Cortex XSIAM Premium Documentation

1 | Broker VM data collector applets

Abstract

Learn more about the different Broker VM data collector applets available to configure.

The Broker VM has a number of data collector applets that you can configure to ingest different types of data. These data collector applets are in addition to the others that are available in the Settings → Configurations → Data Collection → Data Sources page.

1.1 | Activate Apache Kafka Collector

Abstract

Learn more about activating the Broker VM with an Apache Kafka Collector applet.

Apache Kafka is an open-source distributed event streaming platform for high-performance data pipelines, streaming analytics and data integration. Kafka records are organized into Topics. The partitions for each Topic are spread across the bootstrap servers in the Kafka cluster. The bootstrap servers are responsible for transferring data from Producers to Consumer Groups, which enable the Kafka server to save offsets of each partition in the Topic consumed by each group.

The Broker VM provides a Kafka Collector applet that enables you to monitor and collect events from Topics on self-managed on-prem Kafka clusters directly to your log repository for query and visualization purposes. The applet supports Kafka setups with no authentication, with SSL authentication, and SASL SSL authentication.

After you activate the Kafka Collector applet, you can collect events as datasets (`<Vendor>_<Product>_raw`) by defining the following.

- Kafka connection details including the Bootstrap Server List and Authentication Method.
- Topics Collection configuration for the Kafka topics that you want to collect.

> **PREREQUISITE:**
>
> - Apache Kafka version 2.5.1 and above.
> - Kafka cluster set up on premises, from which the data will be ingested.
> - Privileges to manage Broker Service configuration, such as Instance Administrator privileges.
> - Create a user in the Kafka cluster with the necessary permissions and the following authentication details:
>   - Broker Certificate and Private Key for an SSL connection.
>   - Username and Password for an SASL SSL connection.
> - Set up and configure Broker VM

1. Select Settings → Configurations → Data Broker → Broker VMs.
2. Do one of the following:
    - On the Brokers tab, find the Broker VM, and in the APPS column, left-click Add → Kafka Collector.
    - On the Clusters tab, find the Broker VM, and in the APPS column, left-click Add → Kafka Collector.
3. Configure the Kafka Connection.
    a. Specify the Bootstrap Server List, which is the `<hostname/ip>:<port>` of the bootstrap server (or servers). You can specify multiple servers, separated with a comma. For example, `hostname1:9092,1.1.1.1:9092`.

    b. Select one of the Authentication Methods:

    No Authentication

    Default connection method for a new Kafka setup, which doesn’t require authentication. With a standard Kafka setup, any user or application can write messages to any topic, as well as read data from any topic.

    SSL Authentication

    Authenticate your connection to Kafka using an SSL certificate. Use this authentication method when the connection to the Kafka server is a secure TCP, and upload the following:

    - Broker Certificate: Signed certificate used for the applet to authenticate to the Kafka server.
    - Private Key: Private key for the applet used for decrypting the SSL messages coming from the Kafka server.
    - (Optional) CA Certificate: CA certificate that was used to sign the server and private certificates. This CA certificate is also used to authenticate the Kafka server identity.

    SASL SSL (SCRAM-SHA-256)

    Authenticate your connection to the Kafka server with your Username, Password, and optionally, your CA Certificate.

    c. Test Connection to verify that you can connect to the Kafka server. An error message is displayed for each server connection test that fails.
4. Configure the Topics Collection parameters.

Topic Subscription Method

Select the Topic Subscription Method for subscribing to Kafka topics. Use List Topics to specify a list of topics. Use Regex Pattern Matching to specify a regular expression to search available topics.
Topic(s)

Specify Topic(s) from the Kafka server. For the List Topics subscription method, use a comma separated list of topics to subscribe to. For the Regex Pattern Matching subscription method, use a regular expression to match the Topic(s) to subscribe to.

(optional) Consumer Group

Specify a Consumer Group, a unique string or label that identifies the consumer group this log source belongs to. Each record that is published to a Kafka topic is delivered to one consumer instance within each subscribing consumer group. Kafka uses these labels to load balance the records over all consumer instances in a group. When specified, the Kafka collector uses the given consumer group. When not specified, Cortex XSIAM assigns the Kafka applet collector to a new automatically generated consumer group which is automatically generated for this log source with the name `PAN-<Broker VM device name>-<topic name>`.

Log Format

Select the Log Format from the list as either RAW (default), JSON, CEF, LEEF, CISCO, or CORELIGHT. This setting defines the parser used to parse all the processed event types defined in the Topics field, regardless of the file names and extension. For example, if the Topics field is set to `*` and the Log Format is JSON, all files (even those named `file.log`) in the cluster are processed by the collector as JSON, and any entry that does not comply with the JSON format are dropped.

Vendor and Product

Specify the Vendor and Product which will be associated with each entry in the dataset. The vendor and product are used to define the name of your Cortex Query Language (XQL) dataset (`<Vendor>_<Product>_raw`).

> **NOTE:**
>
> For CEF and LEEF logs, Cortex XSIAM takes the vendor and product names from the log itself, regardless of what you configure on this page.

(optional) Add Query

Click Add Query to create another Topic Collection. Each topic can be added for a server only once.

(optional) Other available options for Topic Collection

As needed, you can manage your Topic Collection settings. Here are the actions available to you.

- Edit the Topics Collection details.
- Disable/Enable a Topics Collection by hovering over the top area of the Topics Collection section, on the opposite side of the Topics Collection name, and selecting the applicable button.
- Rename a Topics Collection by hovering over the top area of the Topics Collection section, on the opposite side of the Topics Collection name, and selecting the pen icon.
- Delete a Topics Collection by hovering over the top area of the Topics Collection section, on the opposite side of the Topics Collection name, and selecting the delete icon.

5. (Optional) Click Add Connection to create another Kafka Connection for collecting data.
6. (Optional) Other available options for Connections.

   As needed, you can return to your Kafka Collector settings to manage your connections.

   Here are the actions available to you.

   - Edit the Connection details.
   - Rename a connection by hovering over the default Collection name, and selecting the edit icon to edit the text.
   - Delete a connection by hovering over the top area of the connection section, on the opposite side of the connection name, and selecting the delete icon. You can only delete a connection when you have more than one connection configured. Otherwise, this icon is not displayed.
7. Activate the Kafka Collector applet. The Activate button is enabled when all the mandatory fields are filled in.

   After a successful activation, the APPS field displays Kafka with a green dot indicating a successful connection.
8. (Optional) To view metrics about the Kafka Collector, in the Broker VMs page, left-click the Kafka connection displayed in the APPS field for your Broker VM.

   Cortex XSIAM displays Resources, including the amount of CPU, Memory, and Disk space the applet is using.
9. Manage the Kafka Collector.

   After you activate the Kafka Collector, you can make additional changes as needed. To modify a configuration, left-click the Kafka connection in the APPS column to display the

Kafka Collector settings, and select the following:

- Configure to redefine the Kafka Collector configurations.
- Deactivate to disable the Kafka Collector.

Ensure that you Save your changes, which is enabled when all mandatory fields are filled in.

You can also Ingest Apache Kafka events as datasets.

1.2 | Activate CSV Collector

Abstract

Learn more about activating the Broker VM with a CSV Collector applet.

The Broker VM provides a CSV Collector applet that enables you to monitor and collect CSV (comma-separated values) log files from a shared Windows directory directly to your log repository for query and visualization purposes. After you activate the CSV Collector applet on a Broker VM in your network, you can ingest CSV files as datasets by defining the list of folders mounted to the Broker VM and setting the list of CSV files to monitor and upload to Cortex XSIAM using a username and password.

> **PREREQUISITE:**
>
> - Set up and configure Broker VM.
> - Ensure that you share the applicable CSV files.
> - Know the complete file path for the Windows directory.

How to activate the CSV Collector

1. Select Settings → Configurations → Data Broker → Broker VMs.
2. Do one of the following:
    - On the Brokers tab, find the Broker VM, and in the APPS column, left-click Add → CSV Collector.
    - On the Clusters tab, find the Broker VM, and in the APPS column, left-click Add → CSV Collector.
3. Configure your CSV Collector by defining the list of folders mounted to the Broker VM and specifying the list of CSV files to monitor and upload to Cortex XSIAM. You must also specify a username and password.

    Mounted Folders

    Define the folders mounted onto the Broker VM:

Field	Description
Folder Path	Specify the complete file path to the Windows directory containing the shared CSV files using the format: `//host/<folder_path>`. For example, `//testenv1pc10/CSVFiles`.
Username	Specify the username for accessing the Windows directory.
Password	Specify the password for accessing the Windows directory.

After you configure the mounted folder details, Add (⊕) details to the applet.
Mounted CSV Files

Field	Description
Folder Path + Name	Select the monitored Windows directory and specify the name of the CSV file. Use a wildcard file search using these characters in the name of the directory, CSV file name, and Path Exclusion. • `?`: Matches a single char, such as `202?-report.csv`. • `*`: Matches either multiple characters, such as `2021-report*.csv`, or all CSV files with `*.csv`. • `**`: Searches all directories and subdirectories. For example, if you want to include all the CSV files in the directory and any subdirectories, use the syntax `//host/<folder_path>/**/*.csv`. **NOTE:** When you implement a wildcard file search, ensure that the CSV files share the same columns and header rows as all other logs that are collected from the CSV files to create a single dataset.

Field	Description
Path Exclusion (Optional)	Specify the complete file path for any files from the Windows directory that you do not want included. The same wildcard file search characters are allowed in this field as explained above for the FOLDER PATH +NAME field. For example, if you want to exclude any CSV file prefixed with '`exclude_`' in the directory and subdirectories of `//host/<folder_path>`, use the syntax `//host/<folder_path>/**/exclude_*.csv`.
Tags (Optional)	To easily query the CSV data in the database, you can add a tag to the collected CSV data. This tag is appended to the data using the format `<data>_<tag>`.
Target Dataset	Either select the target dataset for the CSV data or create a new dataset by specifying the name for the new dataset.

4. Activate the CSV Collector applet.

   After a successful activation, the APPS field displays CSV with a green dot indicating a successful connection.

   > **NOTE:**
   >
   > The CSV Collector checks for new CSV files every 10 minutes.

5. (Optional) To view metrics about the CSV Collector, left-click the CSV connection in the APPS field for your Broker VM.

   Cortex XSIAM displays Resources, including the amount of CPU, Memory, and Disk space the applet is using.

6. Manage the CSV Collector.

   After you activate the CSV Collector, you can make additional changes as needed. To modify a configuration, left-click the CSV connection in the APPS column to display the CSV settings, and select:

   - Configure to redefine the CSV Collector configurations.

   - Deactivate to disable the CSV Collector.

1.3 | Activate Database Collector

Abstract

Learn more about activating a Broker VM with a Database Collector applet.

The Broker VM provides a Database Collector applet that enables you to collect data from a client relational database directly to your log repository for query and visualization purposes. After you activate the Database Collector applet on a Broker VM in your network, you can collect records as datasets (`<Vendor>_<Product>_raw`) by defining the following.

- Database connection details, where the connection type can be MySQL, PostgreSQL, MSSQL, and Oracle. Cortex XSIAM uses Open Database Connectivity (ODBC) to access the databases.
- Settings related to the query details for collecting the data from the database to monitor and upload to Cortex XSIAM .

> **PREREQUISITE:**
>
> - Set up and configure Broker VM

How to activate the Database Collector

1. Select Settings → Configurations → Data Broker → Broker VMs.
2. Do one of the following:
   - On the Brokers tab, find the Broker VM, and in the APPS column, left-click Add → DB Collector.
   - On the Clusters tab, find the Broker VM, and in the APPS column, left-click Add → DB Collector.
3. Configure your Database Collector settings.

   Database Connection

Field	Description
Connection	Select the type of database connection as MySQL, PostegreSQL, MSSQL, or Oracle.
Host	Specify the hostname or IP address of the database.

Field	Description
Port	Specify the port number of the database.
Database	Specify the database name for the type of database configured. This field is relevant when configuring a Connection Type for MySQL, PostegreSQL, and MSSQL. When configuring an Oracle connection, this field is called Service Name, so you can specify the name of the service.
Enable SSL	Select whether to Enable SSL (default) to encrypt the data while in transit between the database and the Broker VM.
Username	Enter the username to access the database. The username may only contain the following characters: • Letters: `A-Z` • Digits: `0-9` • Underscore: `_` • Dollar sign: `$` • Hash sign: `#`
Password	Enter the password to access the database.
Test Connection	Select to validate the database connection.

Database Query

Field	Description
Rising Column	Specify a column for the Database Collector applet to keep track of new rows from one input execution to the next. This column must be included in the query results.
Retrieval Value	Specify a Retrieval Value for the Database Collector applet to determine which rows are new from one input execution to the next. Cortex XSIAM supports configuring this value as an integer or a string that contains a timestamp. The following string timestamp formats are supported: ISO 8601 format, RFC 2822 format, date strings with month names spelled out, such as “January 1, 2022”, date strings with abbreviated month names, such as “Jan 1, 2022", and date strings with two-digit years- MM/DD/YY. The first time the input is run, the Database Collector applet only selects those rows that contain a value higher than the value you specified in this field. Each time the input finishes running, the Database Collector applet updates the input's Retrieval Value with the value in the last row of the Rising Column.
Unique IDs (Optional)	Specify the column name(s) to match against when multiple records have the same value in the Rising Column. This column must be included in the query results. This is a comma separated field that supports multiple values. In addition, when specifying a Unique IDs, the query should use the greater than equal to sign (`>=`) in relation to the Retrieval Value. If the Unique IDs is left empty, the user should use the greater than sign (`>`).
Collect Every	Specify the execution frequency of collection by designating a number and then selecting the unit as either Seconds, Minutes, Hours, or Days.
Vendor and Product	Specify the Vendor and Product for the type of data being collected. The vendor and product are used to define the name of your Cortex Query Language (XQL) dataset (`<Vendor>_<Product>_raw`).

Field	Description
SQL Query	Specify the SQL Query to run and collect data from the database by replacing the example query provided in the editor box. The question mark (`?`) in the query is a checkpoint placeholder for the Retrieval Value. Every time the input is run, the Database Collector applet replaces the question mark with the latest checkpoint value (i.e. start value) for the Retrieval Value.
Generate Preview	Select Generate Preview to display up to 10 rows from the SQL Query and Preview the results. The Preview works based on the Database Collector settings, which means that if after running the query no results are returned, then the Preview returns no records.
Add Query (Optional)	To define another Query for data collection on the configured database connection, select Add Query. Another Query section is displayed for you to configure.

4. (Optional) Click Add Connection to define another database connection to collect data from another client relational database.

5. (Optional) Other available options.

   As needed, you can return to your Database Collector settings to manage your connections. Here are the actions available to you:

   - Edit the connection name by hovering over the default Collection name, and selecting the edit icon to edit the text.

   - Edit the query name by hovering over the default Query name, and selecting the edit icon to edit the text.

   - Disable/Enable a query by hovering over the top area of the query section, on the opposite side of the query name, and selecting the applicable button.

   - Delete a connection by hovering over the top area of the connection section, on the opposite side of the connection name, and selecting the delete icon. You can only delete a connection when you have more than one connection configured. Otherwise, this icon is not displayed.

   - Delete a query by hovering over the top area of the query section, on the opposite side of the query name, and selecting the delete icon. You can only delete a query when you have more than one query configured. Otherwise, this icon is not displayed.

