-all: commit succeeded, current ring version 1

SearchEngine status: Active

md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
```

**STEP 10** On the new Log Collector, replace previous Log Collector serial number with the new Log Collector serial number.

You must replace the old Log Collector serial number with the new Log Collector serial number so that the new Log Collector will not run in to purging issues, resulting in the Log Collector being unable to purge old data from the migrated logs when necessary.

1. Access the Log Collector CLI.
2. Replace old Log Collector serial number with new Log Collector serial number:

```
request log-migration-update-logger from <old-log-collector-serial-number> to <new-log-collector-serial-number>
```

### Migrate Logs to a New M-Series Appliance in Panorama Mode

If you need to replace an M-500 or M-100 appliance in Panorama mode (Panorama management server), you can migrate the logs it collected from firewalls by moving its RAID disks to the new M-Series appliance. Moving the disks enables you to recover logs after a system failure on the M-Series appliance or to migrate logs as part of a hardware upgrade (from an M-100 appliance to an M-500 appliance).

This migration procedure covers the following scenario where you are replacing a single M-Series appliance, not in a HA configuration, with a managed collector (Log Collector) in a Collector Group.
STEP 1 | Forward any logs on the SSD of the old M-Series appliance to an external destination if you want to preserve them.

The SSD stores the System and Config logs that Panorama and Log Collectors generate. You cannot move the SSD between M-Series appliances.

Configure Log Forwarding from Panorama to External Destinations.

STEP 2 | Export the Panorama configuration from the decommissioned M-Series appliance in Panorama mode.

1. Log in to the Panorama appliance and select Panorama > Setup > Operations.
2. Click Save named Panorama configuration snapshot, enter a Name to identify the configuration, and click OK.
3. Click Export named Panorama configuration snapshot, select the Name of the configuration you just saved, and click OK. Panorama exports the configuration to your client system as an XML file.

STEP 3 | Remove the RAID disks from the old M-Series appliance.

1. Power off the old M-Series appliance by pressing the Power button until the system shuts down.
2. Remove the disk pairs. For details, refer to the disk replacement procedure in the M-100 or M-500 Appliance Hardware Reference Guide.

STEP 4 | Perform initial setup of the new M-Series appliance.

1. Rack mount the M-Series appliance. Refer to the M-100 or M-500 Appliance Hardware Reference Guide for instructions.
2. Perform Initial Configuration of the M-Series Appliance.
3. Register Panorama.
4. Purchase and activate the Panorama support license or transfer licenses as follows only if the new M-Series appliance is the same hardware model as the old M-Series appliance. If the new M-Series appliance is a different model than the old M-Series appliance, you must purchase new licenses.
   1. Log in to the Palo Alto Networks Customer Support web site.
   2. Select the Assets tab and click the Spares link.
   3. Click the Serial Number of the new M-Series appliance.
   4. Click Transfer Licenses.
   5. Select the old M-Series appliance and click Submit.
5. Activate a firewall management license. If you are migrating from an M-100 appliance to an M-500 appliance, enter the auth-code associated with the migration license.
6. Install Content and Software Updates for Panorama. For important details about software versions, see Panorama, Log Collector, Firewall, and WildFire Version Compatibility.

STEP 5 | Load the Panorama configuration snapshot that you exported from the decommissioned M-Series appliance into the new M-Series appliance in Panorama mode.

1. Log in to the new M-Series appliance and select Panorama > Setup > Operations.
2. Click Import named Panorama configuration snapshot. Browse to the configuration file you exported from the decommissioned M-Series appliance, and click OK.
3. Click Load named Panorama configuration snapshot, select the Name of the configuration you just imported, select a Decryption Key (the master key for Panorama), and click OK. Panorama overwrites its current candidate configuration with the loaded configuration. Panorama displays any errors that occur when loading the configuration file. If errors occurred, save them to a local file. Resolve each error to ensure the migrated configuration is valid.
4. Perform any additional configuration changes as needed.
If the old M-Series appliance used interfaces other than the MGT interface for Panorama services (such as log collection), you must define those interfaces on the new M-Series appliance (Panorama > Setup > Interfaces).

5. Select Commit > Commit to Panorama and Validate Commit. Resolve any errors before proceeding.

6. Commit your changes to the Panorama configuration.

STEP 6 | Insert the disks into the new M-Series appliance. For details, refer to the disk replacement procedure in the M-100 or M-500 Appliance Hardware Reference Guide.

The disk carriers of the M-100 appliance are incompatible with those of the M-500 appliance. Therefore, when migrating between these hardware models, you must unscrew each disk from its old carrier and insert the disk in the new carrier before inserting the disk in the new appliance.

You must maintain the disk pair association. Although you can place a disk pair from slot A1/A2 on the old appliance into slot B1/B2 on the new appliance, you must keep the disks together in the same slot; otherwise, Panorama might not restore the data successfully.

STEP 7 | Contact Palo Alto Networks Customer Support to copy log collector group metadata from the decommissioned M-Series appliance to the new M-Series appliance and restart the mgmtsrvr process.

STEP 8 | If the M-Series appliance was part of a Collector Group, verify that the decommissioned M-Series appliance serial number is still part of the correct Collector Group:

debug log-collector-group show name <Log CollectorGroup name>

If the decommissioned M-Series appliance serial number is no longer a part of the correct Collector Group, then the Tech Support folders were incorrectly copied in Step 4. Contact Palo Alto Networks Customer Support again to copy the Tech Support folders to the correct location.

STEP 9 | 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. To expedite the process, you can launch multiple CLI sessions and run the metadata regeneration command in each session to complete the process simultaneously for every pair. For details, see Regenerate Metadata for M-Series Appliance RAID Pairs.

1. Enable the disk pairs by running the following CLI command for each pair:

   > request system raid add <slot> force no-format

   For example:

   > request system raid add A1 force no-format
   > request system raid add A2 force no-format

   The force and no-format arguments are required. The force argument associates the disk pair with the new appliance. The no-format argument prevents reformatting of the drives and retains the logs stored on the disks.

2. Generate the metadata for each disk pair.
For example:

> request metadata-regenerate slot 1

**STEP 10** | Configure the local Log Collector on the new M-Series appliance.

*For all steps with commands that require a serial number, you must type the entire serial number; pressing the Tab key won’t complete a partial serial number.*

Don’t enable the disks on the new M-Series appliance at this point. When you successfully migrate the logs, Panorama automatically enables the disks.

1. Configure the local Log Collector as a managed collector using the Panorama web interface or using the following CLI commands:

   > configure
   # set log-collector <log-collector_SN> deviceconfig system hostname <log-collector-hostname>
   # exit

2. Commit your changes to Panorama. Don’t commit the changes to the Collector Group just yet.

   > configure
   # commit

3. Verify that the local Log Collector is connected to Panorama and that the status of its disk pairs is present/available.

   > show log-collector serial-number <log-collector_SN>

   The disk pairs will display as disabled at this stage of the restoration process.

**STEP 11** | Add a Log Collector with no disks to a Collector Group.

*From this point, only commits that are required to complete the migration process on Panorama and the Log Collectors. Hold off making any other changes.*

1. Access the Panorama CLI.
2. Overwrite Panorama restriction to allow Log Collector with no disk to be added to a Collector Group: requestlog-migration-set-start

**STEP 12** | Migrate the logs.

1. Access the Panorama CLI.
2. Add the new local Log Collector as a member of the Collector Group and commit your changes to Panorama.

   # set log-collector-group <collector_group_name> logfwd-setting collectors <SN_managed_collector>
   # commit
   # exit
The old local Log Collector still appears in the list of members, because you haven’t deleted it from
the configuration.
3. For each disk pair, migrate the logs to the new appliance.

   > request log-migration from <old_LC_serial_number> old-disk-pair <log_disk_pair> to <new_LC_serial_number> new-disk-pair <log_disk_pair>

   For example:

   > request log-migration from 003001000010 old-disk-pair A to 00300100038 new-disk-pair A

4. Commit the changes to Panorama.

   > configure
   # commit

**STEP 13 |** Reconfigure the Collector Group.

1. Use the web interface to assign the new Log Collector to the firewalls that forward logs (Panorama > Collector Groups > Device Log Forwarding). Give the new Log Collector the same priority in the firewall preference lists as the old Log Collector.

   You cannot use the CLI change the priority assignments of firewall preference lists.

2. Delete the old Log Collector from the Collector Group.

   # delete log-collector-group <group_name> logfwd-setting collectors <old_LC_serial_number>

   For example:

   # delete log-collector-group DC-Collector-Group logfwd-setting collectors 003001000010

3. Delete the old Log Collector from the Panorama configuration and commit your changes to Panorama.

   # delete log-collector <old_LC_serial_number>
   # commit
   # exit

4. Commit the Collector Group changes so that the managed firewalls can send logs to the new Log Collector.

   > commit-all log-collector-config log-collector-group <collector_group_name>

   For example:

   > commit-all log-collector-config log-collector-group DC-Collector-Group
STEP 14 | Generate new keys on the new Log Collector.

   This command is required in order to add the new Log Collector to the Collector Group and should only be run for the Collector Group of the Log Collector being replaced. This step deletes the existing RSA keys and allows Panorama to create new RSA keys.

1. Access the Panorama CLI.
2. Delete all RSA keys on the new Log Collector:
   
   ```
   request logdb update-collector-group-after-replacecollector-group
   <collector-group-name>
   
