Cortex Data Lake
Getting Started Guide
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

## Get Started with Cortex Data Lake

- About Cortex Data Lake
- Cortex Data Lake Log Sources
- Cortex Data Lake Apps
- Plan Your Cortex Data Lake Deployment
- Cortex Data Lake License
- Cortex Data Lake for Panorama-Managed Firewalls
- Activate Cortex Data Lake (Panorama-Managed)
- Forward Logs to Cortex Data Lake (Panorama-Managed)
- Activate Cortex Data Lake
- Allocate Storage Based on Log Type
- Connect Firewalls to Cortex Data Lake
- Start Sending Logs to Cortex Data Lake
- View Cortex Data Lake Status
- View Logs in Cortex Data Lake
- TCP Ports and FQDNs Required for Cortex Data Lake
Get Started with Cortex Data Lake

Welcome to the Palo Alto Networks Cortex Data Lake! The Cortex Data Lake provides cloud-based, centralized log storage and aggregation for cloud-delivered services and apps.

The following topics describe how to get started with the Cortex Data Lake:

- About Cortex Data Lake
- Cortex Data Lake License
- Cortex Data Lake for Panorama-Managed Firewalls
- Activate Cortex Data Lake
- Allocate Storage Based on Log Type
- Connect Firewalls to Cortex Data Lake
- Start Sending Logs to Cortex Data Lake
- View Cortex Data Lake Status
- View Logs in Cortex Data Lake
- TCP Ports and FQDNs Required for Cortex Data Lake

Note: Use the Cortex Sizing Calculator to decide on the amount of storage you’d like in Cortex Data Lake.
About Cortex Data Lake

Palo Alto Networks® Cortex Data Lake provides cloud-based, centralized log storage and aggregation for your on premise, virtual (private cloud and public cloud) firewalls, for Prisma Access, and for cloud-delivered services such as Traps management service.

The Cortex Data Lake is secure, resilient, and fault-tolerant, and it ensures your logging data is up-to-date and available when you need it. It provides a scalable logging infrastructure that alleviates the need for you to plan and deploy Log Collectors to meet your log retention needs. If you already have on premise Log Collectors, the new Cortex Data Lake can easily complement your existing setup. You can augment your existing log collection infrastructure with the cloud-based Cortex Data Lake to expand operational capacity as your business grows, or to meet the capacity needs for new locations.

With this service, Palo Alto Networks takes care of the ongoing maintenance and monitoring of the logging infrastructure so that you can focus on your business. Skip to the next topics to learn more about Cortex Data Lake Log Sources, Cortex Data Lake Apps, and what to consider as you Plan Your Cortex Data Lake Deployment.

Cortex Data Lake Log Sources

Here are the products and services that can send logs to Cortex Data Lake:

- **Palo Alto Networks Firewalls**: You can onboard individual firewalls directly to Cortex Data Lake. Use the app Explore to view all log records that the firewalls forward to Cortex Data Lake.
- **Panorama-Managed Firewalls**: If you’re using Panorama, you can onboard firewalls to Cortex Data Lake at scale, instead of onboarding each individual firewall. All Cortex Data Lake logs are visible directly in Panorama, and in Explore.
- **Traps management service**: Traps management service is a cloud-based logging infrastructure that allows you to centralize the collection and storage of logs generated by your Traps agents regardless of location. The Traps agents and Traps management service can forward all logs to the Cortex Data Lake. You can view the logs for your agents in Traps management service, and in Explore.
- **Prisma Access**: With Prisma Access, Palo Alto Networks deploys and manages the security infrastructure globally to secure your remote networks and mobile users. Prisma Access logs directly to Cortex Data
Lake. You can view the logs, ACC, and reports from Panorama for an aggregated view into your remote network and mobile user traffic. To enable logging for Prisma Access, you must purchase a Cortex Data Lake license. Log traffic does not use the licensed bandwidth you purchased for Prisma Access.

- **Cortex XDR**: Cortex XDR alerts (both Analytics and Investigation and Response alerts) are automatically written to Cortex Data Lake as log records. This is done so that other apps can read and respond to alerts. These logs records are not visible in Explore; however, you can use the Log Forwarding app to forward Cortex XDR alerts to the email or Syslog destination of your choice.

### Cortex Data Lake Apps

Cortex Data Lake includes the following apps which you can use to manage and view your logs. After you’ve activated Cortex Data Lake, these apps are visible to you on the Cortex hub.

- **Cortex Data Lake**: After activating Cortex Data Lake, the Cortex Data Lake app is listed on the Cortex hub as one of your apps. If you have multiple instances of Cortex Data Lake, you can choose which instance of the app you want to open. Use the Cortex Data Lake app to configure log storage quota and to check the status of a Cortex Data Lake instance.
- **Explore**: Use Explore to search, filter, and export log data. This app offers you critical visibility into your enterprise’s network activities by allowing you to easily examine network and endpoint log data.
- **Log Forwarding app**: Use this app to archive the logs you send to the Cortex Data Lake for long-term storage, SOC, or internal audit directly from the Cortex Data Lake. You can forward your Cortex Data Lake logs to an external destination such as a Syslog server or an email server. (Or, you continue to forward logs directly from the firewalls to your Syslog receiver).

### Plan Your Cortex Data Lake Deployment

Here are some requirements and tips to consider as you plan your Cortex Data Lake deployment:

- Use the Cortex Sizing Calculator to calculate the amount of storage you might need in Cortex Data Lake.
- When planning your deployment, consider that Panorama or a next-generation firewall cannot connect to the Cortex Data Lake from behind a proxy (Cortex Data Lake requires mutual authentication).
- Firewalls that are managed by Panorama must be running PAN-OS 8.0.6 or later to forward logs to Cortex Data Lake; firewalls that are not managed by Panorama must be running PAN-OS 9.0.3 or later to forward logs to Cortex Data Lake. For now, PA-220 and PA-800 Series firewalls do not support Cortex Data Lake logging without Panorama—for these firewalls, continue to use Panorama to enable Cortex Data Lake logging.
- The process to activate Cortex Data Lake can vary depending on the other products you’re using—review Cortex Data Lake License to learn more.
- If you’re using Panorama and/or Prisma Access, review this other list of requirements to make sure you have everything you need to get started with Cortex Data Lake.

When you have your plan in place, here’s what you’ll need to do to roll out your Cortex Data Lake deployment:

- Activate Cortex Data Lake
 Allocate Storage Based on Log Type
☐ Connect Firewalls to Cortex Data Lake
☐ Start Sending Logs to Cortex Data Lake
## Cortex Data Lake License

Cortex Data Lake collects log data from next-generation firewalls, Prisma Access, and Traps management service. When you purchase Cortex Data Lake, all firewalls registered to your support account receive a Cortex Data Lake license. You'll also receive an auth code that you'll need to use to activate your Cortex Data Lake instance.