6. Activate the Database Collector applet.

   After a successful activation, the APPS field displays DB with a green dot indicating a successful connection.

7. (Optional) To view metrics about the Database Collector, left-click the DB connection in the APPS field for your Broker VM.

   Cortex XSIAM displays Resources, including the amount of CPU, Memory, and Disk space the applet is using.

8. Manage the Database Collector.

   After you activate the Database Collector, you can make additional changes as needed. To modify a configuration, left-click the DB connection in the APPS column to display the Database Collector settings, and select:

   - Configure to redefine the Database Collector configurations.

   - Deactivate to disable the Database Collector.

1.4 | Activate Files and Folders Collector

Abstract

Learn more about activating a Broker VM with a Files and Folders Collector applet.

The Broker VM provides a Files and Folders Collector applet that enables you to monitor and collect logs from files and folders in a network share for a Windows or Linux directory, directly to your log repository for query and visualization purposes. The Files and Folders collector applet only starts to collect files that are more than 256 bytes and is only supported with a Network File System version 4 (NFSv4). After you activate the Files and Folders Collector applet, you can collect files as datasets (`<Vendor>_<Product>_raw`) by defining the following.

- Details of the folder path on the network share containing the files that you want to monitor and upload to Cortex XSIAM.

- Settings related to the list of files to monitor and upload to Cortex XSIAM, where the log format is either Raw (default), JSON, CSV, TSV, PSV, CEF, LEEF, Corelight, or Cisco.

> **NOTE:**
>
> Cortex XSIAM only supports ingestion of files encoded in UTF-8 format.

> **PREREQUISITE:**

> - Set up and configure Broker VM.
> - Know the complete path to the files and folders that you want Cortex XSIAM to monitor.
> - Ensure that the user permissions for the network share include the ability to rename and delete files in the folder that you want to configure collection.

How to activate the Files and Folders Collector

1. Select Settings → Configurations → Data Broker → Broker VMs.
2. Do one of the following:
   - On the Brokers tab, find the Broker VM, and in the APPS column, left-click Add → Files and Folder Collector.
   - On the Clusters tab, find the Broker VM, and in the APPS column, left-click Add → Files and Folder Collector.
3. Configure the Files and Folder Collector settings.

   Shared Folder Connection

Field	**Description**
Folder Path	Specify the path to the files and folders that you want Cortex XSIAM to monitor continuously to collect the files. The following formats are available based on the type of machine you are using: • Windows: `\\<hostname>\<shared_folder>` or `smb://<hostname>/<shared_folder>` • Linux: `/<srv>/<shared_folder>` or `nfs://<srv>/<shared_folder>` **NOTE:** When using the Linux file share, including the Linux share with nfs, a Username and Password is not required, so these fields are grayed out in the screen.
Recursive	Select this checkbox to configure the Files and Folders Collector applet to recursively examine any subfolders for new files as long as the folders are readable. This is not configured by default.

Field	Description
Username	Specify the username to access the shared resource using a User Principal Name (UPN) format.
Password	Specify the password to access the shared resource.
Test Connection	Select to validate the connection and permissions.

File and Folder Settings

Field	Description
Mode	Select the mode to use for collecting data. The settings displayed change depending on your selection. • Tail: Continuously monitors the files for new data (default). The collector adds the new data from the files to the dataset. • Batch: Reads the files automatically at user determined intervals, updates the lookup datasets, and then renames or deletes the uploaded source files. Renaming or deleting the read source files ensures that the collector always reads the most up-to-date file. Depending on the Storage Method, the collector can Append the new data from the files to the dataset or completely Replace the data in the dataset. **NOTE:** In Batch mode, the Files and Folders Collector supports collecting logs from a network share for a maximum file size of 500 MB.
Collect Every	This option is only displayed in Batch Mode. Specify the execution frequency of collection by designating a number and then selecting the unit as either Minutes, Hours, or Days.

Field	Description
After Files Uploaded	This option is only displayed in Batch Mode. Select what to do with the files after they are uploaded to the Cortex XSIAM server. You can Rename files with a suffix (default) or you can Delete files. When renaming, the suffix is added to the end of the original file name using the format `<file name>.<suffix>`, which becomes the new name of the file.
Include	Specify the files and folders that must match to be monitored by Cortex XSIAM. Multiple values are allowed with commas separating the values and are case-sensitive. Allowed wildcard: • '?' matches a single alphabet character in a specific position. • '*' matches any character or set of characters, including no character. Example 130. `log*.jsonlog*.json` includes any JSON file starting with 'log'.
Exclude (Optional)	Specify the files and folders that must match to not be monitored by Cortex XSIAM . Multiple values are allowed with commas separating the values. Allowed wildcard: • '?' matches a single alphabet character in a specific position. • '*' matches any character or set of characters, including no character. Example 131. `*.backup` excludes any file ending with '.backup'.

Field	Description
Log Format	Select the Log Format from the list as either Raw (default), JSON, CSV, TSV, PSV, CEF, LEEF, Corelight, or Cisco. This setting defines the parser used to parse all the processed files as defined in the Include and Exclude fields, regardless of the file names and extension. For example, if the Include field is set `*` and the Log Format is JSON, all files (even those named `file.log`) in the specified folder are processed by the Files and Folders Collector as JSON, and any entry that does not comply with the JSON format are dropped. **NOTE:** When uploading JSON files, Cortex XSIAM only parses the first level of nesting and only supports single line JSON format, such that every new line means a separate entry.
# of Lines to Skip (Optional)	Specify the number of lines to skip at the beginning of the file. This is set to 0 by default. **NOTE:** Use this option only in cases where your files contain some sort of "header" lines, such as a general description, an introduction, a disclaimer, or similar, and you want to skip ingesting them. The Lines to Skip are not part of the file format. For example, in CSV files, there is no need to skip lines.

Data Source Mapping

Field	Description
Storage Method	This option is only displayed in Batch Mode. Specify whether to Append the read data to the dataset, or to Replace all the data in the dataset with the newly read data. • Append: This mode is useful for log files where you want to keep all the log info from before. • Replace: This mode is useful for adding inventory data from CSV and JSON files which include properties, for example, a list of machines, a list of users, or a mapping of endpoints to users to create a lookup dataset. In each data collection cycle, the new data completely replaces the existing data in the dataset. You can use the records from the lookup datasets for correlation and enrichment through parsing rules, correlation rules, and queries. **NOTE:** ◦ When the storing method is Replace, the maximum size for the total data to be imported into a lookup dataset is 30 MB each time the data is fetched. ◦ The inventory data ingested using the Files and Folders collector is counted towards license utilization. ◦ When you use a JOINT function with a lookup table in a query or correlation rule, make sure you configure the conflict strategy to point to the raw dataset. This ensures that the system fields are taken from the raw dataset and not from the lookup table.

Field	Description
Target Dataset	This option is only displayed in Batch Mode when the storing method is Replace. Select the name of an existing Lookup dataset or create a new Lookup dataset by specifying the name. When you create a new target dataset name, specify a name that will be more meaningful for your users when they query the dataset. For example, if the original file name is `accssusr.csv`, you can save the dataset as `access_per_users`. Dataset names can contain special characters from different languages, numbers (`0-9`) and underscores (_). You can create dataset names using uppercase characters, but in queries, dataset names are always treated as if they are lowercase. **NOTE:** • You can't specify a file name that's the same as a system file name. • The name of a dataset created from a *tsv* file must always include the extension. If the original file name is mrkdptusrsnov23.tsv, you can name save the dataset with the name marketing_dept_users_Nov_2023.tsv.
Vendor and Product	Specify the Vendor and Product for the type of data being collected. The vendor and product are used to define the name of your Cortex Query Language (XQL) dataset (`<Vendor>_<Product>_raw`). **NOTE:** The Vendor and Product defaults to Auto-Detect when the Log Format is set to CEF or LEEF.

Generate Preview

Select Generate Preview to display up to 10 rows from the first file and Preview the results. The Preview works based on the Files and Folders Collector settings, which means that if all the files that were configured to be monitored were already processed, then the Preview returns no records.

4. (Optional) Click Add Connection to define another Files and Folders connection for collecting logs from files and folders in a shared resource.

5. (Optional) Other available options.

As needed, you can return to your Files and Folders Collector settings to manage your connections. Here are the actions available to you:

- Edit the connection name by hovering over the default Collection name, and selecting the edit icon to edit the text.
- Disable/Enable a connection by hovering over the top area of the connection section, on the opposite side of the connection name, and selecting the applicable button.
- Delete a connection by hovering over the top area of the connection section, on the opposite side of the connection name, and selecting the delete icon. You can only delete a connection when you have more than one connection configured. Otherwise, this icon is not displayed.

6. Activate the Files and Folders Collector applet.

   After a successful activation, the APPS field displays File with a green dot indicating a successful connection.

7. (Optional) To view metrics about the Files and Folders, left-click the File connection in the APPS field for your Broker VM.

   Cortex XSIAM displays Resources, including the amount of CPU, Memory, and Disk space the applet is using.

8. Manage the Files and Folders Collector.

   After you activate the Files and Folders Collector, you can make additional changes as needed. To modify a configuration, left-click the File connection in the APPS column to display the Files and Folder Collector settings, and select:

   - Configure to redefine the Files and Folders Collector configurations.
   - Deactivate to disable the Files and Folders Collector.

1.5 | Activate NetFlow Collector

Abstract

Learn more about activating a Broker VM with a NetflFlow Collector applet.

To receive NetFlow flow records from an external source, you must first set up the NetFlow Collector applet on a Broker VM within your network. NetFlow versions 5, 9, and IPFIX are supported.

To increase the log ingestion rate, you can add additional CPUs to the Broker VM. The NetFlow Collector listens for flow records on specific ports either from any, or from specific IP addresses.

After the NetFlow Collector is activated, the NetFlow Exporter sends flow records to the NetFlow Collector, which receives, stores, and pre-processes that data for later analysis.

Performance Requirements

The following setups are required to meet your performance needs:

- 4 CPUs for up to 50K flows per second (FPS).
- 8 CPUs for up to 100K FPS.

> **NOTE:**
>
> Since multiple network devices can send data to a single NetFlow Collector, we recommend that you configure a maximum of 50 NetFlow Collectors per Broker VM applet, with a maximum aggregated rate of approximately 50K flows per second (FPS) to maintain system performance.

> **PREREQUISITE:**
>
> Set up and configure Broker VM

How to activate the NetFlow Collector

1. Select Settings → Configurations → Data Broker → Broker VMs.
2. Do one of the following:
   - On the Brokers tab, find the Broker VM, and in the APPS column, left-click Add → NetFlow Collector.
   - On the Clusters tab, find the Broker VM, and in the APPS column, left-click Add → NetFlow Collector.
3. Click +Add New.
4. Configure your NetFlow Collector.

   General Settings

   Specify the number of the UDP Port on which the NetFlow Collector listens for flow records (default 2055).

   This port number must match the UDP port number in the NetFlow exporter device. The rules for each port are evaluated, line by line, on a first match basis. Cortex XSIAM discards logs for non-configured flow records without an “Any” rule.

   > **NOTE:**
   >
   > Since Cortex XSIAM reserves some port numbers, it is best to select a port number that is not in the range of 0-1024 (except for 514), in the range of 63000-65000 or has one of the following values: 4369, 5671, 5672, 5986, 6379, 8000, 8888, 9100, 15672, or 28672.

   Custom Settings

Field	Description
Source Network	Specify the IP address or a Classless Inter-Domain Routing (CIDR) of the source network device that sends the flow records to Cortex XSIAM . Leave the field empty to receive data from any device on the specified port (default). If you do not specify an IP address or a CIDR, Cortex XSIAM can receive data from any source IP address or CIDR that transmits via the specified port. If IP addresses overlap in multiple rows in the Source Network field, such as 10.0.0.10 in the first row and 10.0.0.0/24 in the second row, the NetFlow Collector captures the IP address in the first row.
Vendor and Product	Specify a particular vendor and product to be associated with each dataset entry or leave the default IP Flow setting. The Vendor and Product values are used to define the name of your Cortex Query Language (XQL) dataset `<Vendor>_<Product>_raw`. If you do not define a vendor or product, Cortex XSIAM uses the default values with the resulting dataset name `ip_flow_ip_flow_raw`. Consider changing the default values in order to uniquely identify the source network device. After each configuration, select ↵ to save your changes and then select Done to update the NetFlow Collector with your settings.

5. (Optional) Make additional changes to the NetFlow Collector data sources.

- You can make additional changes to the Port by right-clicking the applicable UDP port and selecting the following:
  - Edit: To change the UDP Port, Source Network, Vendor, or Product defined.
  - Remove: To delete a Port.
- You can make additional changes to the Source Network by right-clicking on the Source Network value.

  > **NOTE:**
  >
  > The options available change, according to the set Source Network value.

Option	Description
Edit	To change the UDP Port, Source Network, Vendor, or Product defined.
Remove	To delete a Port.
Copy entire row	To copy the Source Network, Product, and Vendor information.
Open IP View	To view network operations and to view any open cases on this IP within a defined period. This option is only available when the Source Network value is a specific IP address or CIDR.
Open in Quick Launcher	To search for information using the Quick Launcher shortcut . This option is only available when the Source Network value is a specific IP address or CIDR.

- To prioritize the order of the NetFlow formats listed for the configured data source, drag and drop the rows to change their order.

6. Activate the NetFlow collector applet.

   After successful activation, the APPS field displays NetFlow with a green dot indicating a successful connection.

7. (Optional) To view NetFlow Collector metrics, left-click the NetFlow connection in the APPS field for your Broker VM.

   Cortex XSIAM displays the following information:

Option	Description
Connectivity Status	Whether the applet is connected to Cortex XSIAM.
Logs Received and Logs Sent	Number of logs that the applet received and sent per second over the last 24 hours. If there are more logs received than sent, this can indicate a connectivity issue.
Resources	Displays the amount of CPU, Memory, and Disk space the applet uses.

8. Manage the NetFlow Collector.

   After you activate the NetFlow Collector, you can make additional changes. To modify a configuration, left-click the NetFlow connection in the APPS column to display the NetFlow Collector settings, and select:

   - Configure to redefine the NetFlow Collector configurations.
   - Deactivate to disable the NetFlow Collector.

   You can also Ingest NetFlow flow records as datasets.

1.6 | Activate Network Mapper

Abstract

Learn more about activating the Network Mapper to scan your network.

> **PREREQUISITE:**
>
> After you have configured and registered your Broker VM, you can choose to activate the Network Mapper application.

The Network Mapper allows you to scan your network to detect and identify unmanaged hosts in your environment according to defined IP address ranges. The Network Mapper configurations are used to locate unmanaged assets that appear in the Assets table. For more information, see Existing Asset Inventory.

1. Select Settings → Configurations → Data Broker → Broker VMs.
2. Do one of the following:
    - On the Brokers tab, find the Broker VM, and in the APPS column, left-click Add → Network Mapper.
    - On the Clusters tab, find the Broker VM, and in the APPS column, left-click Add → Network Mapper.
3. In the Activate Network Mapper window, define the following parameters:

Field	**Description**
Scan Method	Select the either ICMP echo or TCP SYN scan method to identify your network hosts. When selecting TCP SYN you can enter single ports and ranges together, for example `80-83, 443`.
Scan Requests per Second	Define the maximum number of scan requests you want to send on your network per second. By default, the number of scan requests are defined as 1000. **NOTE:** Each IP address range can receive multiple scan requests based on it's availability.
Scanning Scheduler	Define when you want to run the network mapper scan. You can select either daily, weekly, or monthly at a specific time.
Scanned Ranges	Select from the list of exiting IP address ranges to scan. Make sure to ↵ after each selection. **NOTE:** IP address ranges are displayed according to what you defined as your Network Parameters.