   The process can take up to 10 minutes to completed.
   ```

STEP 15 | Confirm that SearchEngine Status is Active for all Log Collectors in the Collector Group.

   Do not continue until SearchEngine Status is Active for all Log Collectors in the Collector Group. This will result in purging of logs from the Log Collector being replaced.

1. Access the Panorama CLI.
2. Show the Log Collector details by running the following commands either:
   - On Panorama for all Log Collectors:
     
     ```
     show log-collector all
     ```
   
   Alternatively, you can run the following command on each Dedicated Log Collector:
   
   ```
   show log-collector detail
   ```

3. Confirm that SearchEngine Status is Active.

   ```
   Redistribution status: none
   
   Last commit-all: commit succeeded, current ring version 1
   
   SearchEngine status: Active
   
   md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19
   ```

STEP 16 | On the new Log Collector, replace previous Log Collector serial number with the new Log Collector serial number.

   You must replace the old Log Collector serial number with the new Log Collector serial number so that the new Log Collector will not run into purging issues, resulting in the Log Collector being unable to purge old data from the migrated logs when necessary.

1. Access the Log Collector CLI.
2. Replace old Log Collector serial number with new Log Collector serial number:
   
   ```
   request log-migration-update-logger from <old-log-collector-serial-number>
   to <new-log-collector-serial-number>
   ```
Migrate Logs to a New M-Series Appliance Model in Panorama Mode in High Availability

If you need to replace an M-500 or M-100 appliance in Panorama mode (Panorama management server) with a different M-Series appliance than the M-Series appliance being replaced, you can migrate the logs it collected from firewalls by moving its RAID disks to the new M-Series appliance. Moving the disks enables you to migrate logs as part of a hardware upgrade (from an M-100 appliance to an M-500 appliance).

This migration procedure covers the following scenarios:

- One Panorama HA peer has a managed collector (Log Collector) in a Collector Group.
- Both Panorama HA peers have managed collectors that belong to a single Collector Group. For details, see Multiple Local Log Collectors Per Collector Group.
- Both Panorama HA peers have a managed collector and each is assigned to a separate Collector Group. For details, see Single Local Log Collector Per Collector Group.

**Figure 29: Panorama HA Peer with Collector Group**

- Both Panorama HA peers have managed collectors that belong to a single Collector Group. For details, see Multiple Local Log Collectors Per Collector Group.
- Both Panorama HA peers have a managed collector and each is assigned to a separate Collector Group. For details, see Single Local Log Collector Per Collector Group.

**STEP 1** | Forward any logs on the SSD of the old M-Series appliance to an external destination if you want to preserve them.

The SSD stores the System and Config logs that Panorama and Log Collectors generate. You cannot move the SSD between M-Series appliances.

Configure Log Forwarding from Panorama to External Destinations.

**STEP 2** | Export the Panorama configuration from the Primary decommissioned M-Series appliance in Panorama mode.

1. Log in to the Panorama appliance and select Panorama > Setup > Operations.
2. Click Save named Panorama configuration snapshot, enter a Name to identify the configuration, and click OK.
3. Click **Export named Panorama configuration snapshot**, select the **Name** of the configuration you just saved, and click **OK**. Panorama exports the configuration to your client system as an XML file.

**STEP 3 |** Remove the RAID disks from the old M-Series appliance.

1. Power off the old M-Series appliance by pressing the Power button until the system shuts down.
2. Remove the disk pairs. For details, refer to the disk replacement procedure in the **M-100 or M-500 Appliance Hardware Reference Guide**.

**STEP 4 |** Perform initial setup of the new M-Series appliance.

Repeat this step for each of the new M-Series appliances in the HA configuration.

1. Rack mount the M-Series appliance. Refer to the **M-100 or M-500 Appliance Hardware Reference Guide** for instructions.
2. Perform Initial Configuration of the M-Series Appliance.
3. Register Panorama.
4. Purchase and **activate the Panorama support license** or transfer licenses as follows only if the new M-Series appliance is the same hardware model as the old M-Series appliance. If the new M-Series appliance is a different model than the old M-Series appliance, you must purchase new licenses.

   1. Log in to the **Palo Alto Networks Customer Support web site**.
   2. Select the **Assets** tab and click the **Spares** link.
   3. Click the Serial Number of the new M-Series appliance.
   4. Click **Transfer Licenses**.
   5. **Select** the old M-Series appliance and click **Submit**.
5. **Activate** a firewall management license. If you are migrating from an M-100 appliance to an M-500 appliance, enter the auth-code associated with the migration license.
6. **Install** Content and Software Updates for Panorama. For important details about software versions, see **Panorama, Log Collector, Firewall, and WildFire Version Compatibility**.
7. **Set Up HA on Panorama**. The new M-Series appliance must have the same priority as the HA peer you are replacing.

**STEP 5 |** Load the Panorama configuration snapshot that you exported from the Primary decommissioned M-Series appliance into the new Primary M-Series appliance in Panorama mode.

1. Log in to the new M-Series appliance and select **Panorama > Setup > Operations**.
2. Click **Import named Panorama configuration snapshot**, **Browse** to the configuration file you exported from the decommissioned M-Series appliance, and click **OK**.
3. Click **Load named Panorama configuration snapshot**, select the **Name** of the configuration you just imported, select a **Decryption Key** (the master key for Panorama), and click **OK**. Panorama overwrites its current candidate configuration with the loaded configuration. Panorama displays any errors that occur when loading the configuration file. If errors occurred, save them to a local file. Resolve each error to ensure the migrated configuration is valid.
4. Perform any additional configuration changes as needed.

   *If the old M-Series appliance used interfaces other than the MGT interface for Panorama services (such as log collection), you must define those interfaces on the new M-Series appliance (Panorama > Setup > Interfaces).*

5. Select **Commit > Commit to Panorama** and **Validate Commit**. Resolve any errors before proceeding.
6. **Commit** your changes to the Panorama configuration. Once committed, the Panorama configuration is synced across the HA peers.
**STEP 6** | Insert the disks into the new M-Series appliance. For details, refer to the disk replacement procedure in the M-100 or M-500 Appliance Hardware Reference Guide.

Repeat this step for each of the new M-Series appliances in the HA configuration.

*The disk carriers of the M-100 appliance are incompatible with those of the M-500 appliance. Therefore, when migrating between these hardware models, you must unscrew each disk from its old carrier and insert the disk in the new carrier before inserting the disk in the new appliance.*

You must maintain the disk pair association. Although you can place a disk pair from slot A1/A2 on the old appliance into slot B1/B2 on the new appliance, you must keep the disks together in the same slot; otherwise, Panorama might not restore the data successfully.

**STEP 7** | Contact Palo Alto Networks Customer Support to copy log collector group metadata from the decommissioned M-Series appliance to the new M-Series appliance and restart the `mgmtsrvr` process.

**STEP 8** | If the M-Series appliance was part of a Collector Group, verify that the decommissioned M-Series appliance serial number is still part of the correct Collector Group:

```
debug log-collector-group show name <Log Collector Group name>
```

If the decommissioned M-Series appliance serial number is no longer a part of the correct Collector Group, then the Tech Support folders were incorrectly copied in Step 4. Contact Palo Alto Networks Customer Support again to copy the Tech Support folders to the correct location.

**STEP 9** | 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. To expedite the process, you can launch multiple CLI sessions and run the metadata regeneration command in each session to complete the process simultaneously for every pair. For details, see Regenerate Metadata for M-Series Appliance RAID Pairs.*

1. Enable the disk pairs by running the following CLI command for each pair:

   ```
   > request system raid add <slot> force no-format
   ```

   For example:

   ```
   > request system raid add A1 force no-format
   > request system raid add A2 force no-format
   ```

   The `force` and `no-format` arguments are required. The `force` argument associates the disk pair with the new appliance. The `no-format` argument prevents reformatting of the drives and retains the logs stored on the disks.

2. Generate the metadata for each disk pair.

   ```
   > request metadata-regenerate slot <slot_number>
   ```

   For example:
STEP 10 | Configure the local Log Collector on the new M-Series appliance.

For all steps with commands that require a serial number, you must type the entire serial number; pressing the Tab key won’t complete a partial serial number.

Don’t enable the disks on the new M-Series appliance at this point. When you successfully migrate the logs, Panorama automatically enables the disks.

1. Configure the local Log Collector as a managed collector using the Panorama web interface or using the following CLI commands:

   ```
   request metadata-regenerate slot 1
   ```

   3. Synchronize the configuration of the M-Series appliance HA peers.

   ```
   request high-availability sync-to-remote running-config
   ```

2. Commit your changes to Panorama. Don’t commit the changes to the Collector Group just yet.

   ```
   configure
   # set log-collector <log-collector_SN> deviceconfig system hostname <log-collector-hostname>
   # exit
   ```

3. Verify that the local Log Collector is connected to Panorama and that the status of its disk pairs is present/available.

   ```
   show log-collector serial-number <log-collector_SN>
   ```

   The disk pairs will display as disabled at this stage of the restoration process.

STEP 11 | Add a Log Collector with no disks to a Collector Group.

From this point, only commits that are required to complete the migration process on Panorama and the Log Collectors. Hold off making any other changes.

1. Access the Panorama CLI.
2. Overwrite Panorama restriction to allow Log Collector with no disk to be added to a Collector Group:

   ```
   request log-migration-set-start
   ```

STEP 12 | Migrate the logs.

1. Access the Panorama CLI.
2. Add the new local Log Collector as a member of the Collector Group and commit your changes to Panorama.

   ```
   set log-collector-group <collector_group_name> logfwd-setting collectors <SN Managed Collector>
   # commit
   # exit
   ```
The old local Log Collector still appears in the list of members, because you haven’t deleted it from the configuration.

3. For each disk pair, migrate the logs to the new appliance.

```
> request log-migration from <old_LC_serial_number> old-disk-pair <log_disk_pair> to <new_LC_serial_number> new-disk-pair <log_disk_pair>
```

For example:

```
> request log-migration from 003001000010 old-disk-pair A to 00300100038 new-disk-pair A
```

4. Commit the changes to Panorama.