How you activate and implement Cortex Data Lake can vary depending on the other products and services you’re using:

<table>
<thead>
<tr>
<th>Product or Service</th>
<th>How to Activate Cortex Data Lake</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewalls without Panorama</strong></td>
<td>□ Use the hub to activate Cortex Data Lake. &lt;br&gt; □ After you’ve activated Cortex Data Lake, you can start forwarding firewall logs.</td>
</tr>
<tr>
<td><strong>Firewalls managed by Panorama</strong></td>
<td>□ Use the Customer Support Portal to activate Cortex Data Lake.  &lt;br&gt; Activating Cortex Data Lake on the Customer Support Portal allows you to associate your auth code with Panorama, and to get the Cloud Services plugin that is required for Panorama. &lt;br&gt; □ After you’ve activated Cortex Data Lake and installed the Cloud Services plugin, you can start forwarding logs from Panorama-managed firewalls.</td>
</tr>
<tr>
<td><strong>Panorama Managed Prisma Access</strong></td>
<td>□ Use the Customer Support Portal to activate Cortex Data Lake.  &lt;br&gt; Activating Cortex Data Lake on the Customer Support Portal allows you to associate your auth code with Panorama, and to get the Cloud Services plugin that is required Panorama Managed Prisma Access. &lt;br&gt; □ Activate and install Panorama Managed Prisma Access. &lt;br&gt; □ Start forwarding Prisma Access log to Cortex Data Lake.</td>
</tr>
<tr>
<td><strong>Cloud Managed Prisma Access</strong></td>
<td>□ Use the hub to activate Cortex Data Lake. &lt;br&gt; □ License and activate Cloud Managed Prisma Access.</td>
</tr>
<tr>
<td><strong>Traps management service</strong></td>
<td>□ (Traps-included Cortex Data Lake storage) If you’re using only the Cortex Data Lake storage that's included with Traps, all you need to do is activate the Traps management service.  &lt;br&gt; □ Otherwise, use the hub to activate Cortex Data Lake.  &lt;br&gt; Activating Cortex Data Lake from the hub also includes the option to merge your Traps-included 100GB instance with a new Cortex Data Lake instance.</td>
</tr>
</tbody>
</table>

As part of another product subscription or evaluation, you might have received some Cortex Data Lake log storage; for example, Traps management service includes access to a 100 GB instance of Cortex Data Lake. To extend your storage capacity, you can purchase and merge a new Cortex Data Lake instance with the instance that came with your product. In this case, consider that the product-included storage is tied to your product license and the additional Cortex Data Lake instance has its own separate license. If the additional Cortex Data Lake license expires before your product license does, your Cortex Data Lake storage capacity reverts to the amount of storage you received with your product (for example, 100 GB with Traps). While
your storage capacity is reduced, your log storage quota settings don't change; the percentage of overall storage you've allocated for each log type remains the same.

In all cases, when your Cortex Data Lake subscription expires, you'll have a 30-day grace period to renew your license before log data is deleted.
Cortex Data Lake for Panorama-Managed Firewalls

Palo Alto Networks firewalls send logs directly to Cortex Data Lake. However, you can use Panorama to onboard firewalls to Cortex Data Lake at scale, instead of onboarding individual firewalls. Cortex Data Lake onboarding includes provisioning the certificates that firewalls need to securely connect to Cortex Data Lake, configuring device groups and templates with the right settings, and then pushing those settings to managed firewalls. When you’re done, you can use Panorama to view records for the logs that are stored in Cortex Data Lake (or, you can also use the Explore app to view and interact with your logs).

If you’re using Prisma Access, using Panorama to implement Cortex Data Lake is required.

Before you begin to onboard Panorama-managed firewalls, review these requirements to make sure you’re ready. You’ll need:

- A Panorama virtual appliance or hardware-based Panorama appliance running Panorama 8.0.6 or later.
- A Panorama device management license.
- The Cloud Services plugin. This plugin is required if you’re using Prisma Access. The following workflow shows you how to download the latest plugin version, and install it on Panorama.
- Next-generation firewalls with a valid support license that are managed by Panorama and are running PAN-OS 8.0.6 or later. Version 8.1.3 or later is recommended if you want to collect enhanced application logs for Magnifier.
- A Cortex Data Lake license, in addition to the device management for Panorama. When you license the Cortex Data Lake, all firewalls registered to your support account receive a Cortex Data Lake license. You can then use Panorama templates and device groups to configure the firewalls to forward logs to the Cortex Data Lake.

   *The Cortex Data Lake license provisions the service in one theatre/region only (for example, Europe or Americas). If you want the firewalls that belong to one template to send logs to one theatre and the firewalls that belong to another template to send logs to a different theatre, you will need two Panorama appliances and two Cortex Data Lake licenses.*

- Consider that Panorama or a next-generation firewall cannot connect to the Cortex Data Lake from behind a proxy (Cortex Data Lake requires mutual authentication).

Now that you’ve reviewed the requirements above, continue on to:

- **Activate Cortex Data Lake (Panorama-Managed)**
- **Forward Logs to Cortex Data Lake (Panorama-Managed)**

### Activate Cortex Data Lake (Panorama-Managed)

If you’re using Panorama to manage Prisma Access or on-prem firewalls, the steps here describe how to use the Customer Support Portal to activate Cortex Data Lake. Because Panorama can provision the certificates that firewalls require to securely connect to the Cortex Data Lake, this gives you a way to onboard multiple firewalls to Cortex Data Lake at once.

Before you begin, review these requirements to make sure you have everything you need to get started.

*If you’re NOT using Panorama, Activate Cortex Data Lake on the hub instead. How you activate and implement Cortex Data Lake varies depending on the products and services you’re using. Learn more about what you should do to get started with Cortex Data Lake based on the product you’re using.*
STEP 1 | To set up Panorama, install the Panorama virtual appliance and perform initial configuration, or set up the M-Series appliance.

⚠️ You must configure DNS server(s) and an NTP server rather than setting the date and time manually so that Panorama can stay in sync with the Cortex Data Lake.

- To configure NTP, select Panorama > Setup > Services > NTP. Set a value for the NTP server, for example pool.ntp.org
- To configure DNS servers, select Panorama > Setup > Services and enter a value for the primary and optionally for the secondary DNS servers.

STEP 2 | Register Panorama and activate the support license.