4. Activate the applet.

After a successful activation, the APPS field displays Network Mapper with a green dot indicating a successful connection.

5. In the APPS field, left-click the Network Mapper connection to view the following scan and applet metrics:

   Scan Details

Field	Description
Connectivity Status	Whether the applet is connected to Cortex XSIAM .
Scan Status	State of the scan.
Scan Start Time	Timestamp of when the scan started.
Scan Duration	Period of time in minutes and seconds the scan is running.
Scan Progress	How much of the scan has been completed in percentage and IP address ratio.
Detected Hosts	Number of hosts identified from within the IP address ranges.
Scan Rate	Number of IP addresses scanned per second.

   Applet Metrics

   Resources: Displays the amount of CPU, Memory, and Disk space the applet is using.

6. Manage the Network Mapper.

   After the network mapper has been activated, left-click the Network Mapper connection in the APPS column to display the Network Mapper settings, and select:

- Configure to redefine the network mapper configurations.
- Scan Now to initiate a scan.
- Deactivate to disable the network mapper.

1.7 | Activate Syslog Collector

Abstract

Learn how to set up and activate the Syslog Collector applet on a Broker VM within your network.

To receive Syslog data from an external source, you must first set up the Syslog Collector applet on a Broker VM within your network. The Syslog Collector supports a log ingestion rate of 90,000 logs per second (lps) with the recommended Broker VM setup.

The Syslog collector supports TCP/Secure TCP/UDP. The RFC 6587 standard, which specifies the transmission of syslog messages over TCP, is supported by the Syslog collector. When syslog messages are transmitted over TCP, there are two options:

- Octet Framing
- Non-Transparent-Framing

  This is the most commonly used option. The Syslog collector supports the newline character `\n` (Hex 0x0A) as the end-of-line delimiter for syslog messages.

To increase the log ingestion rate, you can add additional CPUs to the Broker VM. The Syslog Collector listens for logs on specific ports and from any or specific IP addresses. A Syslog Collector configuration supports up to 100 ports.

> **PREREQUISITE:**
>
> Set up and configure Broker VM

Perform the following procedures in the order listed below.

Task 1. Add a Syslog Collector

1. Select Settings → Configurations → Data Broker → Broker VMs.
2. Do one of the following:
   - On the Brokers tab, find the Broker VM, and in the APPS column, left-click Add → Syslog Collector.
   - On the Clusters tab, find the Broker VM, and in the APPS column, left-click Add → Syslog Collector.

Task 2. Configure the Syslog Collector

Cortex XSIAM supports multiple sources over a single port on a single Syslog Collector. The following options are available:

- Edit the Optional Settings of the default PORT/PROTOCOL: 514/UDP. See Task 3.

  > **NOTE:**
  >
  > Once configured, you cannot change the Port/PROTOCOL. If you don’t want to use a data source, ensure to remove the data source from the list as explained in **Task 5**.

- Add a new Syslog Collector data source. See Task 4.

Task 3. Edit the default 514/UDP Syslog Collector data source

1. Right-click the 514/UDP PORT/PROTOCOL, and select Edit.
2. Configure these Optional Settings:

Field	Description
Format	Select the Syslog format you want to send to the UDP 514 protocol and port on the Syslog Collector: Auto-Detect (default), CEF, LEEF, CISCO, CORELIGHT, or RAW. **NOTE:** • The Vendor and Product defaults to Auto-Detect when the Log Format is set to CEF or LEEF. • For a Log Format set to CEF or LEEF, Cortex XSIAM reads events row by row to look for the Vendor and Product configured in the logs. When the values are populated in the event log row, Cortex XSIAM uses these values even if you specified a value in the Vendor and Product fields in the Syslog Collector settings. Yet, when the values are blank in the event log row, Cortex XSIAM uses the Vendor and Product that you specified in the Syslog Collector settings. If you did not specify a Vendor or Product in the Syslog Collector settings and the values are blank in the event log row, the values for both fields are set to unknown.
Vendor and Product	Specify a particular vendor and product for the Syslog format defined or leave the default Auto-Detect setting.

Field	Description
Source Network	Specify the IP address or Classless Inter-Domain Routing (CIDR). If you leave this blank, Cortex XSIAM will allow receipt of logs from any source IP address or CIDR that transmits over the specified protocol and port. When you specify overlapping addresses in the Source Network field in multiple rows, such as 10.0.0.10 in the first row and 10.0.0.0/24 in the second row, the order of the addresses matter. In this example, the IP address 10.0.0.10 is only captured from the first row definition. For more information on prioritizing the order of the syslog formats, see Task 5.

After each configuration, select ↵ to save the changes and then Done to update the Syslog Collector with your settings.

Task 4. Add a new Syslog Collector data source

1. Select Add New.
2. Configure these mandatory General settings:

   Protocol

   Choose a protocol over which the Syslog will be sent: UDP, TCP, or Secure TCP.

   When configuring the Protocol as Secure TCP, these additional General Settings are available:

   - Server Certificate: Browse to your server certificate to configure server authentication.
   - Private Key: Browse to your private key for the server certificate.
   - Optional CA Certificate: (Optional) Browse to your CA certificate for mutual authentication.

     The log forwarder (for example, a firewall) authenticates the Broker VM by default. The Broker VM does not authenticate the log forwarder by default, but you can use this option to set set up such authentication. If you use this option, ensure that you have a client certificate on the log forwarding side that matches the CA certificate on the Broker VM side.
   - Minimal TLS Version: Select either 1.0 or 1.2 (default) as the minimum TLS version allowed.

> **NOTE:**

> - The server certificate and private key pair is expected in a PEM format.
>
> - Cortex XSIAM will notify you when your certificates are about to expire.

Port

Choose a port on which the Syslog Collector will listen for logs. A Syslog Collector configuration supports up to 100 ports.

> **NOTE:**
>
> Because some port numbers are reserved by Cortex XSIAM , you must choose a port number that is not:
>
> - In the range of 0-1024 (except for 514)
>
> - In the range of 63000-65000
>
> - Values of 4369, 5671, 5672, 5986, 6379, 8000, 8888, 9100, 15672, or 28672

3. Configure these Optional Settings:

Field	Description
Format	Select the Syslog format you want to send to the UDP/514 protocol and port on the Syslog Collector: Auto-Detect (default), CEF, LEEF, CISCO, CORELIGHT, or RAW.
Vendor and Product	Enter a particular vendor and product for the Syslog format defined or leave the default Auto-Detect setting.
Source Network	Specify the IP address or Classless Inter-Domain Routing (CIDR). If you leave this blank, Cortex XSIAM will allow receipt of logs from any source IP address or CIDR that transmits over the specified protocol and port. When you specify overlapping addresses in the Source Network field in multiple rows, such as 10.0.0.10 in the first row and 10.0.0.0/24 in the second row, the order of the addresses matter. In this example, the IP address 10.0.0.10 is only captured from the first row definition. For more information on prioritizing the order of the syslog formats, see Task 5.

After each configuration, select ↵ to save the changes and then Done to update the Syslog Collector with your settings.

Task 5. Make additional changes to the Syslog Collector data sources configured

- To remove a Syslog Collector data source, right-click the row after the Port/Protocol entry, and select Remove.
- To prioritize the order of the Syslog formats listed for the protocols and ports configured, drag and drop the rows to the order you require.

Task 6. Save the Syslog Collector settings

Click Save. After a successful activation, the APPS field displays Syslog with a green dot indicating a successful connection.

Task 7. (optional) View metrics about the Syslog Collector

To view metrics about the Syslog Collector, left-click the Syslog connection in the APPS field for your Broker VM. Cortex XSIAM displays the following information:

Metric	Description
Connectivity Status	Whether the applet is connected to Cortex XSIAM.
Logs Received and Logs Sent	Number of logs received and sent by the applet per second over the last 24 hours. If the number of incoming logs received is larger than the number of logs sent, it could indicate a connectivity issue.
Resources	Displays the amount of CPU, Memory, and Disk space the applet is using.

Step 8. Manage the Syslog Collector

After the Syslog Collector has been activated, you can make additional changes to your configuration if needed. To modify a configuration, left-click the Syslog connection in the APPS column to display the Syslog Collector settings, and select:

- Configure to redefine the Syslog configurations.
- Deactivate to disable the Syslog Collector.

1.8 | Activate Windows Event Collector

Abstract

Set up your Windows Event Collector to connect with the Cortex XSIAM Broker VM and collect events.

After you have configured and registered your Broker VM, activate your Windows Event Collector application.

The Windows Event Collector (WEC) runs on the Broker VM collecting event logs from Windows Servers, including Domain Controllers (DCs). The Windows Event Collector can be deployed in multiple setups, and can be connected directly to multiple event generators (DCs or Windows Servers) or routed using one or more Windows Event Collectors. Behind each Windows event collector there may be multiple generating sources.

To enable the collection of the event logs, you need to configure and establish trust between the Windows Event Forwarding (WEF) collectors and the WEC. Establishing trust between the WEFs and the WEC is achieved by mutual authentication over TLS using server and client certificates. The WEF, a WinRM plugin, runs under the Network Service account. Therefore, you need to provide the WEFs with the relevant certificates and grant the account access permissions to the private key used for client authentication, for example, authenticate with WEC.

> **NOTE:**
>
> You can also activate the Windows Event Collector on Windows Core. For more information, see Activate Windows Event Collector on Windows Core.

> **PREREQUISITE:**
>
> - Set up and configure Broker VM
> - Broker VM version 8.0 and later
> - You have knowledge of Windows Active Directory and Domain Controllers.
> - You must configure different settings related to the FQDN where the instructions differ depending on whether you are configuring a standalone Broker VM or High Availability (HA) cluster.
>
>   Standalone broker
>
>   A FQDN must be configured for the standalone broker as configured in your local DNS server. Therefore, the Broker VM is registered in the DNS, its FQDN is resolvable from the events forwarder (Windows server), and the Broker VM FQDN is configured. For more information, see Configure High Availability Cluster.
>
>   HA cluster
>
>   A FQDN must be configured in the cluster settings as configured in your local DNS server, which points to a Load Balancer. For more information, see Configure High Availability Cluster.
> - Windows Server 2012 r2 or later.

After ingestion, Cortex XSIAM normalizes and saves the Windows event logs in the dataset `xdr_data`. The normalized logs are also saved in a unified format in `microsoft_windows_raw`. This enables you to search the data using Cortex Query Language (XQL) queries, build correlation rules, and generate dashboards based on the data.

Perform the following procedures in the order listed below.

Task 1. Add, configure, and activate a Windows Event Collector

1. Select Settings → Configurations → Data Broker → Broker VMs.
2. Do one of the following:
   - On the Brokers tab, find the Broker VM, and in the APPS column, left-click Add → Windows Event Collector.
   - On the Clusters tab, find the Broker VM, and in the APPS column, left-click Add → Windows Event Collector.
3. In the Activate Windows Event Collector window, define the Collected Events to configure the events collected by the applet. This lists event sources from which you want to collect events.

Field	Description
Source	Select from the pre-populated list with the most common event sources on Windows Servers. The event source is the name of the software that logs the events. A source provider can only appear once in your list. When selecting event sources, depending on the type event you want to forward, ensure the event source is enabled, for example auditing security events. If the source is not enabled, the source configuration in the given row will fail.
Min. Event Level	Minimum severity level of events that are collected.
Event IDs Group	Whether to Include, Exclude, or collect All event ID groups.

Field	Description
Minimal TLS Version	Select either 1.0 or 1.2 (default) as the minimum TLS version allowed. Ensure that you verify that all Windows event forwarders are supporting the minimal defined TLS version.

Example 134.

To forward all the Windows Event Collector events to the Broker VM, define as follows:

- Source: `ForwardedEvents`
- Min. Event Level: `Verbose`
- Event IDs Group: `All`

> **NOTE:**
>
> By default, Cortex XSIAM collects Palo Alto Networks predefined Security events that are used by the Cortex XSIAM detectors. Removing the Security collector interferes with the Cortex XSIAM detection functionality. Restore to Default to reinstate the Security event collection.

4. Click Activate. After a successful activation, the APPS field displays WEC with a green dot indicating a successful connection.

Task 2. Configure the Windows Event Collector settings

1. In the APPS column, left-click the WEC connection to display the Windows Event Collector settings, and select Configure.
2. In the Windows Event Forwarder Configuration window, perform the following tasks:
    a. In the Subscription Manager URL field, click 📋 (copy) . This will be used when you configure the subscription manager in the GPO (Global Policy Object) on your domain controller.

    b. Enter a password in the Define Client Certificate Export Password field to be used to secure the downloaded WEF certificate that establishes the connection between your DC/WEF and the WEC. You will need this password when the certificate is imported to the events forwarder.

    c. Download the WEF certificate in a PFX format to your local machine.

    To view your Windows Event Forwarding configuration details at any time, select your Broker VM, right-click and navigate to Windows Event Collector → Configure.

Cortex XSIAM monitors the certificate and triggers a Certificate Expiration notification 30 days prior to the expiration date. The notification is sent daily specifying the number of days left on the certificate, or if the certificate has already expired.

Task 3. Install your WEF Certificate on the WEF to establish connection

> **NOTE:**
>
> You must install the WEF certificate on every Windows Server, whether DC or not, for the WEFs that are supposed to forward logs to the Windows Event Collector applet on the Broker VM.

1. Locate the PFX file you downloaded from the Cortex XSIAM console and double-click to open the Certificate Import Wizard.

2. In the Certificate Import Wizard:

   a. Select Local Machine, and then click Next.

   b. Verify the File name field displays the PFX certificate file you downloaded and click Next.

   c. In the Passwords field, specify the Client Certificate Export Password you defined in the Cortex XSIAM console followed by Next.

   d. Select Automatically select the certificate store based on the type of certificate, and then click Next and Finish.

3. From a command prompt, run `certlm.msc`.

4. In the file explorer, navigate to Certificates and verify the following for each of the folders:

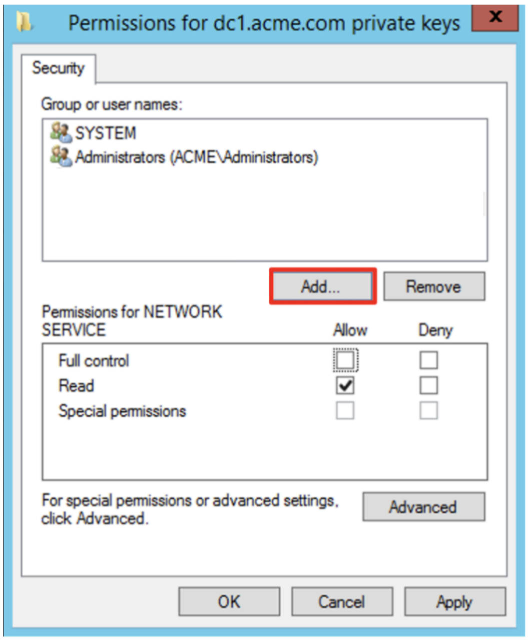
   - In the Personal → Certificates folder, ensure the certificate `forwarder.wec.paloaltonetworks.com` is displayed.

