

ONBOARD PALO ALTO CORTEX TO MANDIANT THREAT DEFENSE



To onboard or rotate credentials, ensure that you are assigned the Team Admin role within the Managed Defense Portal.

Palo Alto Cortex XDR can be integrated with Mandiant Threat Defense to monitor threats.

1. Prerequisites for Palo Alto Cortex XDR

The following prerequisites must be met before connecting your Palo Alto Cortex XDR instance to Mandiant Threat Defense:

Your Cortex subscription must have the following features:

- An active **Cortex XDR Pro license and an Event Forwarding add-on license** (<https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/Manage-Event-Forwarding>) in order to send telemetry to Google Security Operations (SecOps)
- An active cloud storage environment to receive hunting telemetry: Google Cloud Storage (preferred) or Amazon S3

2. Generate a Cortex API key

To create an Advanced Cortex API key, you must first follow the steps outlined in **Palo Alto Cortex XDR's Manage Role documentation** (<https://docs-cortex.paloaltonetworks.com/r/Cortex-XPANSE/2/Cortex-Xpanse-Expander-User-Guide/Manage-Roles>) to create a custom role. Refer to the **Create and save a new role** bullet point. Complete the subsequent numbered steps using the following settings:

- **Role Name:** Mandiant Threat Defense Orchestration
- **Description:** Allows the MTD service to perform investigation and remediation actions.
- **Components:** As outlined in the following table:

Functionality	Role Permission
File Acquisition	◦ Action Center > File Retrieval ◦ Action Center > File Search ◦ Endpoint Administrations > Retrieve Endpoint Data
Host Containment	◦ Action Center > Isolate ◦ Action Center > Quarantine ◦ Endpoint Administrations > Endpoint Management

After you have created the custom role, create an Advanced Cortex API key by following the steps outlined in **Palo Alto's Get Started with Cortex XDR APIs documentation** (<https://cortex-panw.stoplight.io/docs/cortex-xdr/3u3j0e7hcx8t1-get-started-with-cortex-xdr-ap-is>). Select an Advanced level key and the Mandiant Threat Defense Orchestration custom role.

By default, an Expiration Date is not required for the API token, but Mandiant recommends setting this to the expiration of your Mandiant Threat Defense service.

Note the following fields for onboarding:

- **Cortex API FQDN:** The unique FQDN for your Cortex environment. This typically takes the format of `UNIQUE_HOSTNAME.xdr.REGION_IDENTIFIER.paloaltonetworks.com`.
- **Cortex API Key:** A long, random string of alphanumeric characters.
- **Cortex API Key ID:** A short, numeric identifier.
- **Cortex API Key Expiration:** The date the key is set to expire.

3. Set up telemetry forwarding

There are two options for forwarding telemetry from Palo Alto Cortex XDR:

- Google Cloud Storage bucket
- Amazon S3 bucket

Google Cloud Storage bucket integration

To create a Google Cloud Storage bucket integration, follow the instructions provided in [Palo Alto's Cortex XDR Event Forwarding to Google SecOps \(Chronicle\) documentation](https://live.paloaltonetworks.com/t5/general-articles/palo-alto-cortex-xdr-event-forwarding-to-google-secops-chronicle/ta-p/600621) (<https://live.paloaltonetworks.com/t5/general-articles/palo-alto-cortex-xdr-event-forwarding-to-google-secops-chronicle/ta-p/600621>).

Amazon S3 bucket integration

To create an Amazon S3 bucket integration, see [Forward Cortex XDR logs to Amazon S3 bucket](https://docs.mandiant.com/home/mtd-forward-cortex-xdr-logs-to-amazon-s3-bucket) (<https://docs.mandiant.com/home/mtd-forward-cortex-xdr-logs-to-amazon-s3-bucket>).

4. Configure Wildfire API access

Mandiant Threat Defense requires access to the WildFire API to perform actions such as pulling malware samples and reports. Since WildFire is included with a Cortex XDR subscription, an API key must be generated so that the Mandiant Threat Defense service can perform investigations. To generate a WildFire API key for the Mandiant Threat Defense team, follow the steps outlined in the [WildFire API Reference guide](https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-api/get-started-with-the-wildfire-api/get-your-api-key) (<https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-api/get-started-with-the-wildfire-api/get-your-api-key>).