1. Log in to the Customer Support Portal (CSP) and select Assets > Devices > Register New Device.
2. Select Register device using Serial Number or Authorization Code, and click Submit.
3. Enter the Panorama Serial Number provided in the email you received with your order fulfillment along with the required Location Information (as indicated by the asterisks) and then Agree and Submit the EULA.
   After you see the registration complete message, close the Device Registration dialog.
4. Find the Panorama instance you just registered and click the corresponding edit button in the Actions column.
5. To activate the Support license, select Activate Auth-Code and then enter the Support Authorization Code you received in the email and Agree and Submit.

STEP 3 | Activate the Cortex Data Lake.

1. Log in to the Customer Support Portal (CSP) and select Assets > Cloud Services > Activate Cloud Services Auth-Code.
2. To license the Cortex Data Lake, enter the Authorization code you received in the email, select the Panorama Serial Number for the Panorama you plan to use, and select the Logging Region. Then Agree and Submit the EULA.
After you see the registration complete message, close the Device Registration dialog.

**STEP 4** | Verify the Quantity and Part Description of the Cortex Data Lake (named Logging Service below) license you just activated.

**STEP 5** | Retrieve the Cortex Data Lake and support license on Panorama.

1. Select Panorama > Licenses and click Retrieve license keys from license server.
2. Verify that you see the Cortex Data Lake license and the support license.
STEP 6 | Download and install the Cloud Services plugin:

The way you download and install the plugin depends on whether you are using Panorama 8.0.6 or later or Panorama 8.1.0 or later.

On Panorama 8.0.x:

1. Log in to the Customer Support Portal and select Updates > Software Updates.
2. Find the Cloud Services plugin version 1.2.0-h2 or later in the Panorama Integration Plug In section and download it to your local system. Plugin versions 1.0.x are no longer supported on any version of Panorama.
3. To install the plugin, log in to the Panorama Web Interface of the Panorama you selected when you licensed Prisma Access, select Panorama > Plugins > Upload and Browse for the plugin File that you downloaded from the CSP.
4. Install the plugin.

On Panorama 8.1.0 and later:

On Panorama 8.1.0 or later, you can either download the plugin from the CSP and then upload it to Panorama, or you can check for plugin updates directly from Panorama as follows:

1. Select Panorama > Plugins and click Check Now to display the latest cloud_services plugin updates.
2. Download plugin version 1.2.0-h2.

Plugin versions 1.0.x are no longer supported on any version of Panorama.
3. After downloading the plugin, **Install** it.

Installing a newer version of the Cloud Services plugin overwrites the previously installed version. If you are installing the plugin for the first time, after you successfully install, Panorama refreshes and the Cloud Services menu displays on the **Panorama** tab.

**STEP 7 | Verify your account.** You must be a super user on the CSP to generate the one-time password required to verify your account.

When you try to use the Cloud Services plugin for the first time after installing it, you will be prompted to verify your account. This step ensures that the Panorama serial number is registered to use the Cortex Data Lake, and enables a secure communication path between the Cortex Data Lake and Panorama.

1. Log in to the Palo Alto Networks Customer Support Portal (CSP) as a super user and select **Assets > Cloud Services**.
2. Click **Generate OTP**.
3. Select the serial number for the **Panorama** where you installed the Cloud Services plugin and click **Generate OTP**.
4. Click **Copy to Clipboard**.
You have ten minutes to enter the OTP before it expires.

5. Go back to Panorama and click Panorama > Cloud Services > Status to display the Verify Account dialog.
6. Paste the OTP you just generated and click Verify.

   If Verify is disabled, check that you have configured both a DNS server and an NTP server on Panorama > Setup > Services.

STEP 8 | Verify the connection status between Panorama and the Cortex Data Lake.

You can use the Panorama CLI or the Panorama web interface with cloud service plugin 1.2 or later to verify that the connection was successful.

- Use the following CLI command:

```bash
admin@Panorama>

show plugins cloud_services status logging-service
```

   pass{"@status": "success", .....}

- Select Panorama > Cloud Services > Status > Status, and click the details link to verify that Panorama was able to successfully retrieve the Cortex Data Lake certificate, fetch the Customer Identification number and the region in which your Cortex Data Lake instance is deployed, and confirm that the Panorama appliance is connected to the Cortex Data Lake (Logging Service below). If any of these checks fail, the Status is reported as an Error.

STEP 9 | On the Cortex hub, View Cortex Data Lake Status to verify that the Cortex Data Lake is provisioned successfully.

STEP 10 | Allocate Storage Based on Log Type. Make sure to allocate log quota for each log type because there isn’t a default log quota allocation.

STEP 11 | Panorama does not forward any logs to the Cortex Data Lake. Continue to Forward Logs to Cortex Data Lake (Panorama-Managed).
Remember that for any firewalls that you want to forward logs to Cortex Data Lake, if they're not already managed by Panorama, you'll first need to add the firewalls to Panorama as managed devices.

Forward Logs to Cortex Data Lake (Panorama-Managed)

For Panorama-managed firewalls to send logs to Cortex Data Lake, the firewalls and Panorama need to be running PAN-OS 8.0.6 and you'll also need to activate Cortex Data Lake. Activating Cortex Data Lake includes provisioning the certificate that the firewalls need to securely connect to Cortex Data Lake. Only after you've activated Cortex Data Lake can you enable Panorama-managed firewalls to forward logs.

The following steps describe how to start forwarding logs: first, you'll enable firewalls to communicate with Cortex Data Lake, and then you can specify the log types that you want to send. You can use Panorama device groups and templates to push these settings to managed firewalls.

If you’re using:

- **Firewalls without Panorama**—To forward logs to Cortex Data Lake from firewalls that are not managed by Panorama follow these steps instead.
- **Traps**—To enable Traps to log to the Cortex Data Lake, see the Traps Administrator’s Guide.

How you activate and implement Cortex Data Lake varies depending on the products and services you’re using. Learn more about what you should do to get started with Cortex Data Lake based on the product you’re using.

**STEP 1 | Add the firewall as a managed device on Panorama.** Before you add the firewall as a managed device, you must configure NTP so that the firewall can stay in sync with the Cortex Data Lake.

On the firewall, select Device > Setup > Services > NTP and set it to the same NTP Server Address you configured on Panorama, for example pool.ntp.org.

**STEP 2 | Retrieve and push the Cortex Data Lake licenses for managed firewalls.**

1. From Panorama, select Panorama > Device Deployment > License.
2. Click Refresh and then select the firewalls from the list. Panorama retrieves the licenses, deploys them to the selected firewalls, and updates the licensing status on the Panorama web interface.

Make sure you see that Panorama successfully installed the Cortex Data Lake license on the firewall.

*Do not click Refresh again until the first refresh completes. When the refresh completes, you will see Status shows Completed and Progress is 100%, along with some Details about whether the refresh succeeded.*
STEP 3 | From Panorama, create a template and a device group to push log forwarding settings to the firewalls that you want to log to the Cortex Data Lake.