```
> configure
# commit
```

**STEP 13 | Reconfigure the Collector Group.**

1. Use the web interface to assign the new Log Collector to the firewalls that forward logs (Panorama > Collector Groups > Device Log Forwarding). Give the new Log Collector the same priority in the firewall preference lists as the old Log Collector.

   ![Tip](You cannot use the CLI change the priority assignments of firewall preference lists.)

2. Delete the old Log Collector from the Collector Group.

   ```
   # delete log-collector-group <group_name> logfwd-setting collectors <old_LC_serial_number>
   ```

   For example:

   ```
   # delete log-collector-group DC-Collector-Group logfwd-setting collectors 003001000010
   ```

3. Delete the old Log Collector from the Panorama configuration and commit your changes to Panorama.

   ```
   # delete log-collector <old_LC_serial_number>
   # commit
   # exit
   ```

4. Commit the Collector Group changes so that the managed firewalls can send logs to the new Log Collector.

   ```
   > commit-all log-collector-config log-collector-group <collector_group_name>
   ```

   For example:

   ```
   > commit-all log-collector-config log-collector-group DC-Collector-Group
   ```
STEP 14 | Generate new keys on the new Log Collector.

This command is required in order to add the new Log Collector to the Collector Group and should only be run for the Collector Group of the Log Collector being replaced. This step deletes the existing RSA keys and allows Panorama to create new RSA keys.

1. Access the Panorama CLI.
2. Delete all RSA keys on the new Log Collector:
   
   request logdb update-collector-group-after-replace collector-group <collector-group-name>

   The process can take up to 10 minutes to completed.

STEP 15 | Confirm that SearchEngine Status is Active for all Log Collectors in the Collector Group.

Do not continue until SearchEngine Status is Active for all Log Collectors in the Collector Group. This will result in purging of logs from the Log Collector being replaced.

1. Access the Panorama CLI.
2. Show the Log Collector details by running the following commands either:
   - On Panorama for all Log Collectors:
     
     show log-collector all
   
     Alternatively, you can run the following command on each Dedicated Log Collector:
   
   show log-collector detail

3. Confirm that SearchEngine Status is Active.

   Redistribution status: none

   Last commit-all: commit succeeded, current ring version 1

   SearchEngine status: Active

   md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14 09:58:19

STEP 16 | On the new Log Collector, replace previous Log Collector serial number with the new Log Collector serial number.

You must replace the old Log Collector serial number with the new Log Collector serial number so that the new Log Collector will not run in to purging issues, resulting in the Log Collector being unable to purge old data from the migrated logs when necessary.

1. Access the Log Collector CLI.
2. Replace old Log Collector serial number with new Log Collector serial number:

   request log-migration-update-logger from <old-log-collector-serial-number> to <new-log-collector-serial-number>
Migrate Logs to the Same M-Series Appliance Model in Panorama Mode in High Availability

If you need to replace an M-500 or M-100 appliance deployed in high availability (HA) configuration in Panorama mode (Panorama management server) with the same M-Series appliance as the M-Series appliance being replaced, you can migrate the logs it collected from firewalls by moving its RAID disks to the new M-Series appliance. Moving the disks enables you to recover logs after a system failure on the M-Series appliance.

This migration procedure covers the following scenarios:
- One Panorama HA peer has a managed collector (Log Collector) in a Collector Group.
- Both Panorama HA peers have managed collectors that belong to a single Collector Group. For details, see Multiple Local Log Collectors Per Collector Group.
- Both Panorama HA peers have a managed collector and each is assigned to a separate Collector Group. For details, see Single Local Log Collector Per Collector Group.

**Figure 30: Panorama HA Peer with Collector Group**

- Both Panorama HA peers have managed collectors that belong to a single Collector Group. For details, see Multiple Local Log Collectors Per Collector Group.
- Both Panorama HA peers have a managed collector and each is assigned to a separate Collector Group. For details, see Single Local Log Collector Per Collector Group.

**STEP 1** | Forward any logs on the SSD of the old M-Series appliance to an external destination if you want to preserve them.

The SSD stores the System and Config logs that Panorama and Log Collectors generate. You cannot move the SSD between M-Series appliances.

Configure Log Forwarding from Panorama to External Destinations.

**STEP 2** | Remove the RAID disks from the old M-Series appliance.

1. Power off the old M-Series appliance by pressing the Power button until the system shuts down.
2. Remove the disk pairs. For details, refer to the disk replacement procedure in the M-100 or M-500 Appliance Hardware Reference Guide.
STEP 3 | Perform initial setup of the new M-Series appliance.
1. Rack mount the M-Series appliance. Refer to the M-100 or M-500 Appliance Hardware Reference Guide for instructions.
2. Perform Initial Configuration of the M-Series Appliance.
3. Register Panorama.
4. Purchase and activate the Panorama support license or transfer licenses as follows only if the new M-Series appliance is the same hardware model as the old M-Series appliance. If the new M-Series appliance is a different model than the old M-Series appliance, you must purchase new licenses.
   1. Log in to the Palo Alto Networks Customer Support web site.
   2. Select the Assets tab and click the Spares link.
   3. Click the Serial Number of the new M-Series appliance.
   4. Click Transfer Licenses.
   5. Select the old M-Series appliance and click Submit.
5. Activate a firewall management license. If you are migrating from an M-100 appliance to an M-500 appliance, enter the auth-code associated with the migration license.
6. Install Content and Software Updates for Panorama. For important details about software versions, see Panorama, Log Collector, Firewall, and WildFire Version Compatibility.
7. Perform any additional configuration changes as needed.

   If the old M-Series appliance used interfaces other than the MGT interface for Panorama services (such as log collection), you must define those interfaces on the new M-Series appliance (Panorama > Setup > Interfaces).
8. Set Up HA on Panorama. The new M-Series appliance must have the same priority as the HA peer you are replacing.

STEP 4 | Insert the disks into the new M-Series appliance. For details, refer to the disk replacement procedure in the M-100 or M-500 Appliance Hardware Reference Guide.

   The disk carriers of the M-100 appliance are incompatible with those of the M-500 appliance. Therefore, when migrating between these hardware models, you must unscrew each disk from its old carrier and insert the disk in the new carrier before inserting the disk in the new appliance.

You must maintain the disk pair association. Although you can place a disk pair from slot A1/A2 on the old appliance into slot B1/B2 on the new appliance, you must keep the disks together in the same slot; otherwise, Panorama might not restore the data successfully.

STEP 5 | If the M-Series appliance was part of a Collector Group, verify that the decommissioned M-Series appliance serial number is still part of the correct Collector Group:

debug log-collector-group show name <Log CollectorGroup name>

If the decommissioned M-Series appliance serial number is no longer a part of the correct Collector Group, then the Tech Support folders were incorrectly copied in Step 4. Contact Palo Alto Networks Customer Support again to copy the Tech Support folders to the correct location.

STEP 6 | 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. To expedite the process, you can launch multiple CLI sessions and run the metadata regeneration command in each session to complete the process simultaneously for every pair. For details, see Regenerate Metadata for M-Series Appliance RAID Pairs.
1. Enable the disk pairs by running the following CLI command for each pair:

```
> request system raid add <slot> force no-format
```

For example:

```
> request system raid add A1 force no-format
> request system raid add A2 force no-format
```

The `force` and `no-format` arguments are required. The `force` argument associates the disk pair with the new appliance. The `no-format` argument prevents reformatting of the drives and retains the logs stored on the disks.

2. Generate the metadata for each disk pair.

```
> request metadata-regenerate slot <slot_number>
```

For example:

```
> request metadata-regenerate slot 1
```

3. Synchronize the configuration of the M-Series appliance HA peers.

```
> request high-availability sync-to-remote running-config
```

**STEP 7** Configure the local Log Collector on the new M-Series appliance.

For all steps with commands that require a serial number, you must type the entire serial number; pressing the Tab key won’t complete a partial serial number.

Don’t enable the disks on the new M-Series appliance at this point. When you successfully migrate the logs, Panorama automatically enables the disks.

1. Configure the local Log Collector as a managed collector using the Panorama web interface or using the following CLI commands:

```
> configure
# set log-collector <log-collector_SN> deviceconfig system hostname <log-collector-hostname>
# exit
```

2. Commit your changes to Panorama. Don’t commit the changes to the Collector Group just yet.

```
> configure
# commit
```

3. Verify that the local Log Collector is connected to Panorama and that the status of its disk pairs is present/available.

```
> show log-collector serial-number <log-collector_SN>
```

The disk pairs will display as disabled at this stage of the restoration process.
STEP 8 | Add a Log Collector with no disks to a Collector Group.

- From this point, only commits that are required to complete the migration process on Panorama and the Log Collectors. Hold off making any other changes.

1. Access the Panorama CLI.
2. Overwrite Panorama restriction to allow Log Collector with no disk to be added to a Collector Group:

   ```shell
   requestlog-migration-set-start
   ```

STEP 9 | Migrate the logs.

1. Access the Panorama CLI.
2. Add the new local Log Collector as a member of the Collector Group and commit your changes to Panorama.

   ```shell
   # set log-collector-group <collector_group_name> logfwd-setting
   collectors <SN_managed_collector>
   # commit
   # exit
   ```

   The old local Log Collector still appears in the list of members, because you haven’t deleted it from the configuration.

3. For each disk pair, migrate the logs to the new appliance.

   ```shell
   > request log-migration from <old_LC_serial_number> old-disk-pair <log_disk_pair> to <new_LC_serial_number> new-disk-pair <log_disk_pair>
   ```

   For example:

   ```shell
   > request log-migration from 003001000010 old-disk-pair A to 00300100038 new-disk-pair A
   ```

4. Commit the changes to Panorama.

   ```shell
   > configure
   # commit
   ```

STEP 10 | Reconfigure the Collector Group.

1. Use the web interface to assign the new Log Collector to the firewalls that forward logs (Panorama > Collector Groups > Device Log Forwarding). Give the new Log Collector the same priority in the firewall preference lists as the old Log Collector.

   You cannot use the CLI change the priority assignments of firewall preference lists.

2. Delete the old Log Collector from the Collector Group.

   ```shell
   # delete log-collector-group <group_name> logfwd-setting
   collectors <old_LC_serial_number>
   ```

   For example:
3. Delete the old Log Collector from the Panorama configuration and commit your changes to Panorama.

```bash
# delete log-collector-group DC-Collector-Group logfwd-setting collectors 003001000010
```

4. Commit the Collector Group changes so that the managed firewalls can send logs to the new Log Collector.