Note the following fields:

- **WildFire API Key**
- **WildFire API Expiration Date**
- **WildFire Deployment:** Cloud or Appliance

5. Configure containment

Mandiant Threat Defense offers endpoint containment for Palo Alto Networks Cortex XDR. In the Managed Defense Portal, you can configure Mandiant Threat Defense to contain any endpoints with a Palo Alto Cortex agent or a specific set of endpoints in your environment.

Tag specific endpoints

To identify specific endpoints that you want Mandiant Threat Defense to contain, you must tag those endpoints with a `MD_Containment-Allowlist` tag. Refer to the Palo Alto Networks [Manage endpoint tags \(https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-4.x-Documentation/Manage-endpoint-tags\)](https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-4.x-Documentation/Manage-endpoint-tags) documentation for instructions on creating and assigning tags to the endpoints.



The tag must be named `MD_Containment-Allowlist`; the spelling and capitalization must match exactly.

Configure containment settings

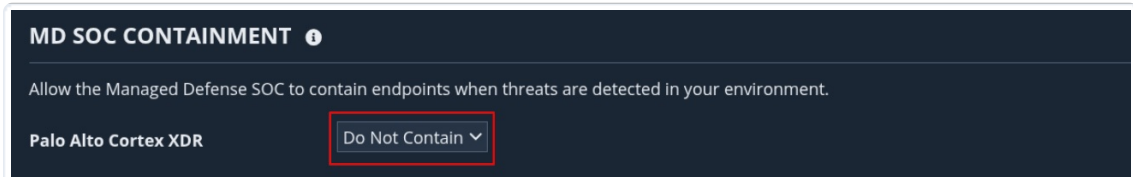
To configure endpoint containment for Palo Alto Networks Cortex XDR, use the following steps:

1. In the **Managed Defense Portal** (<https://md.mandiant.com/>), navigate to **Settings > Organization** and select the organization you want to opt in or out.



Selecting an organization is only required if your Managed Defense account has multiple organizations.

2. Make a selection for the **MD SOC Containment** Palo Alto Cortex XDR setting:
 - **Do Not Contain** (default): Mandiant Threat Defense does not contain endpoints in your environment.
 - **Specific Endpoints**: The endpoints tagged with the `MD_Containment-Allowlist` tag are contained by Mandiant Threat Defense.
 - **Any Endpoints**: Mandiant Threat Defense contains any endpoint that has a Palo Alto Cortex agent. These endpoints do not need to have a tag.



6. Connect Palo Alto Corex to MD Portal

This feature is released as a Public Preview.
Pre-GA products and features are available "as is" and might have limited support. For more information, please contact your TSC, your CSM, or go to [Support](https://docs.mandiant.com/home/mandiant-support-cases). (<https://docs.mandiant.com/home/mandiant-support-cases>)

Once you have generated your API credentials in Palo Alto Cortex XDR, follow these steps to securely onboard the integration directly within the MD Portal:

1. From the MD Portal navigation bar, click **Integrations**.
2. Click **Integrate a Technology**.
3. For the **Type**, choose **PaloAlto Cortex XDR**, and then click **Next**.
4. Fill out the required fields with the Cortex XDR credentials that you created in the previous steps:
 - **API Credentials (All Customers)**: Enter your **Cortex API FQDN**, **Cortex API Key**, **Cortex API Key ID**, and the credential **Expiration date**.



Organizations that have connected their own Google SecOps instance to the service will only see the options for providing an API client to Mandiant for orchestrations. You should configure the Cortex XDR data feeds within your SecOps instance.

5. Click **Save** to finalize the configuration. A banner appears confirming that the integration was onboarded successfully.

After saving the configuration, the integration will be in a **Provisioning** state and will not display any errors with the integration. Please give the integration until the next business day and check back to see if it is in an **Operational** state. The Service Delivery Engineering team will be in contact with you if there is an issue with recommended remediation steps.

If you encounter issues with connecting your technology to the portal, see **Troubleshoot technology onboarding for Mandiant Threat Detection** (<https://docs.mandiant.com/home/mtd-troubleshoot-technology-onboarding>).