Claroty xDome for Healthcare Integration Guide

Claroty xDome for Healthcare is a purpose-built Cyber-Physical Systems (CPS) Protection Platform that reduces cyber-risk with actionable insights across exposure management, threat detection, and network protection solutions.

Deployment Type

GreyMatter supports cloud deployments of Claroty xDome for Healthcare through port 443. If you already know your deployment method, continue to the next step. If you do not know what your Claroty xDome for Healthcare deployment method is, contact your internal Network or IT Infrastructure team to confirm.

Required Information and Setup

Collect the following information:

- URL (default is https://api.medigate.io, but see step 3 below to verify your base URL)
- API token

Obtain authentication variables

1. As an Admin user, create an API user.
    a. In the Claroty xDome for Healthcare platform, navigate to **Settings** > **System Settings** > **User Management** > **Add User** > **API User**. Under the **Role** section, select **Read & Write,** then fill out the remaining fields: Username ("GreyMatter" is recommended), Site Permissions > Create User.
2. After you've created the API user, generate a token.
    a. Navigate to **User Management** to find the API user that was just created. In the Status column, click the **Generate Token** button.
3. To obtain your base URL, navigate to the **Help Center** and select **API Documentation**. Select **Devices**, then click the "POST /api/v1/devices" option.

Note: More detailed instructions can be found in the Claroty xDome help center.

Permissions and Functionality

Permissions

Vendor Documentation

GreyMatter Capability	Action	API Authentication Permission(s)
Investigate/Hunt	PERFORM_QUERY	Read-Only role
Respond – Enrich Device Respond- Enrich Vulnerability	Enrich Device Enrich Vulnerability	Read-Only role
Detection at Source	Get Detections Update Detections	Read-Only role

Respond

PLAYBOOK NAME	REQUIRED INPUT VARIABLE(S)	EXPECTED OUTPUT RESULTS
Enrich Device	Device Name or IPv4 Address or MAC Address • Device Name example: Computer123 • IPv4 Address example: 192.0.2.1 • MAC Address example: 00:23:24:B1:2C:BB	Returns device information and any associated vulnerabilities. In the Claroty xDome console, navigate to “Devices“ > “Devices“ > “All Devices“ to view device information.
Enrich Vulnerability	CVE ID • Example: CVE-2021-40465	Returns vulnerability information and any associated devices. In the Claroty xDome console, navigate to “Risk“ > “Vulnerabilities“ > “All Vulnerabilities“ to view vulnerability information.

Investigate/Hunt

Device Alert Relations

Get details of devices with their related alerts from the database.

- Fields and query sources are static and defined by the vendor.
- If there is a bad field mapping, the entire query will fail.
- You can only use either “AND“ or “OR“ when grouping multiple filters. (See documentation)

Detection

Claroty xDome supports **Detection at Source.**
The capability pulls back Claroty xDome for Healthcare alerts.
Note and State Syncing **are** supported:

- RQ_NEW - unresolved
- RQ_IN_PROGRESS - unresolved
- RQ_ESCALATED - unresolved
- RQ_CLOSED - resolved