```bash
> commit-all log-collector-config log-collector-group <collector_group_name>
```

For example:

```bash
> commit-all log-collector-config log-collector-group DC-Collector-Group
```

**STEP 11** | Generate new keys on the new Log Collector.

![Warning]

This command is required in order to add the new Log Collector to the Collector Group and should only be run for the Collector Group of the Log Collector being replaced. This step deletes the existing RSA keys and allows Panorama to create new RSA keys.

1. Access the Panorama CLI.
2. Delete all RSA keys on the new Log Collector:

```bash
request logdb update-collector-group-after-replace-collector-group <collector-group-name>
```

The process can take up to 10 minutes to completed.

**STEP 12** | Confirm that SearchEngine Status is Active for all Log Collectors in the Collector Group.

![Warning]

Do not continue until SearchEngine Status is Active for all Log Collectors in the Collector Group. This will result in purging of logs from the Log Collector being replaced.

1. Access the Panorama CLI.
2. Show the Log Collector details by running the following commands either:
   - On Panorama for all Log Collectors:
     ```bash
     show log-collector all
     ```
   - Alternatively, you can run the following command on each Dedicated Log Collector:
     ```bash
     show log-collector detail
     ```
3. Confirm that SearchEngine Status is Active.

Redistribution status: none
STEP 13 | On the new Log Collector, replace previous Log Collector serial number with the new Log Collector serial number.

You must replace the old Log Collector serial number with the new Log Collector serial number so that the new Log Collector will not run in to purging issues, resulting in the Log Collector being unable to purge old data from the migrated logs when necessary.

1. Access the Log Collector CLI.
2. Replace old Log Collector serial number with new Log Collector serial number:
   
   ```
   request log-migration-update-logger from <old-log-collector-serial-number>
   to <new-log-collector-serial-number>
   ```

Migrate Log Collectors after Failure/RMA of Non-HA Panorama

If a system failure occurs on a Panorama management server that is not deployed in a high availability (HA) configuration, use this procedure to restore the configuration on the replacement Panorama and restore access to the logs on the Dedicated Log Collectors that it manages. The allowed migration scenarios vary by Panorama management server model:

<table>
<thead>
<tr>
<th>Old/Failed Panorama</th>
<th>New/Replacement Panorama</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panorama virtual appliance</td>
<td>• Panorama virtual appliance</td>
</tr>
<tr>
<td></td>
<td>• M-100 appliance</td>
</tr>
<tr>
<td></td>
<td>• M-500 appliance</td>
</tr>
<tr>
<td>M-100 appliance</td>
<td>• M-100 appliance</td>
</tr>
<tr>
<td></td>
<td>• M-500 appliance</td>
</tr>
<tr>
<td>M-500 appliance</td>
<td>M-500 appliance</td>
</tr>
</tbody>
</table>

Panorama maintains a ring file that maps the segments and partitions that Dedicated Log Collectors use to store logs. An M-Series appliance in Panorama mode stores the ring file on its internal SSD; a Panorama virtual appliance stores the ring file on its internal disk. When a system failure occurs, a non-HA Panorama cannot automatically recover the ring file. Therefore, when you replace Panorama, you must restore the ring file to access the logs on the Dedicated Log Collectors.

This procedure requires that you backed up and exported your Panorama configuration before the system failure occurred.

Palo Alto Networks recommends deploying Panorama in an HA configuration. The active Panorama peer automatically synchronizes the ring file to the passive peer in an HA
configuration, thereby maintaining access to logs on the Dedicated Log Collectors even if you must replace one of the peers.

STEP 1 | Perform initial setup of the new Panorama appliance.
1. Rack mount the M-Series appliance if that is the new appliance. Refer to the M-100 or M-500 Appliance Hardware Reference Guide for instructions.
2. Perform Initial Configuration of the M-Series Appliance or Perform Initial Configuration of the Panorama Virtual Appliance.
   
   If the old M-Series appliance used interfaces other than the MGT interface for Panorama services (such as log collection), you must define those interfaces during initial configuration of the new M-Series appliance (Panorama > Setup > Interfaces).
   The Panorama virtual appliance does not support interfaces other than MGT.
3. Register Panorama.
4. Transfer licenses as follows only if the new Panorama appliance is the same model as the old appliance. Otherwise, you must purchase new licenses.
   1. Log in to the Palo Alto Networks Customer Support web site.
   2. Select the Assets tab and click the Spares link.
   3. Click the Serial Number of the new M-Series appliance.
   4. Click Transfer Licenses.
   5. Select the old appliance and click Submit.
5. Activate a Panorama Support License.
6. Activate a firewall management license.
7. Install Content and Software Updates for Panorama.

   The M-500 appliance requires Panorama 7.0 or a later release. For important details about software versions, see Panorama, Log Collector, Firewall, and WildFire Version Compatibility.

STEP 2 | Restore the configuration from the old Panorama to the replacement Panorama.
1. Log in to the new Panorama and select Panorama > Setup > Operations.
2. Click Import named Panorama configuration snapshot, Browse to the backup configuration file, and click OK.
3. Click Load named Panorama configuration snapshot, select the Name of the file you just imported, and click OK.
4. Select Commit > Commit to Panorama and Commit your changes.
5. Select Panorama > Managed Collectors and verify that the Connected column displays a check mark for the Dedicated Log Collector.
   
   If the Dedicated Log Collector doesn’t appear, you must reconfigure it and its Collector Group as described in step Reconfigure the Dedicated Log Collector and Collector Group if they are missing on Panorama.. Otherwise, skip to Step Fetch the ring file to restore access to the logs stored on the Dedicated Log Collector.

STEP 3 | Reconfigure the Dedicated Log Collector and Collector Group if they are missing on Panorama.
1. Access the CLI of the Dedicated Log Collector and enter the following commands to display the name of its Collector Group.
   1. 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>
```

2. Enter the command:

```
> less mp-log ms.log
```

The following error will display:

```
Dec04 11:07:08 Error:
pan_cms_convert_resp_ring_to_file(pan_ops_cms.c:3719): Current
configuration does not contain group CA-Collector-Group
```

In this example, the error message indicates that the missing Collector Group has the name CA-Collector-Group.

2. Configure the Collector Group and assign the Dedicated Log Collector to it.

```
> configure
# set log-collector-group <collector-group-name>
# set log-collector-group <collector-group-name> logfwd-setting
collector <serial-number>
```

3. Commit the changes to Panorama but not to the Collector Group.

```
# commit
# exit
```

**STEP 4** | Fetch the ring file to restore access to the logs stored on the Dedicated Log Collector.

1. Access the CLI of the new Panorama.
2. Fetch the ring file:

```
> request fetch ring from log-collector <serial-number>
```

For example:

```
> request fetch ring from log-collector 009201000343
```

*If you don’t know the serial number of the Dedicated Log Collector, log in to its CLI and enter the `show system info` operational command.*

3. Commit your changes to the Collector Group.

```
> commit-all log-collector-config log-collector-group <collector-group-name>
```

---

**Regenerate Metadata for M-Series Appliance RAID Pairs**

When a system failure occurs on the M-500 or M-100 appliance and you need to physically move the disks from one appliance to another, regenerating the metadata is necessary. The metadata is required to locate
logs on the disk; when a user issues a log query, the query consults this metadata to access the requested log data.

For each configured RAID disk pair in the M-Series appliance, you must access the appliance CLI and run the following command to regenerate the metadata:

```plaintext
> request metadata-regenerate slot <slot_number>
```

For example:

```plaintext
> request metadata-regenerate slot 1
```

The size of the RAID disks determines how long metadata regeneration takes. On average, it takes an hour for every 100GB. When you run the command, the CLI session is locked until the command is fully executed. You can use multiple CLI sessions to save time. For example, to replace four RAID pairs of 1TB drives with a total of 4TB of log data, launch four CLI sessions and run the command in each session to regenerate metadata simultaneously for all the pairs/slots in about 10 hours.