STEP 4 | Enable the firewalls in the template to send logs to the Cortex Data Lake and select the region where you want the logs stored.

If some firewalls in your deployment are sending logs to dedicated Log Collectors or to Panorama with a local Log Collector, only firewalls that belong to the template with the Enable Cortex Data Lake option selected can send logs to the Cortex Data Lake.

1. Select Device > Setup > Management.
2. Select the Template that contains the firewalls you want to log to the Cortex Data Lake.
3. Edit the Cortex Data Lake settings.

4. Enable only one of the following two options:
   - **Enable Logging Service**—Send and save logs to Cortex Data Lake only. With this option selected, you can still view your firewall logs in Panorama; Panorama connects to Cortex Data Lake and acts as an interface for your log data. You can also use Explore to see and interact with your log data.
   - **Enable Duplicate Logging**—For firewalls running PAN-OS 8.1.x and later, you can send and save logs both to Cortex Data Lake and to your Panorama and log collection setup. Firewalls save a copy of all log data to both Panorama and Cortex Data Lake except for system and config logs which are sent to Panorama only.

5. **Enable Enhanced Application Logging** to allow the firewall to collect data for apps running the Palo Alto Networks Cloud Services environment. These logs provide Palo Alto Networks Cloud services apps increased visibility into network activity, and in some cases, are required to support app features.

6. Select the Region where you want to forward logs for the firewalls associated with this template and then click OK.
Starting with PAN-OS 9.0.2, you might notice an option to Onboard Without Panorama. This setting is important only for firewalls that are not managed by Panorama. There’s no need to populate it when you’re enabling Panorama-managed firewalls to forward logs to Cortex Data Lake.

7. (Panorama 9.0 only) Specify the **Connection count to Cortex Data Lake for PA-7000s and PA-5200s**.

   Specify the number of connections that are established between the firewalls and the Cortex Data Lake (range is 1 to 20; default is 5) to forward logs to the Cortex Data Lake.

8. **Configure interfaces and zones** in the template.

**STEP 5 | (Optional)** If you do not want to use the management interface to forward logs to the Cortex Data Lake, enable the firewall to send traffic through a different interface.

Beginning with content release version 8067, you can use the paloalto-shared-services and paloalto-logging-service App-IDs to safely enable traffic between the firewalls and the Cortex Data Lake. You will also need to create a security policy rule to allow this traffic on any firewalls between the firewalls sending the logs and the internet. If the upstream firewalls are not Palo Alto Networks firewalls, you must enable access to the TCP Ports and FQDNs Required for Cortex Data Lake. Keep in mind that the firewalls and the Cortex Data Lake use mutual certificate authentication and therefore cannot be decrypted and you cannot connect through a proxy server.

1. **Configure a service route** for Palo Alto Networks Services.
2. **Create a security policy rule** that enables the firewalls to communicate with the Cortex Data Lake.

   This is required if you are using the Palo Alto Networks Services service route instead of the management interface to forward logs to the Cortex Data Lake. To create this rule, set the **Application** to `paloalto-shared-services` (requires content release version 8066 or later) and `paloalto-logging-service` (requires content release version 8033 or later). The paloalto-shared-services covers the common traffic for different Palo Alto Networks services and is a dependency for the paloalto-logging-service.
Make sure you place this rule above any rule that allows the web-browsing and SSL traffic to the internet. In addition, if you have a firewall between Panorama and the internet, you must also add a rule that allows paloalto-shared-services and paloalto-logging service traffic on that firewall. The paloalto-logging-service app enables the firewalls and Panorama to connect to the Cortex Data Lake on ports 444 and 3978, the defaults ports for this communication.

If that firewall is not a Palo Alto Networks firewall, create a security policy rule on that firewall that allows outbound SSL traffic to the internet to allow the TCP Ports and FQDNs Required for Cortex Data Lake so that the internet gateway firewall does not block traffic between Panorama and the Cortex Data Lake.

*The firewalls and Panorama need access to the domain 8.0.0 on port 3978 in order to forward logs to the Cortex Data Lake. This is true even if you are using the paloalto-logging-service App-ID to safely enable Cortex Data Lake traffic.*

**STEP 6 | Specify the log types to forward to the Cortex Data Lake.**

The way you enable forwarding depends on the log type. For logs that are generated based on a policy match, use a log forwarding profile within a device group. For other log types, use the Log Settings configuration within a template.

1. To configure forwarding of System, Configuration, User-ID, and HIP Match logs:
   1. Select **Device > Log Settings**.
   2. Select the **Template** that contains the firewalls you want to forward logs to the Cortex Data Lake.
   3. For each log type that you want to forward to the Cortex Data Lake, **Add** a match list filter. Give it a **Name**, optionally define a **Filter**, select the **Panorama/Logging Service** check box, and click **OK**.
2. To configure forwarding of all other log types that are generated when a policy match occurs, such as Traffic, Threat, WildFire Submission, URL Filtering, Data Filtering, and Authentication logs, create and attach a Log Forwarding profile to each policy rule for which you want to forward logs.

   1. Select the Device Group, and then select Objects > Log Forwarding to Add a profile. In the log forwarding profile match list, add each log type that you want to forward.

      If you have already turned on Enhanced Application Logs, fully enable the firewall to forward these log types by selecting Enable enhanced application logging to Cortex Data Lake. Notice that when you select this option, match lists that specify the log types required for enhanced application logging are automatically added to the profile.

   2. Select Panorama/Cortex Data Lake as the Forward Method to enable the firewalls in the device group to forward the logs to the Cortex Data Lake. You will be able to monitor the logs and generate reports from Panorama.

3. Create basic security policy rules in the device group.

   Until the firewall has interfaces and zones and a basic security policy, it will not let any traffic through, and only traffic that matches a security policy rule will be logged (by default).

4. For each rule you create, select Actions and select the Log Forwarding profile that allows the firewall to send logs to the Cortex Data Lake.
STEP 7 | Commit your changes to Panorama and push them to the template and device group you created.

STEP 8 | Verify that the firewall logs are being forwarded to the Cortex Data Lake.

- On Panorama 8.1.7 or later, select Monitor > Logs and find the column From Logging Service to identify whether the logs that you view on Panorama are stored on the Cortex Data Lake. The value yes indicates that the logs are saved on the Cortex Data Lake.

Use the CLI command request logging-service-forwarding status for detailed information on the connectivity status to the Cortex Data Lake and to verify whether you have enabled duplicate log forwarding and Enhanced Application Logs.