   - In the Trusted Root Certification Authorities → Certificates folder, ensure the CA `ca.wec.paloaltonetworks.com` is displayed.

5. Navigate to Certificates Personal Certificates.

6. Right-click the certificate and navigate to All tasks → Manage Private Keys.

7. In the Permissions window, select Add and in the Enter the object name section, enter `NETWORK SERVICE`, and then click Check Names to verify the object name. The object name is displayed with an underline when valid. and then click OK.



Permissions for dc1.acme.com private keys

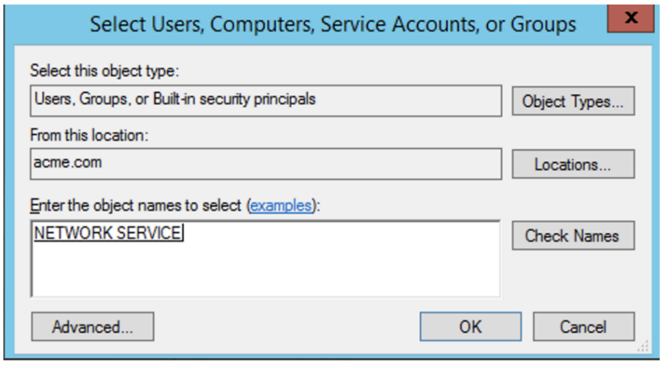
Group or user names:

SYSTEM
Administrators (ACME\Administrators)

Permissions for NETWORK SERVICE

	Allow	Deny
Full control	□	□
Read	☑	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced.



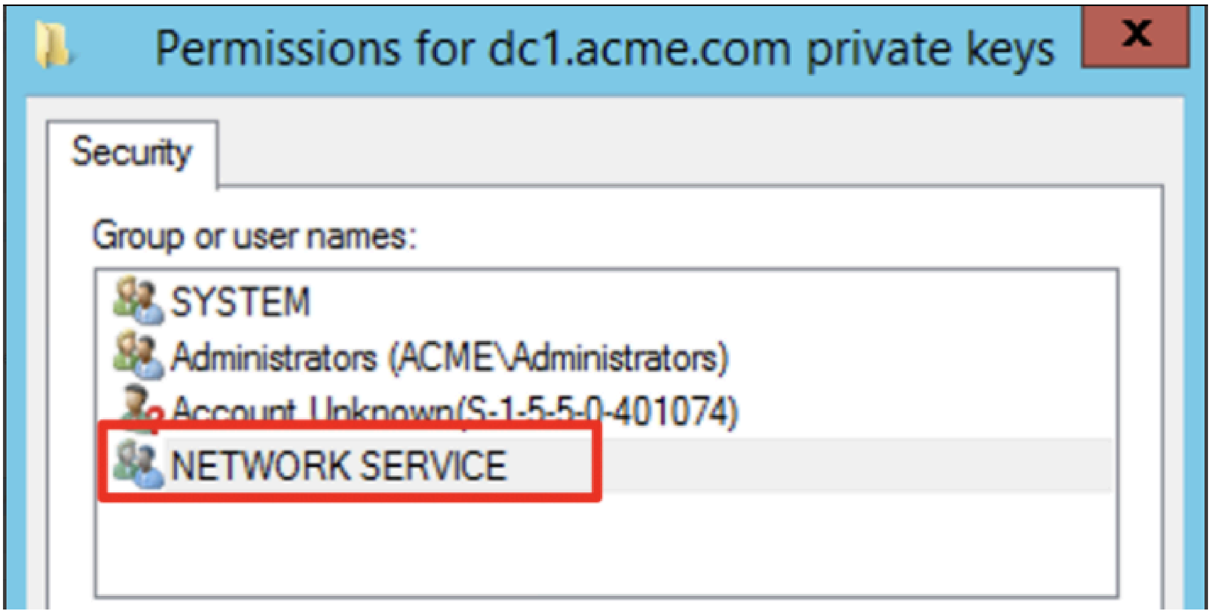
Select Users, Computers, Service Accounts, or Groups

Select this object type: Users, Groups, or Built-in security principals

From this location: acme.com

Enter the object names to select (examples): NETWORK SERVICE

8. Click OK, verify the Group or user names that are displayed, and then click Apply Permissions for private keys.



Permissions for dc1.acme.com private keys

Group or user names:

SYSTEM
Administrators (ACME\Administrators)
Account Unknown(S-1-5-5-0-401074)
NETWORK SERVICE

Task 4. Add the Network Service account to the domain controller Event Log Readers group.

> **NOTE:**
>
> You must install the WEF certificate on every Windows Server, whether DC or not, for the WEFs that are supposed to forward logs to the Windows Event Collector applet on the Broker VM.

1. To enable events forwarders to forward events, the Network Service account must be a member of the Active Directory Event Log Readers group. In PowerShell, execute the following command on the domain controller that is acting as the event forwarder:

```
PS C:\> net localgroup "Event Log Readers" "NT Authority\Network Service" /add
```

Make sure you see `The command completed successfully` message.

2. Grant access to view the security event logs.

    a. Run `wevtutil gl security` and take note of your `channelAccess` value.

    Example 135.

    ```
    `PS C:\Users\Administrator> wevtutil gl security
    name: security
    enabled: true
    type: Admin
    owningPublisher:
    isolation: Custom
    channelAccess: O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)
    logging:
      logFileName: %SystemRoot%\System32\Winevt\Logs\security.evtx
      retention: false
      autoBackup: false
      maxSize: 134217728
    publishing:
      fileMax: 1
    ```

    Take note of value: `channelAccess: O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)`

    b. Run `wevtutil sl security "/ca:<channelAccess value>(A;;0x1;;;S-1-5-20)"`

    Example 136.

    ```
    PS C:\Users\Administrator> wevtutil sl security "/ca:O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)
    (A;;0x1;;;S-1-5-32-573)(A;;0x1;;;S-1-5-20)"
    ```

    Make sure you grant access on each of your domain controller hosts.

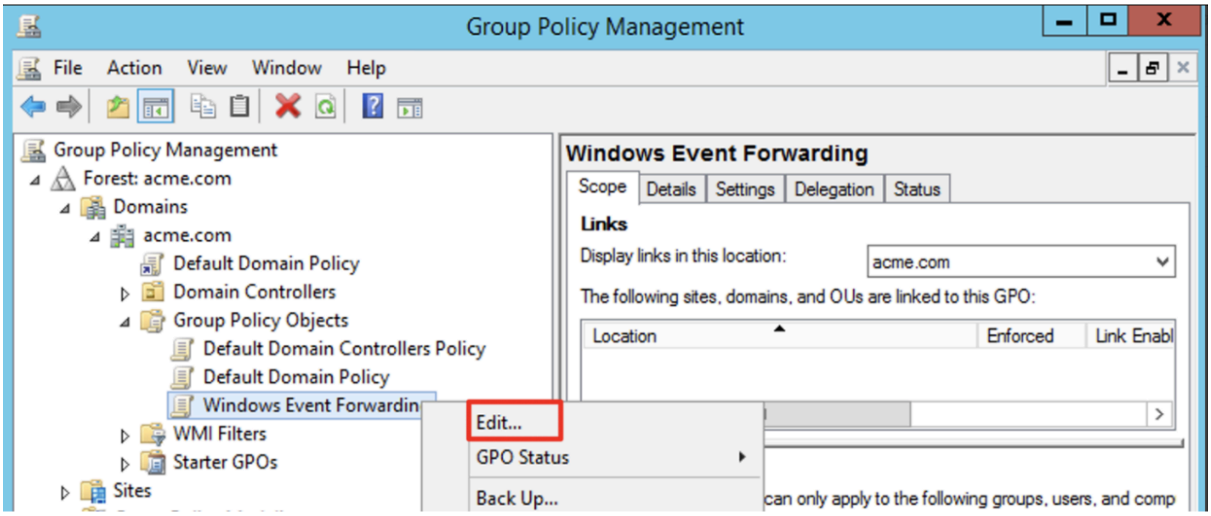
Task 5. Create a WEF Group Policy that applies to every Windows server you want to configure as a WEF

1. In a command prompt, open `gpmc.msc`.

2. In the Group Policy Management window, navigate to Domains → your domain name → Group Policy Object, right-click and select New.

3. In the New GPO window, enter your group policy Name: as Windows Event Forwarding, and click OK.

4. Navigate to Domains → your domain name → Group Policy Objects → Windows Event Forwarding, right-click and select Edit.



5. In the Group Policy Management Editor:

- Set the Windows Remote Management Service for automatic startup.

    1. Select Computer Configuration → Policies → Windows Settings → Security Settings → System Services, and in the view panel locate and double-click Windows Remote Management (WS-Management).

    2. Mark the Define this policy setting checkbox, select Automatic, and then click Apply and OK.

- At a minimum for your WEC configuration, you must enable logging of the same events that you have configured to be collected in your WEC configuration on your domain controller. Otherwise, you will not be able to view these events as the WEC only controls querying not logging. For example, if you have configured authentication events to be collected by your WEC using an authentication protocol, such as Kerberos, you should ensure all relevant audit events for authentication are configured on your domain controller. In addition, you should ensure that all relevant audit events that you want collected, such as the success and failure of account logins for Windows Event ID 4625, are properly configured, particularly for those that you want Cortex XSIAM to apply grouping and analytics inspection.

    > **NOTE:**
    >
    > This step overrides any local policy settings.

    Example 137.

    Here is an example of how to configure the WEC to collect authentication events using Kerberos as the authentication protocol to enable the collection of Broker VM supported Kerberos events, Kerberos pre-authentication, authentication, request, and renewal tickets.

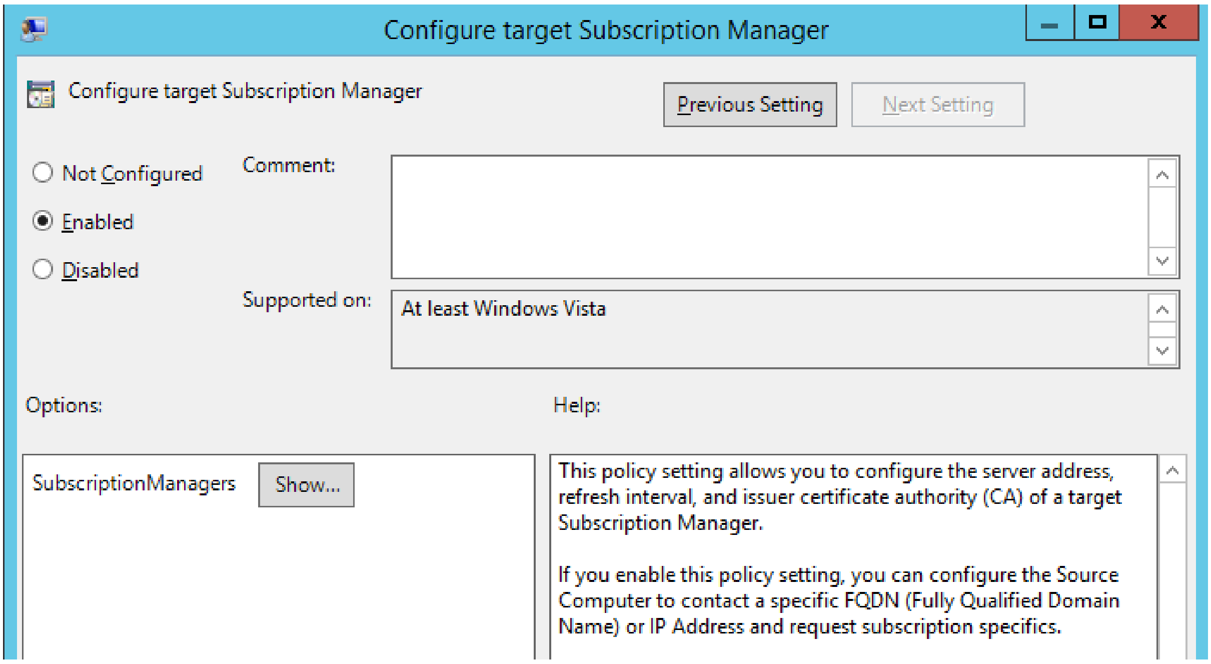
    1. Select Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies → Account Logon.

    2. In the view pane, right-click Audit Kerberos Authentication Service and select Properties. In the Audit Kerberos Authentication Service window, mark Configure the following audit events:, and click Success and Failure followed by Apply and OK.

        Repeat for Audit Kerberos Service Ticket Operations.

6. Configure the subscription manager.

    Navigate to Computer Configuration → Policies → Administrative Templates: Policy definitions → Windows Components → Event Forwarding, right-click Configure target Subscription Manager and select Edit.



Configure target Subscription Manager

Configure target Subscription Manager

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

SubscriptionManagers

Help:

This policy setting allows you to configure the server address, refresh interval, and issuer certificate authority (CA) of a target Subscription Manager.

If you enable this policy setting, you can configure the Source Computer to contact a specific FQDN (Fully Qualified Domain Name) or IP Address and request subscription specifics.

In the Configure target Subscription Manager window, perform the following:

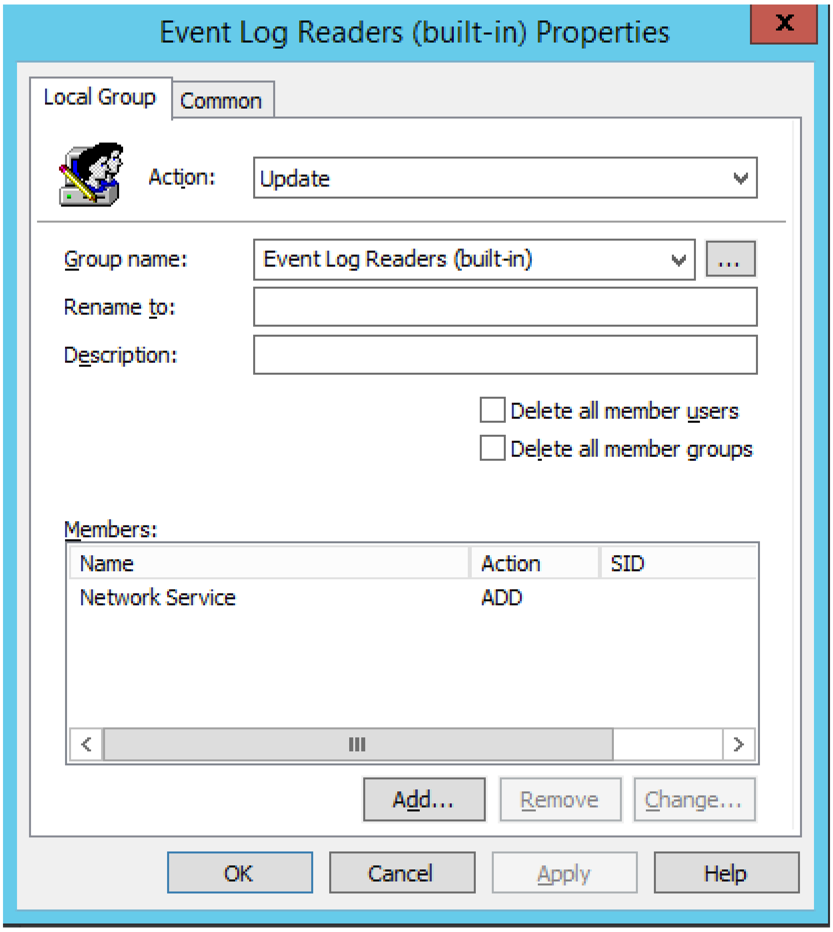
a. Mark Configure target Subscription Manager as Enabled.

b. In the Options section, select Show and in the Show Contents window, paste the Subscription Manage URL you copied from the Cortex XSIAM console, and then click OK.

c. Click Apply and OK to save your changes.