During metadata regeneration, the Collector Group to which these disks belong is not available and the disk pair is not available for any logging or reporting operations (writes/queries). However, you can perform other tasks such as handling new firewall connections or managing configuration changes on the managed firewalls. All other Collector Groups that Panorama manages and that aren’t part of this RMA process can perform the assigned logging and reporting functionality as normal.
Replace an RMA Firewall

To minimize the effort required to restore the configuration on a managed firewall involving a Return Merchandise Authorization (RMA), replace the serial number of the old firewall with that of the new firewall on Panorama. To then restore the configuration on the replacement firewall, either import a firewall state that you previously generated and exported from the firewall or use Panorama to generate a partial device state for managed firewalls running PAN-OS 5.0 and later versions. By replacing the serial number and importing the firewall state, you can resume using Panorama to manage the firewall.

- Partial Device State Generation for Firewalls
- Before Starting RMA Firewall Replacement
- Restore the Firewall Configuration after Replacement

Partial Device State Generation for Firewalls

When you use Panorama to generate a partial device state, it replicates the configuration of the managed firewalls with a few exceptions for Large Scale VPN (LSVPN) setups. You create the partial device state by combining two facets of the firewall configuration:

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

In an LSVPN setup, the partial device state bundle that you generate on Panorama is not the same as the version that you export from a firewall (by selecting Device > Setup > Operations and clicking Export device state). If you manually ran the device state export or scheduled an XML API script to export the file to a remote server, you can use the exported device state in your firewall replacement workflow.

If you did not export the device state, the device state that you generate in the replacement workflow will not include the dynamic configuration information, such as the certificate details and registered firewalls, that is required to restore the complete configuration of a firewall functioning as an LSVPN portal. See Before Starting RMA Firewall Replacement for more information.

Panorama does not store the device state; you generate it on request using the CLI commands listed in Restore the Firewall Configuration after Replacement.

Before Starting RMA Firewall Replacement

☐ The firewall you will replace must have PAN-OS 5.0.4 or a later version. Panorama cannot generate the device state for firewalls running older PAN-OS versions.
☐ Record the following details about the firewall you will replace:
  - **Serial number**—You must enter the serial number on the Palo Alto Networks Customer Support website to transfer the licenses from the old firewall to the replacement firewall. You will also enter this information on Panorama, to replace all references to the old serial number with the new serial number of the replacement firewall.
  - **(Recommended) PAN-OS version and the content database version**—Installing the same software and content database versions, including the URL database vendor, enables you to create the same state on the replacement firewall. If you decide to install the latest version of the content database,
you might notice differences because of updates and additions to the database. To determine the versions installed on the firewall, access the firewall System logs stored on Panorama.

☐ Prepare the replacement firewall for deployment. Before you import the device state bundle and restore the configuration, you must:

- Verify that the replacement firewall is the same model as the old firewall and is enabled for similar operational capability. Consider the following operational features: must the replacement firewall have multiple virtual systems, support jumbo frames support, or operate in CC or FIPS mode?
- Configure network access, transfer the licenses, and install the appropriate PAN-OS and content database versions.

☐ You must use the Panorama CLI to complete this firewall replacement process, and therefore your administrator account must have the superuser or panorama-admin user role.

☐ If you have an LSVPN configuration, and are replacing a Palo Alto Networks firewall deployed as a satellite or as an LSVPN portal, the dynamic configuration information that is required to restore LSVPN connectivity will not be available when you restore the partial device state generated on Panorama. If you followed the recommendation to frequently generate and export the device state for firewalls in an LSVPN configuration, use the device state that you previously exported from the firewall itself instead of generating one on Panorama.

If you have not manually exported the device state from the firewall, and need to generate a partial device state on Panorama, the missing dynamic configuration impacts the firewall replacement process as follows:

- **If the firewall you are replacing is a GlobalProtect portal** that is explicitly configured with the serial number of the satellites (Network > GlobalProtect > Portals > Satellite Configuration), when restoring the firewall configuration, although the dynamic configuration is lost, the portal firewall will be able to authenticate the satellites successfully. The successful authentication will populate the dynamic configuration information and LSVPN connectivity will be reinstated.
- **If you are replacing a satellite firewall**, it will not be able to connect and authenticate to the portal. This failure occurs either because the serial number was not explicitly configured on the firewall (Network > GlobalProtect > Portals > Satellite Configuration) or, if the serial number was explicitly configured, because the serial number of the replaced firewall does not match that of the old firewall. To restore connectivity after importing the device state bundle, the satellite administrator must log in to the firewall and enter the credentials (username and password) for authenticating to the portal. After authentication, the dynamic configuration required for LSVPN connectivity is generated on the portal.

However, if the firewall was configured in a high availability configuration, after restoring the configuration, the firewall will automatically synchronize the running configuration with its peer and attain the latest dynamic configuration required to function seamlessly.

### Restore the Firewall Configuration after Replacement

To restore the firewall configuration on the new firewall, you will first perform initial configuration on the new firewall, including setting the operational mode, upgrading the PAN-OS software and content release version to match what was installed on the old firewall. You will then export the device state of the old firewall from Panorama and import it onto the new firewall. Finally, you will go back to Panorama to validate that the new firewall has connected and then sync it with Panorama.

**STEP 1 | Perform initial configuration** on the new firewall and verify network connectivity.

Use a serial port connection or a Secure Shell (SSH) connection to add an IP address, a DNS server IP address, and to verify that the new firewall can access the Palo Alto Networks updates server.

**STEP 2 | (Optional) Set the Operational mode** on the new firewall to match that on the old firewall.

A serial port connection is required for this task.
1. Enter the following CLI command to access maintenance mode on the firewall:

   > debug system maintenance-mode

2. For Operational mode, select **Set FIPS Mode** or **Set CCEAL 4 Mode** from the main menu.

**STEP 3**
Retrieve the license(s) on the new firewall.

Enter the following command to retrieve the licenses:

   > request license fetch

**STEP 4** *(Optional)* Match the operational state of the new firewall with that of the old firewall. For example, enable multi-virtual system (multi-vsyst) capability for a firewall that was enabled for multi-vsyst capability.

Enter the commands that pertain to your firewall settings:

   > set system setting multi-vsyst on
   > set system setting jumbo-frame on

**STEP 5**
Upgrade the PAN-OS version on the new firewall.

You must upgrade to the same PAN-OS installed on the old firewall. You must upgrade the content release versions to the same or later version that is installed on the old firewall.

Enter the following commands:

1. To upgrade the content release version:

   > request content upgrade download latest
   > request content upgrade install version latest

2. To upgrade the PAN-OS software version:

   > request system software download version <version>
   > request system software install version <version>

**STEP 6**
Go to the Panorama CLI and export the device state bundle from the old firewall to a computer using Secure Copy (SCP) or TFTP (you cannot do this from the web interface).

*If you manually exported the device state from the firewall, you can skip this step.*

The export command generates the device state bundle as a tar zipped file and exports it to the specified location. This device state will not include the LSVPN dynamic configuration (satellite information and certificate details).

Enter one of the following commands:

   > scp export device-state device <old serial#> to <login>
   @ <serverIP>: <path>

   or
STEP 7 | Replace the serial number of the old firewall with that of the new replacement firewall on Panorama.

By replacing the serial number on Panorama you allow the new firewall to connect to Panorama after you restore the configuration on the firewall.

1. Enter the following command in Operational mode:

```
tftp export device-state device <old serial#> to <login>
@ <serverIP>: <path>
```

2. Enter Configuration mode and commit your changes.

```
> replace device old <old SN#> new <new SN#>
configure
# commit
```

3. Exit Configuration mode.

```
# exit
```

STEP 8 | On the new firewall, import the device state and commit the changes.

1. Access the web interface of the new firewall.
2. Select **Device** > **Setup** > **Operations** and click the **Import Device State** link in the Configuration Management section.
3. Browse to locate the file and click **OK**.
4. **Commit** your changes to the running configuration on the firewall.