- On a firewall (PAN-OS 8.0.6 or later), enter the CLI command show logging-status:

<table>
<thead>
<tr>
<th>Type</th>
<th>Last Log Created</th>
<th>Last Log Fwded</th>
<th>Last Log Fwded Total Seq Num Acked</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fwded</td>
<td>Last Seq Num</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Log Fwded</td>
<td>Total Logs Fwded</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

> CMS 0
Not Sending to CMS 0

> CMS 1

Not Sending to CMS 1

>Log Collection Service

'Log Collection log forwarding agent' is active and connected to xx.xxx.xxx.xx

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>2017/07/26 16:33:20</td>
<td>2017/07/26 16:34:09</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>323</td>
<td>321</td>
<td>2</td>
</tr>
</tbody>
</table>

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>13634645</td>
<td>13634637</td>
<td>84831</td>
</tr>
</tbody>
</table>

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>threat</td>
<td>2014/12/01 14:47:52</td>
<td>2017/07/26 16:34:24</td>
<td>93</td>
</tr>
<tr>
<td></td>
<td>557404252</td>
<td>557404169</td>
<td>93</td>
</tr>
</tbody>
</table>

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>traffic</td>
<td>2017/07/28 18:03:39</td>
<td>2017/07/28 18:03:50</td>
<td>1740</td>
</tr>
<tr>
<td></td>
<td>3619306590</td>
<td>3619306590</td>
<td>1740</td>
</tr>
</tbody>
</table>

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>hipmatch</td>
<td>Not Available</td>
<td>Not Available</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>Not Available</td>
<td>0</td>
</tr>
</tbody>
</table>

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>gtp-tunnel</td>
<td>Not Available</td>
<td>Not Available</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>Not Available</td>
<td>0</td>
</tr>
</tbody>
</table>
Look for the ‘Log collection log forwardingagent’ is active and connected to <IP_address> line. You can also see that CMS 0 and CMS (the Log Collectors) are not receiving logs.

On firewalls running PAN-OS 8.1.7 or later, select the Show Status link on Device > Setup > Management > Cortex Data Lake to verify that the firewall is connected and sending logs to the Cortex Data Lake.

STEP 9 | Use the ACC on Panorama to monitor network activity.

You can also use Monitor > Manage Custom Reports and generate Run Now reports on summary logs. You cannot generate scheduled reports or generate reports on detailed logs stored on the Cortex Data Lake.

STEP 10 | Archive Cortex Data Lake logs.

If you want to be able to archive the logs you send to the Cortex Data Lake for long-term storage, SOC, or internal audit directly from the Cortex Data Lake, you can use the Log Forwarding app, which is included with your Cortex Data Lake (formerly called Logging Service) license. This app enables log forwarding from the Cortex Data Lake to an external destination such as a Syslog server or an email server. Refer to the Log Forwarding App Getting Started Guide for more information. Alternatively, you continue to forward logs directly from the firewalls to your Syslog receiver.
Activate Cortex Data Lake

After purchasing Cortex Data Lake, you received an auth code that you’ll use to activate Cortex Data Lake. The steps here describe how to activate Cortex Data Lake on the hub if you’re using Traps Management Service, Cloud Managed Prisma Access, or firewalls that are not managed by Panorama. These steps include the option to merge logs from a Traps-included storage instance of Cortex Data Lake with a new Cortex Data Lake instance.

How you activate and implement Cortex Data Lake varies depending on the products and services you’re using. Learn more about what you should do to get started with Cortex Data Lake based on the product you’re using. For example, if you’re using Panorama (either to manage on-prem firewalls or for Panorama Managed Prisma Access), you’ll need to use the Customer Support Portal to activate Cortex Data Lake instead of the hub.

STEP 1 | Activate Cortex Data Lake.
1. Log in to the hub.
3. Enter the Auth Code you received to activate Cortex Data Lake and Continue.
4. Enter an Instance Name so that you can identify this app instance in the hub, and optionally add a Description.
5. Select the Region you want to host the Cortex Data Lake instance: Europe or Americas.
6. (If you’re using Traps management service) Select the Cortex Data Lake instance with Traps Included Storage-100GB so that you can merge the logs from the 100GB tenant into the Cortex Data Lake instance that you are activating.
7. Click Agree and Activate.
8. Verify the Cortex Data Lake is successfully activated on the hub.
Cortex Data Lake was previously called the Logging Service, and you might continue to see that name listed as the application name.

STEP 2 | In the hub, log in to the Cortex Data Lake app instance you just activated.

STEP 3 | Select Configuration and allocate storage for each log type that you plan to forward to Cortex Data Lake.

When you add a new log source (like the firewall or Cortex XDR), log storage quota is not allocated for the log types that belong to this source. Until you allocate log storage, logs are not saved in Cortex Data Lake.

STEP 4 | Continue to Connect Firewalls to Cortex Data Lake.

After you enable firewalls to authenticate to Cortex Data Lake, you can start forwarding logs.
Allocate Storage Based on Log Type

For each log type you’re storing in Cortex Data Lake, you must set the log storage quota (the amount of storage you want to allocate for each log type). By default, when you add a new log source, quota is not allocated for the log types that belong to this source. Until you configure the log storage quota, logs are not saved in Cortex Data Lake.

STEP 1 | Sign In to the Cortex hub at https://apps.paloaltonetworks.com/.

If you do not see the Cortex Data Lake app, you might not have the correct user role. Learn more about app roles and how to assign them.

STEP 2 | Select the Cortex Data Lake instance for which you want to allocate log storage quota.

If you have multiple Cortex Data Lake instances, hover over the Cortex Data Lake tile and then select the Cortex Data Lake instance from the list of available instances associated with your account.

STEP 3 | Select Configuration and adjust the storage allocated for each type of log.

STEP 4 | Expand the log type drop-down and configure the following settings for each log type.

- Enter the Size with units—KB, MB, GB, TB—of the log storage space that you want to allocate for the log type. You cannot view the log sub types until you allocate log storage space.
- Set the Quota for each log sub type as a percentage of the total size you allocated.

Setting the quota for a log subtype to 0% means that the Cortex Data Lake does not store the logs. If you reset quota to 0%, all existing logs will be deleted.

For a log type such as Firewall or Traps, you must allocate 100% of the total quota across the log sub types. The percentage allocation across all log sub types is summed up and displayed as the total percentage of quota for the log type. If the quota allocated is over or under 100%, you cannot apply your changes.

- (Optional) Specify the MAX DAYS the Cortex Data Lake should retain logs. Set this value only if you have a company or regulatory retention policy and you need to delete logs after a given time period. If you do not enter a value here (leave it blank), logs will not be deleted on the Cortex Data Lake until the available storage space runs out.