7. Add Network Service to Event Log Readers group.

Select Computer Configuration → Preferences → Control Panel Settings → Local Users and Groups, right-click and select New → Local Group.



Action: Update

Group name: Event Log Readers (built-in)

Rename to:

Description:

□ Delete all member users

□ Delete all member groups

Members:

Name	Action	SID
Network Service	ADD	

In the New Local Group Properties window:

a. In the Group name field, select Event Log Readers (built-in).

b. In the Members section, click Add and enter in the Name filed `Network Service` followed by OK.

> **NOTE:**
>
> You must type out the name, do not select the name from the browse button.

c. Click Apply and OK to save your changes, and close the Group Policy Management Editor window.

8. Configure the Windows Firewall.

> **NOTE:**
>
> If Windows Firewall is enabled on your event forwarders, you will have to define an outbound rule to enable the WEF to reach port 5986 on the WEC.

In the Group Policy Management window, select Computer Configuration → Policies → Windows Settings → Security Settings → Windows Firewall with Advanced Security → Outbound Rules, right-click and select New Rule.

In the New Outbound Rule Wizard define the following Steps:

a. Rule Type: Select Port followed by Next.

b. Protocols and Ports: Select TCP and in the Specific Remote Ports field enter `5986` followed by Next.

c. Action: Select Allow the connection followed by Next.

d. Profile: Select Domain and disable Private and Public followed by Next.

e. Name: Specify `Windows Event Forwarding`.

f. To save your changes, click Finish.

Task 6. Apply the WEF Group Policy

Link the policy to the OU or the group of Windows servers you would like to configure as event forwarders. In the following flow, the domain controllers are configured as an event forwarder.

1. Select Group Policy Management → <your domain name> → Domain Controllers, right-click and select Link an existing GPO....
2. In the Select GPO window, click Windows Event Forwarding followed by OK.
3. In an administrative PowerShell console, execute the following commands:

   a.
   ```
   PS C:\Users\Administrator> gpupdate /force
   ```

   Verify that the `Computer Policy update has completed successfully. User Policy update has completed successfully.` confirmation message is displayed.

   b.
   ```
   PS C:\Users\Administrator> Restart-Service WinRM
   ```

Task 7. Verify Windows Event Forwarding

1. In an administrative PowerShell console, run the following command:

   ```
   PS C:\Users\Administrator> Get-WinEvent Microsoft-windows-WinRM/operational -MaxEvents 10
   ```

2. Look for `WSMan operation EventDelivery completed successfully` confirmation messages. These indicate events forwarded successfully.

Task 8. Manage the Window Event Collector (Optional)

After the Windows Event Collector has been activated in the Cortex XSIAM Management Console, left-click the WEC connection in the APPS column to display the Windows Event Collector settings, and select:

- Configure to define the event configuration information.
- Collection Configuration to view or edit existing or add new events to collect.
- Deactivate to disable the Windows Event Collector.

Task 9. View Windows Event Collector metrics (Optional)

To view metrics about the Windows Event Collector, left-click the WEC connection in the APPS field for your Broker VM, and you'll see the following metrics:

- Connectivity Status: Whether the applet is connected to Cortex XSIAM.
- Logs Received and Logs Sent: Number of logs received and sent by the applet per second over the last 24 hours. If the number of incoming logs received is larger than the number of logs sent, it could indicate a connectivity issue.
- Resources: Displays the amount of CPU, Memory, and Disk space the applet is using.

1.8.1 | Activate Windows Event Collector on Windows Core

Abstract

Learn more about activating the Windrows Event Collector on Windows Core OS to connect with the Broker VM.

After you have configured and registered your Broker VM, you can activate your Windows Event Collector application on Windows Core OS (WCOS). WCOS is a stripped-down, lightweight version of Windows that can be adapted to run on a wide variety of devices with minimal work compared to the previous way explained in Activate Windows Event Collector.

The Windows Event Collector (WEC) runs on the Broker VM collecting event logs from Windows Servers, including Domain Controllers (DCs). The Windows Event Collector can be deployed in multiple setups, and can be connected directly to multiple event generators (DCs or Windows Servers) or routed using one or more Windows Event Collectors. Behind each Windows event collector there may be multiple generating sources.

To enable the collection of the event logs, you are configuring and establishing trust between the Windows Event Forwarding (WEF) collectors and the WEC. Establishing trust between the WEFs and the WEC is achieved by mutual authentication over TLS using server and client certificates. The WEF, a WinRM plugin, runs under the Network Service account. Therefore, you need to provide the WEFs with the relevant certificates and grant the account access permissions to the private key used for client authentication, for example, authenticate with WEC.

> **PREREQUISITE:**

> - Set up and configure Broker VM
> - Broker VM version 8.0 and later
> - You have knowledge of Windows Active Directory and Domain Controllers.
> - You must configure different settings related to the FQDN where the instructions differ depending on whether you are configuring a standalone Broker VM or High Availability (HA) cluster.
>
>   Standalone broker
>
>   A FQDN must be configured for the standalone broker as configured in your local DNS server. Therefore, the Broker VM is registered in the DNS, its FQDN is resolvable from the events forwarder (Windows server), and the Broker VM FQDN is configured. For more information, see Edit Broker VM Configuration.
>
>   HA cluster
>
>   A FQDN must be configured in the cluster settings as configured in your local DNS server, which points to a Load Balancer. For more information, see Configure High Availability Cluster.
> - Windows Server 2012 r2 or later.

After ingestion, Cortex XSIAM normalizes and saves the Windows event logs in the dataset `xdr_data`. The normalized logs are also saved in a unified format in `microsoft_windows_raw`. This enables you to search the data using XQL queries, build correlation rules, and generate dashboards based on the data.

Perform the following procedures in the order listed below.

Task 1. Add, configure, and activate a Windows Event Collector

1. Select Settings → Configurations → Data Broker → Broker VMs.
2. Do one of the following:
   - On the Brokers tab, find the Broker VM, and in the APPS column, left-click Add → Windows Event Collector.
   - On the Clusters tab, find the Broker VM, and in the APPS column, left-click Add → Windows Event Collector.
3. In the Activate Windows Event Collector window, define the Collected Events to configure the events collected by the applet. This lists event sources from which you want to collect events.

Field	Description
Source	Select from the pre-populated list with the most common event sources on Windows Servers. The event source is the name of the software that logs the events. A source provider can only appear once in your list. When selecting event sources, depending on the type event you want to forward, ensure the event source is enabled, for example auditing security events. If the source is not enabled, the source configuration in the given row will fail.
Min. Event Level	Minimum severity level of events that are collected.
Event IDs Group	Whether to Include, Exclude, or collect All event ID groups.
Minimal TLS Version	Select either 1.0 or 1.2 (default) as the minimum TLS version allowed. Ensure that you verify that all Windows event forwarders are supporting the minimal defined TLS version.

Example 138.

To forward all the Windows Event Collector events to the Broker VM, define as follows:

- Source: `ForwardedEvents`
- Min. Event Level: `Verbose`
- Event IDs Group: `All`

> **NOTE:**
>
> By default, Cortex XSIAM collects Palo Alto Networks predefined Security events that are used by the Cortex XSIAM detectors. Removing the Security collector interferes with the Cortex XSIAM detection functionality. Restore to Default to reinstate the Security event collection.

4. Click Activate. After a successful activation, the APPS field displays WEC with a green dot indicating a successful connection.

1. In the APPS column, left-click the WEC connection to display the Windows Event Collector settings, and select Configure.

2. In the Windows Event Forwarder Configuration window, perform the following tasks.:

    a. In the Subscription Manager URL field, click 🗐 (copy) . This will be used when you configure the subscription manager in the GPO (Global Policy Object) on your domain controller.

    b. Enter a password in the Define Client Certificate Export Password field to be used to secure the downloaded WEF certificate that establishes the connection between your DC/WEF and the WEC. You will need this password when the certificate is imported to the events forwarder.

    c. Download the WEF certificate in a PFX format to your local machine.

    To view your Windows Event Forwarding configuration details at any time, select your Broker VM, right-click and navigate to Windows Event Collector → Configure.

   Cortex XSIAM monitors the certificate and triggers a Certificate Expiration notification 30 days prior to the expiration date. The notification is sent daily specifying the number of days left on the certificate, or if the certificate has already expired.

Task 3. Install your WEF Certificate on the WEF to establish connection

1. Start PowerShell with elevated privileges.

    a. Run PowerShell with the following command:

    ```
    PowerShell
    ```

    b. From inside a `PowerShell` command run the following command:

    ```
    Start-Process -Verb RunAs PowerShell
    ```

2. Copy the PFX file that you downloaded to the local Core machine in one of the following ways:

- (Recommended) If you're able to RDP to your server, open Notepad, and select File → Open to copy and paste files from your local machine directly to the server. If you have any local drives mapped through the RDP options, the local drives are also displayed. We recommend this method as it's the simplest.

- If you have enabled `WinRM` for remote `PowerShell` execution, you can copy over PowerShell using this command:

  ```
  $session = New-PSSession –ComputerName <computer name>

  Copy-Item –Path <path to PFX certificate file> –Destination '<temporary file path>' –ToSession $session
  ```

  Example 139.

  ```
  $session = New-PSSession –ComputerName SERVER1

  Copy-Item –Path C:\Downloads\forwarder.wec.paloaltonetworks.com.pfx –Destination 'C:\temp\forwarder.wec.paloaltonetworks.com.pfx' –ToSession $session
  ```

  To enable `WinRM`, use this command:

  ```
  Execute "Start-Service winRM"

  Execute "WinRM quickconfig"
  ```

- Use SSH on server core. This includes enabling SSH on server core and using `winscp` to drag and drop the PFX file.

- Use SMB to open the file share `c$` on the `\\server1\c$` server. You can only use this option if you are an administrator and the firewall on your network isn't set to block file sharing.

  You can also launch PowerShell and run the following command to tell the remote server to copy a file from your local computer using SMB:

  ```
  Copy-Item –Path <path to PFX certificate file> –Destination '\\<computer name>\c$\<path to PFX file>
  ```

  Example 140.

  ```
  Copy-Item –Path C:\Downloads\forwarder.wec.paloaltonetworks.com.pfx –Destination '\\windows-core-server\c$\forwarder.wec.paloaltonetworks.com.pfx
  ```

3. Import the PFX file from PowerShell.

   Use the following command to import the PFX file:

   ```
   certutil -f -importpfx '<path to PFX file from Destination>'
   ```

   Example 141.

   ```
   certutil -f -importpfx '.\forwarder.wec.paloaltonetworks.com.pfx'
   ```

You will need to enter the Client Certificate Export Password you defined in the Cortex XSIAM console.

When the import is complete, the following message is displayed:

```
CertUtil: -importPFX command completed successfully.
```

4. Verify that the certificates are in the correct locations.

   - Ensure the client certificate appears in "My" (Personal) store by running the following command:

     ```
     certutil -store My
     ```

   - Ensure the CA appears in Trusted Root Certification Authorities by running the following command:

     ```
     certutil -store root
     ```

5. Manage the private key of the `forwarder.wec.paloaltonetworks.com.pfx` certificate.

   This entails applying permissions for the `NETWORK SERVICE` user.

   a. Retrieve the Thumbprint of the `forwarder.wec.paloaltonetworks.com.pfx` certificate by running the following script:

   ```
   $store = New-Object System.Security.Cryptography.X509Certificates.X509Store("My","LocalMachine")
   $store.Open("ReadWrite")
   echo $store.Certificates
   ```

   After the script runs, copy the relevant thumbprint.

   b. Grant `NT AUTHORITY\NETWORK SERVICE` with read permissions by running the following script with the `$thumbprint` set to the value you copied in the previous step by replacing `<Thumbprint retrieved value>`.

   ```
   $thumbprint = '<Thumbprint retrieved value>'
   $account = 'NT AUTHORITY\NETWORK SERVICE'
   #Open Certificate store and locate certificate based on provided thumbprint
   $store = New-Object System.Security.Cryptography.X509Certificates.X509Store("My","LocalMachine")
   $store.Open("ReadWrite")
   $cert = $store.Certificates | where {$_.Thumbprint -eq $thumbprint}

   #Create new CSP object based on existing certificate provider and key name
   #Note: Ensure this command is pasted to the same row and doesn’t break to multiple rows.
   #Otherwise, the command will fail with errors.
   $csp = New-Object
   System.Security.Cryptography.CspParameters($cert.PrivateKey.CspKeyContainerInfo.ProviderType,
   $cert.PrivateKey.CspKeyContainerInfo.ProviderName,
   $cert.PrivateKey.CspKeyContainerInfo.KeyContainerName)

   # Set flags and key security based on existing cert
   $csp.Flags = "UseExistingKey","UseMachineKeyStore"
   $csp.CryptoKeySecurity = $cert.PrivateKey.CspKeyContainerInfo.CryptoKeySecurity
   $csp.KeyNumber = $cert.PrivateKey.CspKeyContainerInfo.KeyNumber

   # Create new access rule - could use parameters for permissions, but I only needed GenericRead
   ```

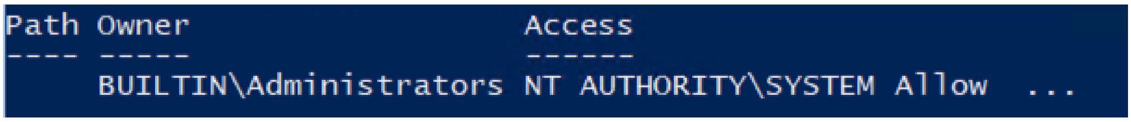
```
$access = New-Object
System.Security.AccessControl.CryptoKeyAccessRule($account,"GenericRead","Allow")
# Add access rule to CSP object

$csp.CryptoKeySecurity.AddAccessRule($access)

#Create new CryptoServiceProvider object which updates Key with CSP information created/modified
above
$rsa2 = New-Object System.Security.Cryptography.RSACryptoServiceProvider($csp)

#Close certificate store
$store.Close()
echo $csp.CryptoKeySecurity
```

c. After the script runs, validate the permissions are now set correctly.



```
Path Owner                  Access
---- -----                  ------
     BUILTIN\Administrators NT AUTHORITY\SYSTEM Allow  ...
```

Task 4. Add the Network Service account to the domain controller Event Log Readers group.

> **NOTE:**
>
> You must install the WEF certificate on every Windows Server, whether DC or not, for the WEFs that are supposed to forward logs to the Windows Event Collector applet on the Broker VM.

1. To enable events forwarders to forward events, the Network Service account must be a member of the Active Directory Event Log Readers group. In PowerShell, execute the following command on the domain controller that is acting as the event forwarder:

```
PS C:\> net localgroup "Event Log Readers" "NT Authority\Network Service" /add
```

Make sure you see `The command completed successfully` message.

2. Grant access to view the security event logs.

a. Run `wevtutil gl security` and take note of your `channelAccess` value.