STEP 9 | From Panorama, verify that you successfully restored the firewall configuration.

1. Access the Panorama web interface and select **Panorama** > **Managed Devices**.
2. Verify that the Connected column for the new firewall has a check mark.

STEP 10 | Synchronize the firewall with Panorama.

1. Access the Panorama web interface, select **Commit** > **Commit and Push** and **Edit Selections** in the Push Scope.
2. Select **Device Groups**, select the device group that contains the firewall, and **Include Device and Network Templates**.
3. Select **Collector Groups** and select the Collector Group that contains the firewall.
4. Click **OK** to save your changes to the Push Scope.
5. **Commit and Push** your changes.

*If you need to generate reports for a period when the old firewall was still functional after you installed the new firewall, you must generate a separate query for each firewall serial number because replacing the serial number on Panorama does not overwrite the information in logs.*
## Troubleshoot Commit Failures

If commit or push operation failures occur on Panorama, check for the following conditions:

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Condition</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template or device group push failure</td>
<td>The ability to receive template and device groups configuration changes from Panorama is disabled on the firewall.</td>
<td>Access the firewall web interface, select <strong>Device &gt; Setup</strong>, edit the Panorama Settings, and then click <strong>Enable Device and Network Template</strong> and <strong>Enable Panorama Policy and Objects</strong>.</td>
</tr>
<tr>
<td>Panorama commit failure or template, device group, or Collector Group push failure</td>
<td>The Panorama management server has an earlier software version than the Dedicated Log Collectors or firewalls that it manages.</td>
<td>Upgrade the Panorama management server to the same or a higher software version than the managed firewalls, Log Collectors, and WildFire appliances and appliance clusters. For details, see Panorama, Log Collector, Firewall, and WildFire Version Compatibility.</td>
</tr>
</tbody>
</table>
Troubleshoot Registration or Serial Number Errors

On the M-500 or M-100 appliance, if the Panorama > Support page doesn't display support license details or the Panorama > Setup > Management page displays Unknown for the Serial Number even after you Register Panorama, perform the following steps:

**STEP 1 |** Record the Panorama serial number from the order fulfillment email that Palo Alto Networks sent when you placed your order for Panorama.

**STEP 2 |** Select Panorama > Setup > Management and edit the General Settings.

**STEP 3 |** Enter the Serial Number and click OK.

**STEP 4 |** Select Commit > Commit to Panorama and Commit your changes.
Troubleshoot Reporting Errors

If Panorama fails to generate a report, or the report is missing expected data, its content versions (such as the Applications database) might differ from those on the managed collectors and firewalls. The content versions on Panorama must be the same as or lower than the content versions on the managed collectors and firewalls. For details, see Panorama, Log Collector, Firewall, and WildFire Version Compatibility.
View Task Success or Failure Status

Click the Task Manager icon at the bottom right of the Panorama web interface to view the success or failure of a task. The Task Manager also displays a detailed message to help debug an issue. For details, see Use the Panorama Task Manager.
Downgrade from Panorama 8.0

Panorama 8.0 introduced enhanced logging capabilities. However, this format is not backwards compatible with Panorama or Log Collectors running a release earlier than Panorama 8.0. Before you downgrade Panorama, Log Collectors, and firewalls, use the following workflow to first migrate logs to the pre-PAN-OS 8.0 log format. Then, downgrade firewalls before you downgrade Log Collectors and Panorama running a Panorama 8.0 release to an earlier feature release. This procedure works for both Panorama managing a local Log Collector and managing one or more Dedicated Log Collectors.

Migrating logs is not a required step. If you do not need to access your existing log data, or are planning to upgrade back to a Panorama 8.0 release soon, then you can avoid migrating your logs. However, if access to previous log data is required, continue with the log migration task. Before you begin this downgrade, schedule a maintenance window that can accommodate the log migration task, which takes approximately 24 hours for each 2TB of data, during which you cannot query or search logs, generate reports, or push configuration changes to Log Collectors undergoing migration. The downgrade workflow involves first upgrading your Panorama and Log Collectors to Panorama 8.0.2 before you migrate logs and downgrade Log Collectors or Panorama. If the Log Collectors aggregate logs from firewalls running PAN-OS 8.0, you must also downgrade those firewalls to the same or an earlier release than the release version to which you are downgrading Panorama.

STEP 1 | Save a backup of the Panorama and managed devices configuration files.
1. Export Panorama and device configuration snapshot (Panorama > Setup > Operations).
2. Save the exported .tgz file to a location external to Panorama, Log Collectors, or firewalls. You can use this backup to restore the configuration if you experience problems that cause you to start over.

STEP 2 | (Panorama and Log Collectors running Panorama 8.0 or 8.0.1 only) Upgrade Panorama and Log Collectors to Panorama 8.0.2 or later release.

Panorama 8.0 introduced a new log format that previous releases do not support. However, the ability to migrate the log format was introduced in Panorama 8.0.2. As a result, you will first need to upgrade the software to Panorama 8.0.2 from an 8.0 or 8.0.1 release before migrating the log format and software to Panorama 7.1.

Use the following procedures to upgrade Panorama and Log Collectors to Panorama 8.0.2 or later release as needed:
1. Install content and then software updates for Panorama.
2. Deploy content and then software updates to Log Collectors.

STEP 3 | Save a backup of the Panorama and managed devices configuration files.
1. Export Panorama and device configuration snapshot (Panorama > Setup > Operations).
2. Save the exported .tgz file to a location external to Panorama, Log Collectors, or firewalls. You can use this backup to restore the configuration if you experience problems that cause you to start over.

**STEP 4** | Downgrade each firewall running a PAN-OS 8.0 release.

*If downgrading more than one firewall, streamline the process by having each firewall-specific PAN-OS 7.1 image downloaded to Panorama before you start downgrading. For example, to downgrade your PA-200, PA-3050, and PA-5060 firewalls to PAN-OS 7.1, download the PanOS_700-7.1.0, PanOS_3000-7.1.0, and PanOS_5000-7.1.0 images.*

Panorama requires that all firewalls are running the same or an earlier PAN-OS release. Thus, before you can downgrade Panorama, use and repeat the appropriate tasks below according to your environment to downgrade all managed firewalls:

1. **Check Now** for available images (Panorama > Device Deployment > Software).
2. Locate the PAN-OS 7.1 image for each model or series of firewalls you intend to downgrade. If the image is not already downloaded, then **Download** it.

**Non-HA Firewalls**

Click **Install** in the Action column for the PAN-OS 7.1 version, select all the firewalls you intend to downgrade, select **Reboot device after install**, and click **OK**.

**Active/Active HA Firewalls**

1. Click **Install**, disable (clear) **Group HA Peers**, select either of the HA peers, select **Reboot device after install**, and click **OK**. Wait for the firewall to finish rebooting before you proceed.
2. Click **Install**, disable (clear) **Group HA Peers**, select the HA peer that you didn’t update in the previous step, select **Reboot device after install**, and click **OK**.

**Active/Passive HA Firewalls**

In this example, the active firewall is named fw1 and the passive firewall is named fw2:

1. Click **Install** in the Action column for the appropriate update, clear **Group HA Peers**, select fw2, select **Reboot device after install**, and click **OK**.
2. After fw2 finishes rebooting, verify fw1 (Dashboard > High Availability widget) that fw2 is still the passive peer (the Local firewall state is **active** and the Peer-fw2 is **passive**).
3. Access fw1 and **Suspend local device** (Device > High Availability > Operational Commands).
4. Access fw2 (Dashboard > High Availability widget) and verify that the Local firewall state is **active** and the Peer firewall is suspended.
5. Access Panorama, select **Panorama** > **Device Deployment** > **Software**, click **Install** in the Action column for the appropriate update, clear **Group HA Peers**, select fw1, select **Reboot device after install**, and click **OK**. Wait for fw1 to finish rebooting before you proceed.
6. Access fw1 (Dashboard > High Availability widget) and verify that the Local firewall state is **passive** and the Peer (fw2) is **active**.