- Specify the MIN RETENTION WARNING, which is the threshold (in days) for which you want to store logs and be warned if there isn't enough space on your Cortex Data Lake instance to hold logs for the minimum number of specified days. You can specify a retention period of up to 2000 days. On reaching this threshold, the Cortex Data Lake displays a warning to inform you that the desired log retention period is not being met. If you don't specify a threshold, the Cortex Data Lake does not notify you.

- View the ACTUAL RETENTION DAYS, which is the number of days for which logs have been stored on the Logging Service. Logs are rolled over when the max days is reached or the available storage space runs out. Use this information to learn about the current utilization of the logging service or which logs have the longest duration, and assess if you need to reallocate quota across the log subtypes to meet your log retention policy.

STEP 5 | Apply your changes.
### Configuration

#### Quota Allocation

<table>
<thead>
<tr>
<th>LOG TYPE</th>
<th>QUOTA</th>
<th>SIZE</th>
<th>MAX DAYS</th>
<th>MIN RETENTION DAYS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>100%</td>
<td>2 TB</td>
<td>[0-2000]</td>
<td>[0-2000]</td>
</tr>
<tr>
<td>Detailed</td>
<td>60%</td>
<td>1.2 TB</td>
<td>[0-2000]</td>
<td>[0-2000]</td>
</tr>
<tr>
<td>Infrastructure and Audit</td>
<td>10%</td>
<td>204.8 GB</td>
<td>[0-2000]</td>
<td>[0-2000]</td>
</tr>
<tr>
<td>Summary</td>
<td>30%</td>
<td>614.4 GB</td>
<td>[0-2000]</td>
<td>[0-2000]</td>
</tr>
<tr>
<td>Traps</td>
<td>100%</td>
<td>1024 GB</td>
<td>[0-2000]</td>
<td>[0-2000]</td>
</tr>
<tr>
<td>Threat</td>
<td>1%</td>
<td>10.24 GB</td>
<td>[0-2000]</td>
<td>[0-2000]</td>
</tr>
<tr>
<td>Config</td>
<td>1%</td>
<td>10.24 GB</td>
<td>[0-2000]</td>
<td>[0-2000]</td>
</tr>
<tr>
<td>System</td>
<td>15%</td>
<td>153.6 GB</td>
<td>[0-2000]</td>
<td>[0-2000]</td>
</tr>
<tr>
<td>Analytic</td>
<td>65%</td>
<td>649.92 GB</td>
<td>[0-2000]</td>
<td>[0-2000]</td>
</tr>
<tr>
<td>Unallocated</td>
<td></td>
<td>32.21 KB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Connect Firewalls to Cortex Data Lake

Before you can start sending logs to Cortex Data Lake, you must generate the key that allows firewalls to securely connect to Cortex Data Lake. Onboarding keys are valid for 24 hours, and you can use a single key for as many firewalls as you'd like to onboard in that 24-hour period.

After you use the Cortex Data Lake app to generate the key, copy the key down. You'll no longer be able to reference it when you close out of the Cortex Data Lake app, and you need to add the key to the each firewall that you want to connect to Cortex Data Lake. Generating a new key invalidates any other valid keys generated in the last 24 hours.

This direct onboarding to Cortex Data Lake—where you do not need Panorama to provision the key that firewalls require to connect to Cortex Data Lake—is supported for firewalls running PAN-OS 9.0.3 and later (upgrade now).

If you’re using Panorama or Prisma Access: Follow this workflow instead to connect firewalls to Cortex Data Lake and to start forwarding logs.

STEP 1 | Log in to the hub and open the Cortex Data Lake app.

STEP 2 | Select Firewall On-Boarding and Generate PSK to generate the onboarding key. Copy or save the key so that you can use it in the coming steps.

STEP 3 | Log in to the firewall that you want to connect to Cortex Data Lake.

STEP 4 | Select Device > Licenses and confirm that the Logging Service (now called Cortex Data Lake) license is active.

When you purchased Cortex Data Lake, all firewalls registered to your support account received a Cortex Data Lake license. If you don’t see the Logging Service license, select Retrieve license keys from license server to manually refresh the firewall licenses.

STEP 5 | Ensure that the Palo Alto Networks Services service route is set to use the management interface.

1. Select Device > Setup > Services > Global (Omit Global on a firewall without multiple virtual system capability).
2. Under Services Features, click Service Route Configuration.
3. Select Customize.
5. For Source Interface, select MGT.
6. Click OK to exit the Service Route Source window, and click OK again to exit Service Route Configuration.

You only need to use the management interface during activation. After, you can configure a different interface to forward logs to Cortex Data Lake. For details, see how to Start Sending Logs to Cortex Data Lake.

STEP 6 | Set up the connection to Cortex Data Lake and check connection status:

1. Select Device > Setup > Management and find the Logging Service settings (Cortex Data Lake used to be called the Logging Service).
2. (Important) Before you populate any other settings, find the Onboard to Cloud option. Click Connect and enter the PSK (onboarding key) you generated in the Cortex Data Lake app. Then, click Connect again.

After connecting, a window should pop-up to confirm that the firewall is equipped with the certificate it needs to authenticate to Cortex Data Lake. You can also check the Task Manager to confirm that the firewall has successfully authenticated to Cortex Data Lake.

3. Next, Enable Logging Service to connect the firewall to Cortex Data Lake. If you want the firewall to collect data that increases visibility for Palo Alto Networks applications, like Cortex XDR, you can also Enable Enhanced Application Logging.

Cortex Data Lake logging doesn’t begin until after you’ve specified the log types you want to forward. Complete the steps here first, to make sure that the firewall is connected to Cortex Data Lake, and then you can Start Sending Logs to Cortex Data Lake.

Do not select the option to Enable Duplicate Logging. This option applies only to Panorama-managed firewalls (in this case, you can choose if you’d like Panorama to also store firewall logs, in addition to Cortex Data Lake).

4. Select the geographic Region of the Cortex Data Lake instance to which you’ll be forwarding logs. This is the region you chose when you were activating the Cortex Data Lake (either Europe or Americas).

5. Show Status to check Logging Service Status (Cortex Data Lake). The status for License, Certificate, and Customer Info should show as green.

Device connectivity might not display a green status indicator, even when the firewall is successfully connected to Cortex Data Lake (we’re working on this issue).

STEP 7 | The firewall is now connected to Cortex Data Lake, but it is not yet forwarding logs. Follow these steps to start sending logs and to best secure the traffic between the firewall and Cortex Data Lake.
Start Sending Logs to Cortex Data Lake

Before you can start sending logs to Cortex Data Lake, you must:

- Activate your Cortex Data Lake instance and
- connect the firewall to Cortex Data Lake.

The following steps describe how to start forwarding logs to Cortex Data Lake, from firewalls that are not managed by Panorama. You’ll specify the log types you want to forward, and also take steps to make sure that the traffic between the firewall and Cortex Data Lake remains secure.