Example 142.

```
`PS C:\Users\Administrator> wevtutil gl security
name: security
enabled: true
type: Admin
owningPublisher:
isolation: Custom
channelAccess: O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\security.evtx
  retention: false
  autoBackup: false
  maxSize: 134217728
publishing:
  fileMax: 1
```

Take note of value: `channelAccess: O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)`

b. Run `wevtutil sl security "/ca:<channelAccess value>(A;;0x1;;;S-1-5-20)"`

Example 143.

```
PS C:\Users\Administrator> wevtutil sl security "/ca:O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)
(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;S-1-5-20)"
```

Make sure you grant access on each of your domain controller hosts.

Task 5. Create a WEF Group Policy that applies to every Windows server you want to configure as a WEF

As a Group Policy Management Console is not available on Core servers, it’s not possible to fully edit a Group Policy Object (GPO) either with PowerShell or using a web solution. As a result, follow this alternative method, which is based on configuring a group policy from another Windows DC by remotely configuring the group policy.

1. Use any DC that has the Group Policy Management Console available in the same domain as the Core server, and verify the connection between the servers with a simple ping.

2. Run `cmd` as an administrator.

3. Run the following command:

   ```
   gpmc.msc /gpcomputer: <computer name.Domain>
   ```

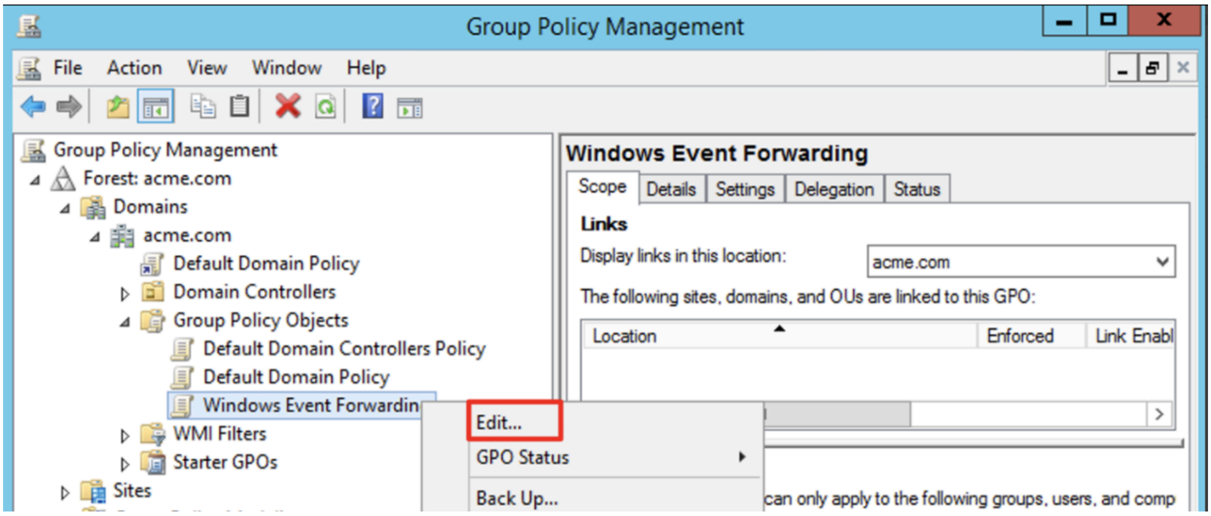
   Example 144.

   ```
   gpmc.msc /gpcomputer: WIN-SI2SVDOKIMV.ENV21.LOCAL
   ```

4. In the Group Policy Management window, navigate to Domains → your domain name → Group Policy Object, right-click and select New.

5. In the New GPO window, enter your group policy Name: as Windows Event Forwarding, and click OK.

6. Navigate to Domains → your domain name → Group Policy Objects → Windows Event Forwarding, right-click and select Edit.



Links

Display links in this location: acme.com

The following sites, domains, and OUs are linked to this GPO:

can only apply to the following groups, users, and comp

7. In the Group Policy Management Editor:

- Set the Windows Remote Management Service for automatic startup.

    1. Select Computer Configuration → Policies → Windows Settings → Security Settings → System Services, and in the view panel locate and double-click Windows Remote Management (WS-Management).

    2. Mark the Define this policy setting checkbox, select Automatic, and then click Apply and OK.

- At a minimum for your WEC configuration, you must enable logging of the same events that you have configured to be collected in your WEC configuration on your domain controller. Otherwise, you will not be able to view these events as the WEC only controls querying not logging. For example, if you have configured authentication events to be collected by your WEC using an authentication protocol, such as Kerberos, you should ensure all relevant audit events for authentication are configured on your domain controller. In addition, you should ensure that all relevant audit events that you want collected, such as the success and failure of account logins for Windows Event ID 4625, are properly configured, particularly for those that you want Cortex XSIAM to apply grouping and analytics inspection.

    > **NOTE:**
    >
    > This step overrides any local policy settings.

    Example 145.

    Here is an example of how to configure the WEC to collect authentication events using Kerberos as the authentication protocol to enable the collection of Broker VM supported Kerberos events, Kerberos pre-authentication, authentication, request, and renewal tickets.

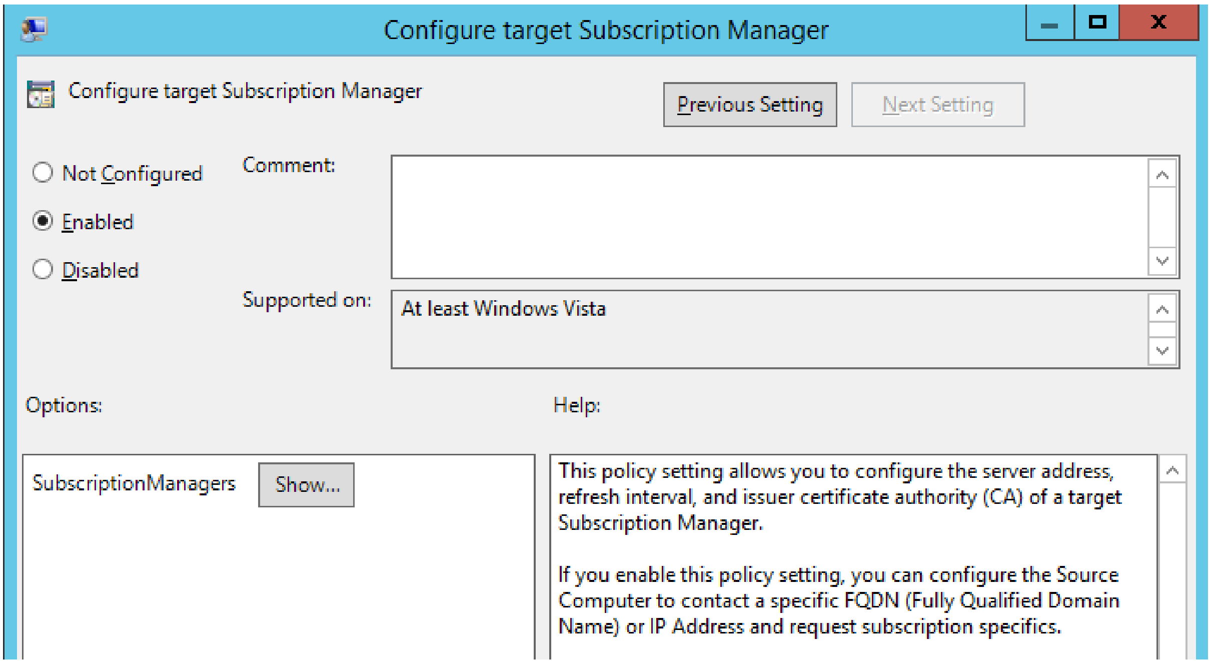
    1. Select Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies → Account Logon.

    2. In the view pane, right-click Audit Kerberos Authentication Service and select Properties. In the Audit Kerberos Authentication Service window, mark Configure the following audit events:, and click Success and Failure followed by Apply and OK.

        Repeat for Audit Kerberos Service Ticket Operations.

8. Configure the subscription manager.

    Navigate to Computer Configuration → Policies → Administrative Templates: Policy definitions → Windows Components → Event Forwarding, right-click Configure target Subscription Manager and select Edit.



Configure target Subscription Manager

Configure target Subscription Manager

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

SubscriptionManagers

Help:

This policy setting allows you to configure the server address, refresh interval, and issuer certificate authority (CA) of a target Subscription Manager.

If you enable this policy setting, you can configure the Source Computer to contact a specific FQDN (Fully Qualified Domain Name) or IP Address and request subscription specifics.

In the Configure target Subscription Manager window:

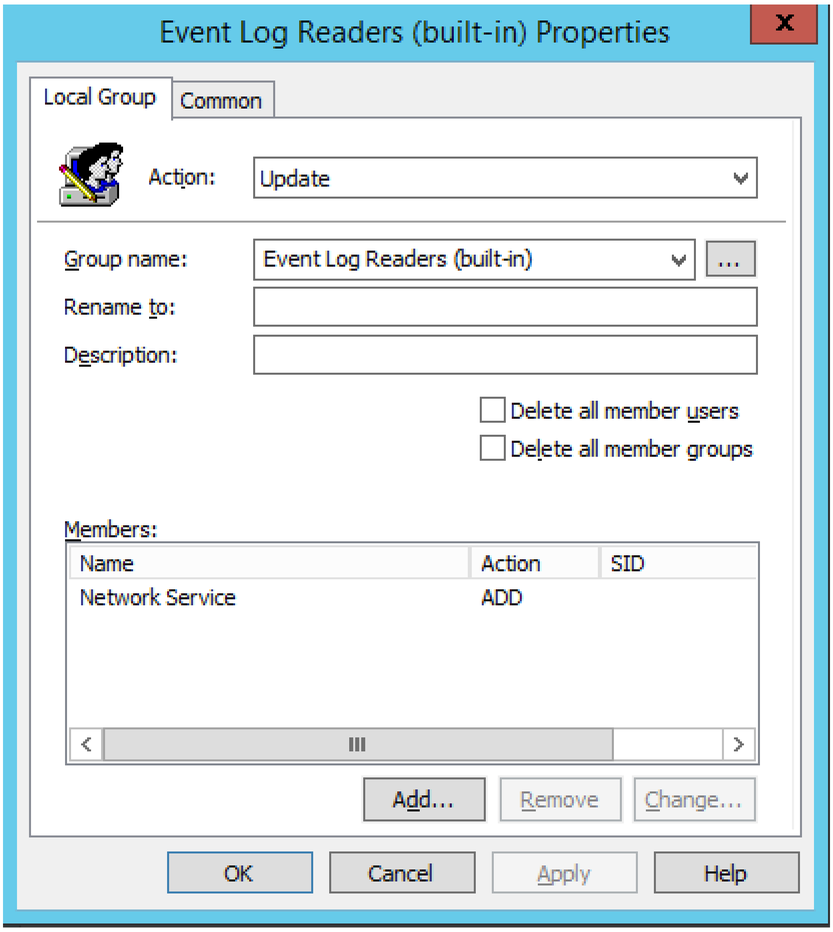
a. Mark Configure target Subscription Manager as Enabled.

b. In the Options section, select Show and in the Show Contents window, paste the Subscription Manage URL you copied from the Cortex XSIAM console, and then click OK.

c. Click Apply and OK to save your changes.

9. Add Network Service to Event Log Readers group.

Select Computer Configuration → Preferences → Control Panel Settings → Local Users and Groups, right-click and select New → Local Group.


Event Log Readers (built-in) Properties

Local Group | Common

Action: Update

Group name: Event Log Readers (built-in)

Rename to:

Description:

□ Delete all member users

□ Delete all member groups

Members:

Name	Action	SID
Network Service	ADD	

In the New Local Group Properties window:

a. In the Group name field, select Event Log Readers (built-in).

b. In the Members section, click Add and enter in the Name filed `Network Service` followed by OK.

> **NOTE:**
>
> You must type out the name, do not select the name from the browse button.

c. Click Apply and OK to save your changes, and close the Group Policy Management Editor window.

10. Configure the Windows Firewall.

> **NOTE:**
>
> If Windows Firewall is enabled on your event forwarders, you will have to define an outbound rule to enable the WEF to reach port 5986 on the WEC.

In the Group Policy Management window, select Computer Configuration → Policies → Windows Settings → Security Settings → Windows Firewall with Advanced Security → Outbound Rules, right-click and select New Rule.

In the New Outbound Rule Wizard define the following Steps:

a. Rule Type: Select Port followed by Next.

b. Protocols and Ports: Select TCP and in the Specific Remote Ports field enter `5986` followed by Next.

c. Action: Select Allow the connection followed by Next.

d. Profile: Select Domain and disable Private and Public followed by Next.

e. Name: Specify `Windows Event Forwarding`.

f. To save your changes, click Finish.

Task 6. Apply the WEF Group Policy

Link the policy to the OU or the group of Windows servers you would like to configure as event forwarders. In the following flow, the domain controllers are configured as an event forwarder.

1. Select Group Policy Management → <your domain name> → Domain Controllers, right-click and select Link an existing GPO....
2. In the Select GPO window, click Windows Event Forwarding followed by OK.
3. In an administrative PowerShell console, execute the following commands:

   a. `PS C:\Users\Administrator> gpupdate /force`

   Verify that the `Computer Policy update has completed successfully. User Policy update has completed successfully.` confirmation message is displayed.

   b. `PS C:\Users\Administrator> Restart-Service WinRM`

Task 7. Verify Windows Event Forwarding

1. In an administrative PowerShell console, run the following command:

   ```
   PS C:\Users\Administrator> Get-WinEvent Microsoft-windows-WinRM/operational -MaxEvents 10
   ```

2. Look for `WSMan operation EventDelivery completed successfully` confirmation messages. These indicate events forwarded successfully.

Task 8. Manage the Window Event Collector (Optional)

After the Windows Event Collector has been activated in the Cortex XSIAM Management Console, left-click the WEC connection in the APPS column to display the Windows Event Collector settings, and select:

- Configure to define the event configuration information.
- Collection Configuration to view or edit existing or add new events to collect.
- Deactivate to disable the Windows Event Collector.

Task 9. View Windows Event Collector metrics (Optional)

To view metrics about the Windows Event Collector, left-click the WEC connection in the APPS field for your Broker VM, and you'll see the following metrics:

- Connectivity Status: Whether the applet is connected to Cortex XSIAM.
- Logs Received and Logs Sent: Number of logs received and sent by the applet per second over the last 24 hours. If the number of incoming logs received is larger than the number of logs sent, it could indicate a connectivity issue.
- Resources: Displays the amount of CPU, Memory, and Disk space the applet is using.

1.8.2 | Renew WEC certificates

Abstract

Learn more about renewing your WEC certificates in Cortex XSIAM.

Renewing your WEC certificates in Cortex XSIAM includes renewing your Windows Event Forwarding (WEF) client certificate and your WEC server certificate. You must install the WEF certificate on every Windows server, whether a Domain Controller (DC) or not, for the WEFs that are supposed to forward logs to the Windows Event Collector applet on the Broker VM.

> **IMPORTANT:**
>
> After you receive a notification for renewing your WEC CA certificate, we recommend that you do not add any new WEF clients until the WEC certification renewal process is complete. Events from these WEF clients that are added afterwards will not be collected by the server until the WEC certificates are renewed.