*If you enabled preemption in the Election settings (Device > High Availability > General), then fw1 will be reinstated as the active peer after reboot.*

**STEP 5** | Before downgrading a Log Collector, disable log forwarding to that Log Collector to avoid losing the log data during migration.

*Make sure to not push the configuration changes to any device group or template. This will apply the new IP addresses to the devices, and log forwarding will continue.*
You will need to temporarily disable log forwarding to avoid data loss and avoid putting unnecessary stress on devices undergoing log migration. Logs generated during the migration will be buffered on the firewall, and forwarded to the designated location once log forwarding is enabled.

*Make sure to keep track of the original IP addresses that will be edited to disable log forwarding. You will need to restore these IPs to re-enable log forwarding.*

**For Panorama in Panorama Mode:**

1. Select Panorama > Setup > Interfaces and select Management.
2. Change the IP Address to different routable IP address and click OK.
3. If a dedicated port on Panorama is used for log forwarding, select the port and disable (clear) Device Management and Device Log Collection. Repeat this step for all dedicated ports used for log forwarding.

   *To quickly identify if a dedicated port is used for log forwarding, refer to the Services Enabled column and confirm that Device Management and Log Collection is listed.*

4. Commit to Panorama. Do not push the configuration change to devices, as it will push the new Management IP address to the firewalls and log forwarding will continue.
5. Log back in to Panorama using the new IP address.
6. Select Push to Devices and Edit Selections. You will need to Deselect All Device Groups and Templates, and Select All Collector Groups. Click OK and Push.

**For Panorama with logs forwarded to Dedicated Log Collectors undergoing downgrade:**

1. Select Panorama > Managed Collectors, select a Dedicated Log Collector that will undergo downgrade from Panorama 8.0 and select Interfaces.
2. Select Management and change the IP Address to a different routable IP address and click OK.
3. If a dedicated port on Panorama is used for log forwarding, select the port and disable (clear) Device Management and Device Log Collection. Repeat this for all dedicated ports used for log forwarding.

   *To quickly identify if a dedicated port is used for log forwarding, refer to the Services Enabled column and confirm that Device Management and Log Collection is listed.*

4. Click OK to exit the configuration screen and Commit to Panorama.
5. Select Push to Devices and Edit Selections. You will need to Deselect All Device Groups and Templates, and Select All Collector Groups. Click OK and Push.

**STEP 6 | Migrate existing logs to the pre-8.0 format so Panorama and Log Collectors can read log data after the downgrade.**

You cannot pause or stop the migration after you begin. Disrupting the migration will cause some or all log data to become inaccessible. If the log migration is interrupted for any reason, repeat this step to restart the migration process. The migration will start anew, and not pick up from the point where the disruption occurred.

Migrating your logs is not a required step. If you do not need to access your existing logs, or are planning to upgrade back to Panorama soon, then avoid migrating your logs. Existing log data will be accessible again once Panorama and Log Collectors have been upgraded back to an 8.0 or later release. However, if access to your previous logs is required, continue with the log migration task.

During the migration, you cannot search within or query logs or generate reports and Panorama and Log Collectors cannot receive any new logs.
1. **Access the Panorama CLI.**
2. Migrate logs to the pre-8.0 format using the commands appropriate for your environment:
   - On Panorama with a local Log Collector or on a Dedicated Log Collector:
     ```bash
     request logdb downgrade
     ```
   - On Panorama for each Collector Group:
     ```bash
     request logdb downgrade collector-group <collector-group-name>
     ```

**STEP 7 |** Monitor the status of the log migration.

If you decide that you would like to end the log migration and continue with downgrade, you will need to gracefully power down the Panorama or Log Collector to avoid any data inconsistencies or data corruption. Alternatively, you can continuing to Step Downgrade each Log Collector running Panorama 8.0 to downgrade while the migration is running. This will ensure that the appliance is powered down gracefully. Please note that not all data will have been migrated, meaning that only some data will be available upon downgrade.

The migration takes approximately 24 hours for each 2TB of data. You can monitor progress during the downgrade process.

You can continue to push configuration changes to your managed firewalls during the migration. You cannot push configuration changes to a Log Collector that is undergoing a log format migration.

1. **Access the Panorama CLI.**
2. Check the status of the migration:
   - On Panorama with a local Log Collector or on a Dedicated Log Collector:
     ```bash
     request logdb downgrade-in-progress
     ```
   - On Panorama for each Collector Group:
     ```bash
     request logdb downgrade-in-progress <collector-group-name>
     ```

It takes roughly 30-40 minutes after you start the migration before these commands display an output. When they do display output, the result is `Logger downgrade in progress` if the migration is still in progress. If the migration is finished (or was interrupted or was not started), the command displays `No logger downgrade is in progress`.

**STEP 8 |** Downgrade each Log Collector running Panorama 8.0.

1. **Check Now** for available images (Panorama > Device Deployment > Software).
2. Locate the Panorama 7.1 image. If the image is not already downloaded, then **Download** it (Action column).
3. After the download completes, **Install** the image on each Log Collector running Panorama 8.0. Select **Reboot device after install** to automatically reboot the device when the upgrade has completed.

**STEP 9 |** Downgrade Panorama.

1. **Check Now** for available images (Panorama > Device Deployment > Software).
2. Locate the Panorama 7.1 image. If the image is not already downloaded, then **Download** it.
3. After the download completes, **Install** the image on Panorama.
4. Reboot Panorama if the downgrade requires that:
   - If prompted to reboot, click **Yes**. If you see a CMS **Login** prompt, press Enter without typing the username or password. When the Panorama login prompt appears, enter the username and password you set during initial configuration.
• If you are not prompted to reboot, select Panorama > Setup > Operations and click Reboot Panorama in the Device Operations section.

STEP 10 | Re-enable log forwarding from the firewalls to Log Collectors.

If you disabled log forwarding in Step Before downgrading a Log Collector, disable log forwarding to that Log Collector to avoid losing the log data during migration., you will need to re-enable log forwarding once the downgrade has completed for Panorama and Log Collectors. All logs that would have been sent during the procedure will be forwarded to the appropriate Log Collector.

For Panorama in Panorama Mode:
1. Select Panorama > Setup > Interfaces and select Management.
2. Change the IP Address back to the original IP address.
3. If a dedicated port on Panorama is used for log forwarding, select the port and enable Device Management and Device Log Collection. Repeat this for all dedicated ports used for log forwarding.
4. Commit to Panorama.
5. Log back in to Panorama using the original IP address.
6. Select Push to Devices and Edit Selections. You will need to Deselect All Device Groups and Templates, and Select All Collector Groups. Click OK and Push.

For Panorama with logs forwarded to Dedicated Log Collectors undergoing downgrade:
7. Select Panorama > Managed Collectors, select a Dedicated Log Collector that underwent downgrade from Panorama 8.0 and select Interfaces.
8. Select Management and change the IP Address back to the original IP address and click OK.
9. If a dedicated port on Panorama is used for log forwarding, select the port and enable Device Management and Device Log Collection. Repeat this for all dedicated ports used for log forwarding.
10. Click OK to exit the configuration screen and Commit to Panorama.
11. Select Push to Devices and Edit Selections. You will need to Deselect All Device Groups and Templates, and Select All Collector Groups. Click OK and Push.