**If you’re using PAN-OS 9.0.2 or earlier release versions, Panorama-managed firewalls, or Traps:**

- **PAN-OS 9.0.2 or earlier**—Direct firewall onboarding to Cortex Data Lake is supported for firewalls running PAN-OS 9.0.3 and later. If your firewall is running PAN-OS 9.0.2 or an earlier release version, you either need Panorama or you need to upgrade to PAN-OS 9.0.3 to support a Cortex Data Lake deployment.
- **Panorama**—Follow this workflow instead to enable Panorama-managed firewalls to start forwarding logs to Cortex Data Lake.
- **Traps**—To enable Traps to log to the Cortex Data Lake, see the Traps Administrator’s Guide.

How you activate and implement Cortex Data Lake varies depending on the products and services you’re using. Learn more about what you should do to get started with Cortex Data Lake based on the product you’re using.

*Cortex Data Lake was previously called the Logging Service; you might continue to see references to the Logging Service in the firewall web interface.*

**STEP 1** | If you haven’t done so already, Activate Cortex Data Lake and Connect Firewalls to Cortex Data Lake.

**STEP 2** | Configure NTP so that the firewall can stay in sync with Cortex Data Lake.

On the firewall, select Device > Setup > Services > NTP and set it to the same NTP Server Address you configured on Panorama, for example pool.ntp.org.

**STEP 3** | *(Optional)* If you do not want to use the management interface to forward logs to the Cortex Data Lake, enable the firewall to send traffic through a different interface.

Beginning with content release version 8067, you can use the paloalto-shared-services and paloalto-logging-service App-IDs to safely enable traffic between the firewalls and the Cortex Data Lake. You will also need to create a security policy rule to allow this traffic on any firewalls between the firewalls sending the logs and the internet. If the upstream firewalls are not Palo Alto Networks firewalls, you must enable access to the TCP Ports and FQDNs Required for Cortex Data Lake. Keep in mind that the firewalls and the Cortex Data Lake use mutual certificate authentication, so they cannot be decrypted and you cannot connect through a proxy server.

1. Configure a service route for Palo Alto Networks Services.
2. **Create a security policy rule** that enables the firewalls to communicate with the Cortex Data Lake.

   This is required if you are using the Palo Alto Networks Services service route instead of the management interface to forward logs to the Cortex Data Lake. To create this rule, set the **Application** to `paloalto-shared-services` (requires content release version 8066 or later) and `paloalto-logging-service` (requires content release version 8033 or later). The paloalto-shared-services covers the common traffic for different Palo Alto Networks services and is a dependency for the paloalto-logging-service.
Make sure you place this rule above any rule that allows web-browsing and SSL traffic to the internet. In addition, if you have a firewall between Panorama and the internet, you must also add a rule that allows paloalto-shared-services and paloalto-logging service traffic on that firewall. The paloalto-logging-service app enables the firewalls and Panorama to connect to the Cortex Data Lake on ports 444 and 3978, the defaults ports for this communication.

If that firewall is not a Palo Alto Networks firewall, create a security policy rule on that firewall that allows outbound SSL traffic to the internet to allow the TCP Ports and FQDNs Required for Cortex Data Lake so that the internet gateway firewall does not block traffic between Panorama and the Cortex Data Lake.

The firewalls and Panorama need access to the domain 8.0.0 on port 3978 in order to forward logs to the Cortex Data Lake. This is true even if you are using the paloalto-logging-service App-ID to safely enable Cortex Data Lake traffic.

**STEP 4 **Specify the log types to forward to Cortex Data Lake.

1. To forward System, Configuration, User-ID, and HIP Match logs:
   1. Select **Device > Log Settings**.
   2. For each log type that you want to forward to the Cortex Data Lake, **Add** a match list filter. Give it a **Name**, optionally define a **Filter**, select the **Logging Service** check box, and click **OK**.

2. To forward log types that are generated when a policy match occurs—Traffic, Threat, WildFire Submission, URL Filtering, Data Filtering, and Authentication logs—create and attach a Log Forwarding profile to each policy rule for which you want to forward logs.
   1. Select **Objects > Log Forwarding** to **Add** a profile. In the log forwarding profile match list, add each log type that you want to forward.

   If you have already turned on Enhanced Application Logs, fully enable the firewall to forward these log types by selecting **Enable enhanced application logging to Cortex Data Lake**. Notice that when you select this option, match lists that specify the logs types required for enhanced application logging are automatically added to the profile.

   2. Select **Logging Service** as the Forward Method to enable the firewalls in the device group to forward the logs to the Cortex Data Lake. You will be able to monitor the logs and generate reports from Panorama.

   3. If you haven't already done so, **Create basic security policy rules** now.

   Until the firewall has interfaces and zones and a basic security policy, it will not let any traffic through, and only traffic that matches a security policy rule will be logged (by default).

   4. For each rule you create, select **Actions** and select the Log Forwarding profile that allows the firewall to send logs to the Cortex Data Lake.
STEP 5 | **Commit** your changes.

STEP 6 | Verify that the firewall logs are being forwarded to the Cortex Data Lake.

- Log in to **Explore**, available in the Cortex hub, to view and filter Cortex Data Lake logs.
- On a firewall, enter the CLI command **show logging-status**:

```
> CMS 0
Not Sending to CMS 0

> CMS 1
Not Sending to CMS 1

>Log Collection Service

'Log Collection log forwarding agent' is active and connected to xx.xxx.xxx.xx

          config   2017/07/26 16:33:20   2017/07/26 16:34:09
> CMS 0   323                 321                        2

> CMS 1   13634645            13634637                    84831
```
### Table

<table>
<thead>
<tr>
<th>Column</th>
<th>Value 1</th>
<th>Value 2</th>
<th>Value 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>threat</td>
<td>2014/12/01 14:47:52</td>
<td>2017/07/26 16:34:24</td>
<td>93</td>
</tr>
<tr>
<td></td>
<td>557404252</td>
<td>557404169</td>
<td></td>
</tr>
<tr>
<td>traffic</td>
<td>2017/07/28 18:03:39</td>
<td>2017/07/28 18:03:50</td>
<td>1740</td>
</tr>
<tr>
<td></td>
<td>3619306590</td>
<td>3619306590</td>
<td></td>
</tr>
<tr>
<td>hipmatch</td>
<td>Not Available</td>
<td>Not Available</td>
<td>Not Available</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gtp-tunnel</td>
<td>Not Available</td>
<td>Not Available</td>
<td>Not Available</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>userid</td>
<td>Not Available</td>
<td>Not Available</td>
<td>Not Available</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>auth</td>
<td>Not Available</td>
<td>Not Available</td>
<td>Not Available</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Look for the** ‘Log collection log forwardingagent’ **is active and connected to** `<IP_Address>` **line. You can also see that CMS 0 and CMS (the Log Collectors) are not receiving logs.**

*Select the Show Status link on Device > Setup > Management > Cortex Data Lake to verify that the firewall is connected and sending logs to the Cortex Data Lake.*

### STEP 7 | Next steps:

- Use **Explore** to search, filter, and export log data. This app offers you critical visibility into your enterprise’s network activities by allowing you to easily examine network and endpoint log data.
- Use the Log Forwarding app to forward logs stored in Cortex Data Lake to a Syslog or email destination.