In addition, Cortex XSIAM manages the renewal of your WEC certificates by implementing the following time limits:

- The WEC CA certificate is increased for an extended period of time for a maximum of 20 years.
- The Broker VM applet includes an automatic renewal mechanism for a WEC server certificate, which has a lifespan of 12 months.
- The WEC client certificate after the renewal is issued with a lifespan of 5 years.

Perform the following procedures in the order listed below.

Task 1. Renew your WEF client certificate in Cortex XSIAM

1. Select Settings → Configurations → Data Broker → Broker VMs.
2. Do one of the following:

- On the Brokers tab, find the Broker VM, and in the APPS column, left-click the WEC connection to display the Windows Event Collector settings, and select Configure.

- On the Clusters tab, find the Broker VM, and in the APPS column, left-click the WEC connection to display the Windows Event Collector settings, and select Configure.

3. In the Windows Event Forwarder Configuration window, perform the following tasks:

   a. In the Subscription Manager URL field, click 📋 (copy) . This will be used when you configure the subscription manager in the GPO (Global Policy Object) on your domain controller.

   b. Enter a password in the Define Client Certificate Export Password field to be used to secure the downloaded WEF certificate that establishes the connection between your DC/WEF and the WEC. You will need this password when the certificate is imported to the events forwarder.

   c. Download the WEF certificate in a PFX format to your local machine.

4. Install your WEF Certificate on the WEF to establish connection.

   > **NOTE:**
   >
   > You must install the WEF certificate on every Windows Server, whether DC or not, for the WEFs that are supposed to forward logs to the Windows Event Collector applet on the Broker VM.

   a. Locate the PFX file you downloaded from the Cortex XSIAM console and double-click to open the Certificate Import Wizard.

   b. In the Certificate Import Wizard:

      1. Select Local Machine, and then click Next.

      2. Verify the File name field displays the PFX certificate file you downloaded and click Next.

      3. In the Passwords field, enter the Client Certificate Export Password you defined in the Cortex XSIAM console followed by Next.

      4. Select Automatically select the certificate store based on the type of certificate, and then click Next and Finish.

   c. From a command prompt, run `certlm.msc`.

   d. In the file explorer, navigate to Certificates and verify the following for each of the folders:

- In the Personal → Certificates folder, ensure the certificate `forwarder.wec.paloaltonetworks.com` is displayed.

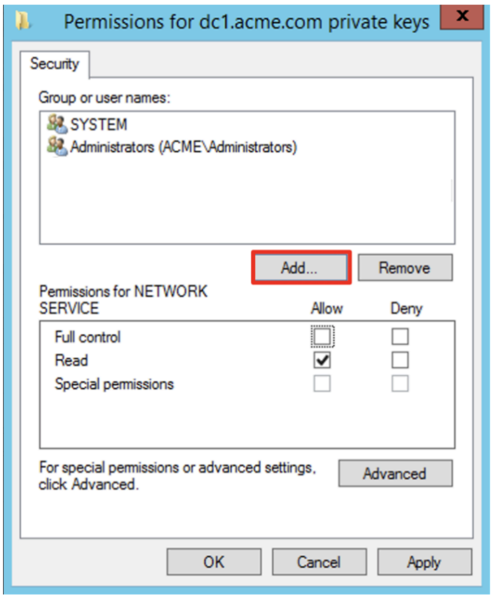
- In the Trusted Root Certification Authorities → Certificates folder, ensure the CA `ca.wec.paloaltonetworks.com` is displayed.

> **NOTE:**
>
> You can see more than one `ca.wec.paloaltonetworks.com` and `forwarder.wec.paloaltonetworks.com` file from a previous installation in the directory, so select the file with the most extended Expiration Date. You can verify that you are using the correct certificate:
>
> - To verify the client certificate in the Personal → Certificates folder is related to the CA, you can select your `forwarder.wec.paloaltonetworks.com` file and from the Certification Path tab, double-click ca.wec.paloaltonetworks.com. In the Details tab, Show: Properties only, and verify the Thumbprint matches the `ca.wec.paloaltonetworks.com` file Thumbprint.
>
> - For the Trusted Root Certificate (i.e. CA certificate), you can verify the Thumbprint of your `ca.wec.paloaltonetworks.com` file matches the Subscription Manager URL by double-clicking the file and from the Details tab verifying the Thumbprint.

e. Navigate to Certificates Personal Certificates.

f. Right-click the certificate and navigate to All tasks → Manage Private Keys.

g. In the Permissions window, select Add and in the Enter the object name section, enter `NETWORK SERVICE`, and then click Check Names to verify the object name. The object name is displayed with an underline when valid. and then click OK.



Permissions for dc1.acme.com private keys

Security

Group or user names:

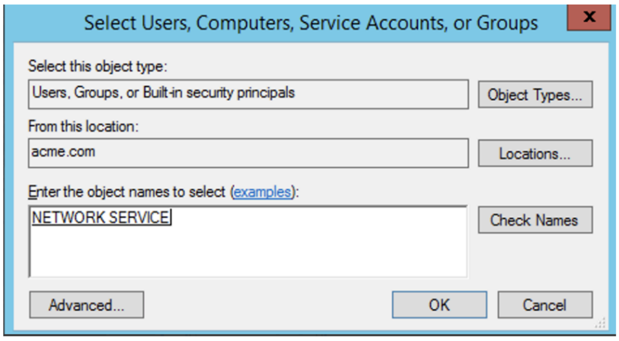
SYSTEM

Administrators (ACME\Administrators)

Permissions for NETWORK SERVICE

Permissions for NETWORK SERVICE	Allow	Deny
Full control	□	□
Read	☑	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced.



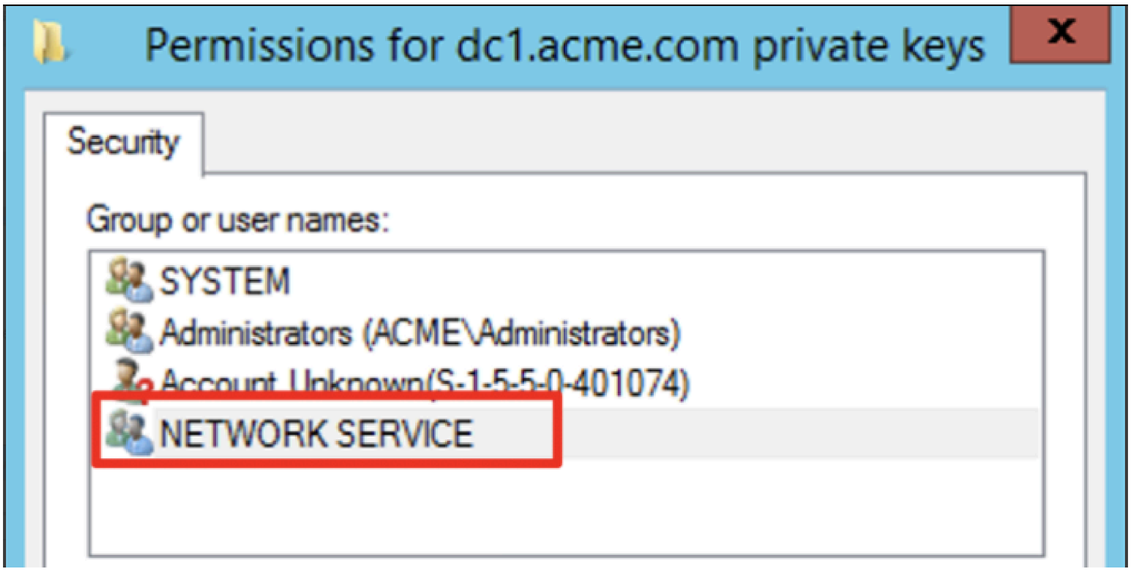
Select Users, Computers, Service Accounts, or Groups

Select this object type: Users, Groups, or Built-in security principals

From this location: acme.com

Enter the object names to select (examples): NETWORK SERVICE

h. Click OK, verify the Group or user names that are displayed, and then click Apply Permissions for private keys.



Permissions for dc1.acme.com private keys

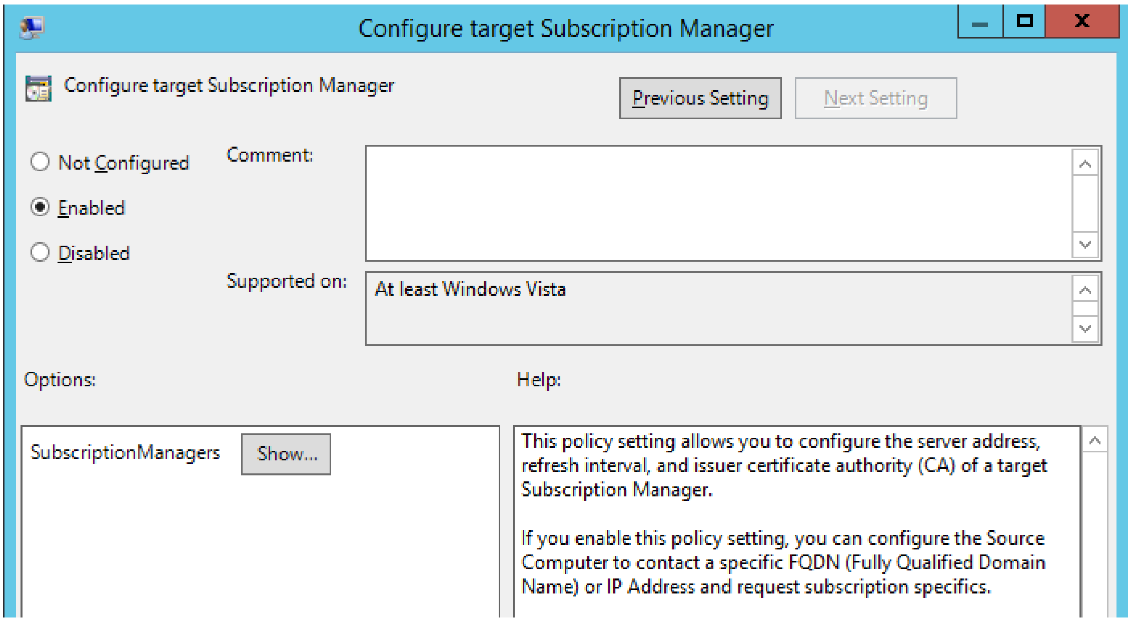
Security

Group or user names:

- SYSTEM
- Administrators (ACME\Administrators)
- Account Unknown(S-1-5-5-0-401074)
- NETWORK SERVICE

5. Configure the subscription manager.

   a. Navigate to Computer Configuration → Policies → Administrative Templates: Policy definitions → Windows Components → Event Forwarding, right-click Configure target Subscription Manager and select Edit.



Configure target Subscription Manager

Configure target Subscription Manager

Previous Setting | Next Setting

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

SubscriptionManagers Show...

Help:

This policy setting allows you to configure the server address, refresh interval, and issuer certificate authority (CA) of a target Subscription Manager.

If you enable this policy setting, you can configure the Source Computer to contact a specific FQDN (Fully Qualified Domain Name) or IP Address and request subscription specifics.

   b. In the Configure target Subscription Manager window, perform the following:

      1. Mark Configure target Subscription Manager as Enabled.

      2. In the Options section, select Show and in the Show Contents window, paste the Subscription Manage URL you copied from the Cortex XSIAM console, and then click OK.

      3. Click Apply and OK to save your changes.

6. Complete the WEF Client certificate renewal.

   On every WEF DC, perform the following from a command prompt:

a. Run `gpupdate /force` to update the group policy.

b. To apply the configurations, `Restart-Service WinRM`.

Task 2. Renew your WEC server certificate in Cortex XSIAM

> **NOTE:**
>
> Only perform this step under the following conditions:
>
> - You have completed the WEF certification renewal process for ALL clients in your environment. Otherwise, events from the WEFs that you did not install the new client certificate will not be collected by the WEC.
>
> - You are approaching the WEC server CA certificate expiration date, which is 2 years after the Windows Event Collector applet activation, and receive a notification in the Cortex XSIAM console.

1. Select Settings → Configurations → Data Broker → Broker VMs.

2. Do one of the following:

   - On the Brokers tab, find the Broker VM, and in the APPS column, left-click the WEC connection to display the Windows Event Collector settings, and select Renew WEC Server Certificate.

   - On the Clusters tab, find the Broker VM, and in the APPS column, left-click the WEC connection to display the Windows Event Collector settings, and select Renew WEC Server Certificate.

3. Click Renew.

   Once Cortex XSIAM renews the WEC server certificate, the status of the WEC in the APPS field on the Broker VMs machine is Connected indicating the applet is running. In addition, the health status of the Windows Event Collector applet is now green instead of yellow and the warning message that appeared when you hovered over the health status no longer appears. Your WEC server certificate is issued with a lifespan of 12 months.

   We also suggest that you run the following XQL query to verify that your event logs are being captured:

   ```
   dataset = xdr_data
   | filter _product = "Windows"
   | fields _vendor,_product,action_evtlog_level,action_evtlog_event_id
   | sort desc _time
   | limit 20
   ```

   > **NOTE:**
   >
   > If this query does not display results with a timestamp from after the renewal process, it could indicate that the renewal process is not complete, so wait a few minutes before running another query. If you are still having a problem, contact Technical Support.

2 | XDR Collectors

Abstract

Learn how XDR Collectors can be used for on-premise data collection on Windows and Linux machines.

> **NOTE:**
>
> Ingestion of log events larger than 5 MB is not supported.

Cortex XSIAM provides an XDR Collectors (XDRC) configuration that is dedicated for on-premise data collection on Windows and Linux machines. The XDRC includes a dedicated installer, a collector upgrade configuration, content updates, and policy management. The XDRC is a data collector that gathers and processes logs and events from multiple sources. It leverages Elasticsearch Filebeat, a lightweight log shipper, to collect log data from various systems and applications. Additionally, Winlogbeat gathers Windows event logs, ensuring comprehensive visibility into Windows environments. These components facilitate centralized analysis, threat detection, and investigation across the Cortex XSIAM ecosystem.

2.1 | Manage XDR Collectors

Abstract

Manage Cortex XSIAM collectors.

On the XDR Collectors Administration page, you can view the list of collectors and perform additional tasks such as changing the alias of the collector, upgrading the collector version, and setting a proxy address and port for the collector.

2.1.1 | Install the XDR Collector installation package for Windows

Abstract

Learn about the Cortex XDR Collector installation options on Windows collector machines.

A standard XDR Collector installation for Windows is intended for standard physical collector machines or persistent virtual collector machines. You can perform the Windows installation for the XDR Collectors using the MSI or Msiexec.

2.1.1.1 | Install the XDR Collector on Windows using the MSI

Abstract

Learn how to install the Cortex XDR Collector on Windows using the MSI file.

Use the following workflow to install the XDR Collector using the MSI file.

Before completing this task, ensure that you create and download a Cortex XDR Collector installation package in Cortex XSIAM.

To install an XDR Collector installation package on Windows using the MSI file.

> **NOTE:**
>
> When the package is executed using the MSI, an installation log is generated in `%TEMP%\MSI<Random characters>.log` by default.

1. With Administrator level privileges, run the MSI file that you downloaded in Cortex XSIAM on the collector machine.

   The installer displays a welcome dialog.

2. Click Next.

3. Select I accept the terms in the License Agreement and click Next.

4. Install the XDR Collector.

   The installer displays the User Account Control dialog box.