If you want to be able to archive the logs you send to the Cortex Data Lake for long-term storage, SOC, or internal audit directly from the Cortex Data Lake, you can use the Log Forwarding app, which is included with your Cortex Data Lake (formerly called Logging Service) license. This app enables log forwarding from the Cortex Data Lake to an external destination such as a Syslog server or an email server. Refer to the Log Forwarding App Getting Started Guide for more information. Alternatively, you continue to forward logs directly from the firewalls to your Syslog receiver.
View Cortex Data Lake Status

The Cortex Data Lake app in the Cortex hub allows you to confirm that your service is provisioned in the region you chose when you activated your auth code, and that the quota matches the storage quantity you purchased. The service status includes details on how you allocated log storage quota, the available storage space, and the number of days the logs are retained based on your incoming log rate.

STEP 1 | Sign In to the hub at https://apps.paloaltonetworks.com/.

STEP 2 | Select the Cortex Data Lake instance for which you want to view status. If you have multiple Cortex Data Lake instances, hover over the Cortex Data Lake tile and then select from the list of available instances associated with your account.

STEP 3 | Confirm the following Status details:

- Service status and the amount of storage used as a ratio of total storage you have purchased.
- Cortex Data Lake theatre where your logs are stored.
- Verify your configuration on the different log types (sources) from which the Cortex Data Lake is receiving logs, and the log storage space allocated for each logsub type.

To change the log allocation quota, Allocate Storage Based on Log Type.
# View Logs in Cortex Data Lake

In most cases, you can view logs stored in Cortex Data Lake locally on the product that is sending logs, or in Explore. The Explore app is free with Cortex Data Lake, and you should see it as listed on the Cortex hub as one of your apps after you’ve activated Cortex Data Lake. Explore provides an aggregated view of logs stored in Cortex Data Lake, and you can use Explore to search, filter, and export log data. This app offers you critical visibility into your enterprise’s network activities by allowing you to easily examine network and endpoint log data.

<table>
<thead>
<tr>
<th>Product or Service Sending Logs to Cortex Data Lake</th>
<th>Where to see the logs stored in Cortex Data Lake</th>
</tr>
</thead>
<tbody>
<tr>
<td>Palo Alto Networks Firewalls (not managed by Panorama)</td>
<td>• Use Explore to search, filter, and export firewall logs stored in Cortex Data Lake.</td>
</tr>
</tbody>
</table>
| Panorama-Managed Firewalls | • Use Explore to search, filter, and export firewall logs stored in Cortex Data Lake.  
• Use Panorama to view logs stored in Cortex Data Lake. The Panorama ACC and reports give you an aggregated view into your remote network traffic. |
| Prisma Access | • Use Explore to search, filter, and export firewall logs stored in Cortex Data Lake.  
• Use Panorama to view Prisma Access logs stored in Cortex Data Lake. The Panorama ACC and reports give you an aggregated view into your remote network and mobile user traffic. |
| Traps management service | • Use Explore to search, filter, and export firewall logs stored in Cortex Data Lake.  
• View the logs for your agents in Traps management service. |
| Cortex XDR—Analytics | • Cortex XDR™—Analytics alerts are automatically written to Cortex Data Lake as log records. Log in to Cortex XDR—Analytics to view these alerts (they are not visible in Explore). |
TCP Ports and FQDNs Required for Cortex Data Lake

If you are using a Palo Alto Networks firewall to secure traffic between Panorama, the firewalls, and the Cortex Data Lake, use the App-ID “paloalto-logging-service” in a Security policy rule to allow Panorama and the firewalls to connect to the Cortex Data Lake and forward logs on TCP 444 and 3978, the default ports for the application.

If you are using another vendor’s firewall, use the following table to identify the fully qualified domain names (FQDNs) and ports to which you must allow traffic to ensure that Panorama and the firewalls can successfully connect to the Cortex Data Lake.

<table>
<thead>
<tr>
<th>FQDNs and Ports used</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>US Region:</strong></td>
<td>Use the FQDNs that match the Cortex Data Lake region to which your firewalls and Panorama connect:</td>
</tr>
<tr>
<td>*lc.prod.us.cs.paloaltonetworks.com</td>
<td>• The firewalls use the FQDN on port 3978 and 444 to forward logs to the Cortex Data Lake.</td>
</tr>
<tr>
<td>• in.lc.prod.us.cs.paloaltonetworks.com (TCP port 3978)</td>
<td>• Panorama uses the FQDNs on port 444 to connect to the Cortex Data Lake for other log query and validity checks.</td>
</tr>
<tr>
<td>• api.lc.prod.us.cs.paloaltonetworks.com (TCP port 444)</td>
<td></td>
</tr>
<tr>
<td>• lic.lc.prod.us.cs.paloaltonetworks.com (TCP port 444)</td>
<td></td>
</tr>
<tr>
<td><strong>EU Region:</strong></td>
<td></td>
</tr>
<tr>
<td>*lc.prod.eu.cs.paloaltonetworks.com</td>
<td></td>
</tr>
<tr>
<td>• in.lc.prod.eu.cs.paloaltonetworks.com (TCP port 3978)</td>
<td></td>
</tr>
<tr>
<td>• api.lc.prod.eu.cs.paloaltonetworks.com (TCP port 444)</td>
<td></td>
</tr>
<tr>
<td>• lic.lc.prod.us.cs.paloaltonetworks.com (TCP port 444)</td>
<td>A firewall forwarding logs to a Cortex Data Lake instance in the EU connects to this US-based domain only during the onboarding process.</td>
</tr>
</tbody>
</table>

- https://api.paloaltonetworks.com (TCP port 443)
- https://apitrusted.paloaltonetworks.com (TCP port 443)
- http://ocsp.paloaltonetworks.com/
- http://crl.paloaltonetworks.com/
- http://ocsp.godaddy.com/ (TCP port 80)
- *.gpcloudservice.com (TCP port 444)

Panorama needs to access these FQDNs for the initial setup and one-time password, and for ongoing certificate revocation checks.

For OCSP, you must also allow the firewalls to access ocsp.paloaltonetworks.com on port 80.