5. Click Yes.

6. After you complete the installation, verify that the Cortex XDR Collector can establish a connection with Cortex XSIAM.

   > **NOTE:**
   >
   > If the XDR Collector does not connect to Cortex XSIAM, verify your internet connection on the collector machine. If the XDR Collector still does not connect, verify that the installation package has not been removed from the Cortex XSIAM tenant.

2.1.1.2 | Install the XDR Collector on Windows using Msiexec

Abstract

Learn how to install the Cortex XDR Collectors on Windows using the Msiexec.

Msiexec provides full control over the installation process and allows you to install, modify, and perform operations on a Windows Installer from the command line interface (CLI). You can also use Msiexec to log any issues encountered during installation.

You can also use Msiexec in conjunction with a System Center Configuration Manager (SCCM), Altiris, Group Policy Object (GPO), or other MSI deployment software to install the XDR Collector on multiple collector machines for the first time.

When you install the XDR Collector with Msiexec, you must install the XDR Collector per-machine and not per-user.

Although Msiexec supports additional options, the XDR Collectors installers support only the options listed here. For example, with Msiexec, the option to install the software in a non-standard directory is not supported—you must use the default path.

The following parameters apply to the initial installation of the XDR Collector on the collector machine.

- `/i <installer path>\<installer file name>.msi DATA_PATH=<Path> PROXY_LIST=<address or list> /quiet /l*v <installation log path>`: Installs a package quietly, changes data path, adds proxies, and creates an installation log.

  For example, `msiexec /i c:\install\XDRCollector-Win_x64.msi DATA_PATH=c:\data PROXY_LIST=2.2.2.2:8888,1.1.1.1:8080 /quiet /l*v c:\installlog.txt`

  Where

  - `LOG_LEVEL`: Sets the level of logging for the XDR Collector log (`INFO`, `DEBUG`, `ERROR`, and `TRACE`).
  - `LOG_MAX_BYTES`: Sets the maximum log size in bytes.
  - `LOG_BACKUP_COUNT`: Number of cycling logs for the XDR Collector.
  - `PROXY_LIST`: Proxy address or name, where you can add a comma separated list, such as 2.2.2.2:8888,1.1.1.1:8080.
  - `LOG_PATH`: The path to save the XDR Collector, Filebeat, and Winlogbeat logs.
  - `DATA_PATH`: The path for persistence, content, Filebeat application data, Winlogbeat application data, and transaction data.
  - `PROVISIONING_SERVER`: Provisioning server address.
  - `DISTRIBUTION_ID`
  - `ELB_ADDRESS`: Load balancer for fresh XDR Collector installation.

Before completing this task, ensure that you create and download a Cortex XDR Collector installation package in Cortex XSIAM.

To install XDR Collectors using Msiexec:

1. Use one of the following methods to open a command prompt as an administrator.

   - Select Start → All Programs Accessories. Right-click Command prompt and Run as administrator.
   - Select Start. In the Start Search box, type `cmd`. Then, to open the command prompt as an administrator, press CTRL+SHIFT+ENTER keys.

2. Run the `msiexec` command followed by one or more supported options and properties.

   For example:

```
msiexec /i XDRCollector-Win_x64.msi DATA_PATH=c:\data
PROXY_LIST=2.2.2.2:8888,1.1.1.1:8080 /quiet /l*v c:\installlog.txt
```

2.1.2 | Install the XDR Collector installation package for Linux

Abstract

Learn how to install the Cortex XDR Collector on Linux collector machines.

You can install the XDR Collector using three available packages for a Linux installation: Linux RPM, Linux DEB, and Linux SH. You can install the XDR Collector package on any Linux server, including a physical or virtual machine, and as temporary sessions.

You can install XDR Collectors in any Linux server period, whether its a physical or virtual machine. Temporary sessions can be in either of them.

> **NOTE:**
>
> We recommend that you perform a Linux RPM or Linux DEB installation.

Before completing this task, ensure that you create and download a Cortex XDR Collector installation package, and then upload these installation files to your Linux environment.

To install the XDR Collectors installation package for Linux.

1. Log on to the Linux server.

   For example:

   ```
   user@local ~
                                                   $
                                                   ssh root@ubuntu.example.com
                                                   Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-1041-
   aws x86_64)


                                                   * Documentation:  https://help.ubuntu.com
                                                   * Management:     https://landscape.canonical.com
                                                   * Support:        https://ubuntu.com/advantage

                                                   Get cloud support with Ubuntu Advantage Cloud Guest:
                                                   http://www.ubuntu.com/business/services/cloud

                                                   0 packages can be updated.
                                                   0 updates are security updates.


                                                   Last login: Tue Aug 26 22:14:15 2021 from
   192.168.1.100
   ```

2. Extract the installation files you uploaded using one of the following commands, which is dependent on the Linux package you downloaded:

Linux Package	Extract Command
Linux RPM	`tar xvf <installation_package_name>.rpm`
Linux DEB	`tar xvf <installation_package_name>.deb`
Linux SH	`tar xvf <installation_package_name>.sh`

3. Create a directory and copy the `collector.conf` installation file to the `/etc/panw/` directory.

   ```
   sudo mkdir -p /etc/panw
   sudo cp ./collector.conf /etc/panw/
   ```

4. Install the XDR Collectors software.

   You can install the XDR Collectors on the collector machine manually using the shell installer or using the Linux package manager for `.rpm` and `.deb` installers:

   > **IMPORTANT:**
   >
   > When performing a XDR Collector installation or upgrade in Linux using a shell installer, the `/tmp` folder cannot be marked as `noexec`. Otherwise, the installation or upgrade fails. As a workaround, before the installation or upgrade, use the following command:
   >
   > ```
   > mount -o remount,exec /tmp
   > ```

   To deploy using package manager:

   1. Depending on your Linux distribution, install the XDR Collectors using one of the following commands, where the `<file name>` is taken from the files provided in the downloaded Linux installation package:

Distribution	Install Command
RHEL or Oracle	• `yum install ./<file_name>.rpm` • `rpm -i ./<file_name>.rpm`

Distribution	Install Command
Ubuntu or Debian	• `apt-get install ./<file_name>.deb` • `dpkg -i ./<file_name>.deb`
SUSE	• `zypper install ./<file_name>.rpm` • `rpm -i ./<file_name>.rpm`

2. Verify the XDR Collectors was installed on the collector machine.

   Enter the following command on the collector machine:

   `dpkg -l | grep xdr-collector` or `rpm -qa | grep xdr-collector`.

To deploy the shell installer:

1. Enable execution of the script using the `chmod +x <file_name>.sh` command, where the `<file name>` is taken from the file provided in the downloaded Linux installation package.

2. Run the install script as root or with root permissions.

   For example:

```
root@ubuntu:/home# chmod +x linux.sh
root@ubuntu:/home# ./linux.sh

Verifying archive integrity... All good.
Uncompressing XDR-Collector version 1.0.0.467 100%
Systemd: starting xdr-collector service
Synchronizing state of xdr-collector.service with SysV service script with /lib/systemd/systemd-
sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable xdr-collector
Created symlink /etc/systemd/system/multi-user.target.wants/xdr-collector.service→
/lib/systemd/system/xdr-collector.service.
```

> **NOTE:**
>
> If the XDR Collector does not connect to Cortex XSIAM, verify your Internet connection on the collector machine. If the XDR Collector still does not connect, verify the installation package has not been removed from the Cortex XSIAM management console.

Additional options are available to help you customize your installation if needed. The following table describes common options and parameters.

If you are using `rpm` or `deb` installers, you must also add these parameters to the `/etc/panw/collector.conf` file prior to installation.

Option	Description
`--proxy-list "<proxyserver>:<port>"`	Proxy communication Configure the XDR Collector to communicate through an intermediary such as a proxy. To enable the XDR Collector to direct communication to an intermediary, you use this installation option to assign the IP address and port number you want the XDR Collector to use. You can also configure the proxy by entering the FQDN and port number. When you enter the FQDN, you can use both lowercase and uppercase letters. Avoid using special characters or spaces. Use double quotes (" ") to enclose the IP address and port number. Use commas to separate multiple addresses. For example: `--proxy-list "My.Network.Name:808, 10.196.20.244:8080"` After the initial installation, you can change the proxy settings from using the configuration XML. **NOTE:** The XDR Collector does not support proxy communication in environments where proxy authentication is required.
`--data-path <directory path>`	Directory path The path for persistence, content, Filebeat application data, and transaction data. `--data-path=/tmp/xdrLog`

2.1.3 | Configure the XDR Collector upgrade scheduler

Abstract

You can configure the Cortex XDR Collector upgrade scheduler and the number of parallel upgrades.

You can configure the Cortex XDR Collector upgrade scheduler and the number of parallel upgrades. There can be a maximum of 500 parallel upgrades scheduled in a week, which is the default configuration at any time of day.

To define the XDR Collector upgrade scheduler and number of parallel upgrades.

1. In Cortex XSIAM, select Settings → Configurations → XDR Collectors → Configuration.
2. Set the XDR Collectors Configurations settings.
    - `Amount of Parallel Upgrades`: Specify the number of parallel upgrades, where the maximum number is 500 (default).
    - `Days in Week`: Select the specific days in the week that you want the upgrade to occur, where the default is configured as every day in the week.
    - `Schedule`: Select whether you want the upgrade to be at Any time (default) or at a Specific time. When setting a specific time, you can set the From and To times.
3. Click Save.

2.1.4 | Set an application proxy for XDR Collectors

Abstract

You can set an application-specific proxy for a Cortex XDR Collector without affecting the communication of other applications on the collector machine.

In environments where Cortex XDR Collectors communicate with the Cortex XSIAM server through a wide system proxy, you can set an application-specific proxy for the XDR Collector without affecting the communication of other applications on the collector machine. You can set the proxy after installation from the XDR Collectors Administration page in Cortex XSIAM as described in this topic. You can assign up to ten different proxy servers per XDR Collector. The proxy server that the agent uses is selected randomly and with equal probability. If the communication between the XDR Collector and the Cortex XSIAM server through the app-specific proxies fails, the XDR Collector resumes communication through the system-wide proxy defined on the collector machine. If that fails as well, the XDR Collector resumes communication with Cortex XSIAM directly.

1. In Cortex XSIAM, select Settings → Configurations → XDR Collectors → Administration.
2. If needed, filter the list of on-premise collector machines.

3. Set an agent proxy.

    a. Select the row of the on-premises collector machine that you want to set as a proxy.

    b. Right-click the collector machine, and select Set Collector proxy.

    c. You can assign up to ten different proxies per XDR Collector. For each proxy, specify the IP address and port number. After each Proxy Address and Port added, select ↵ to add the values to a list underneath these fields. Broker VMs in the same tenant can also be configured to use as a proxy, by enabling Agent proxy in the Broker VMs.

    d. Click Set when you’re done.

    e. If necessary later, you can disable the collector proxy by selecting Disable Collector Proxy from the right-click menu.

    When you disable the proxy configuration, all proxies associated with that XDR Collector are removed. The XDR Collector resumes communication with the Cortex XSIAM server through the wide-system proxy if defined; otherwise, if a wide-system is not defined, the XDR Collector resumes communicating directly with the Cortex XSIAM server. If neither a wide-system proxy nor direct communication exist and you disable the proxy, the XDR Collector disconnects from Cortex XSIAM.

2.1.5 | Set an alias for an XDR Collector machine

Abstract

Configure an alias to identify one or more collector machines by a name that is different from the collector machine hostname.

To identify one or more collector machines by a name that is different from the collector machine hostname, you can configure an alias. You can set an alias for a single collector machine or you can set an alias for multiple collector machines in bulk. To quickly search for the collector machines during investigation and when you need to take action, you can use the either the collector machine hostname or the alias.

1. Select Settings → Configurations → XDR Collectors → Administration.

2. Select one or more collector machines.

3. Right-click anywhere in the collector machine rows, and select Change Collector Alias.

4. Specify the alias name and Update.

5. Use the Quick Launcher to search the collector machines by alias across the XDR Collectors console.

2.2 | XDR Collector profiles

Abstract

Add an XDR collector profile to define the type of data to collect from a Linux or Windows platform.

You can add XDR collector profiles that define the type of data that is collected from Linux or Windows platforms.

2.2.1 | Add an XDR Collector profile for Windows

Abstract

Add a Cortex XDR Collector profile, which defines the data that is collected from a Windows collector machine, and defines automatic XDR Collector upgrade settings.

> **NOTE:**
>
> Ingestion of log events larger than 5 MB is not supported.

XDR Collector profiles define the data that is collected from a Windows collector machine, and define automatic upgrade settings for the XDR collector. For Windows, you can configure a Filebeat profile, a Winlogbeat profile, and a Settings profile.

The Filebeat and Winlogbeat profiles use configuration files in YAML format. To facilitate the configuration of the YAML file, you can use out-of-the-box collection templates and templates added by the content packs installed from the XSIAM Marketplace. Templates save you time, and don't require previous knowledge of configuration file generation. You can edit and combine the provided templates, and you can add your own collection settings to the configuration file.

- Use an XDR Collector Windows Filebeat profile to collect file and log data using the Elasticsearch Filebeat default configuration file, called `filebeat.yml`.

  Cortex XSIAM supports using Filebeat version 8.15 with the operating systems listed in the Elasticsearch support matrix that conform with the collector machine operating systems supported by Cortex XSIAM. Cortex XSIAM supports the input types and modules available in Elasticsearch Filebeat.

  > **NOTE:**
  >
  > - Fileset validation is enforced. You must enable at least one fileset in the module, because filesets are disabled by default.
  > - Cortex XSIAM collects all logs in either an uncompressed JSON or text format. Compressed files, such as the gzip format, are not supported.
  > - Cortex XSIAM supports logs in single line format or multiline format. For more information about handling messages that span multiple lines of text in Elasticsearch Filebeat, see Manage Multiline Messages.

  Related Information

  - Elasticsearch Filebeat Overview Documentation
  - Configure Filebeat Inputs in Elasticsearch
  - Configure Filebeat Modules in Elasticsearch
  - Elasticsearch Support Matrix
  - XDR Collector machine requirements and supported operating systems
  - Collection of Windows DHCP logs and Windows DNS Debug logs:
    - Windows DHCP logs
    - Windows DNS Debug logs

- Use an XDR Collector Windows Winlogbeat profile to collect event log data, using the Elasticsearch Winlogbeat default configuration file, called `winlogbeat.yml`.

  Cortex XSIAM supports using Winlogbeat version 8.15 with the Windows versions listed in the Elasticsearch support matrix that conform with the collector machine operating systems supported by Cortex XSIAM. Cortex XSIAM supports the modules available in Elasticsearch Winlogbeat.

  After ingestion, Cortex XSIAM normalizes and saves the Windows event logs collected by the Winlogbeat profile in the dataset `xdr_data`. The normalized logs are also saved in a unified format in `<vendor>_<product>_raw` if the product and vendor are defined, and otherwise, in `microsoft_windows_raw`. You can search the data using Cortex Query Language XQL queries, build correlation rules, and generate dashboards based on the data.

  Related information

    - Elasticsearch Winlogbeat Overview Documentation
    - Winlogbeat Modules in ElasticSearch
    - Elasticsearch Support Matrix
    - Cortex XSIAM, see XDR Collector machine requirements and supported operating systems

- Use an XDR Collector Settings profile to configure automatic upgrade settings for XDR Collector releases.

To map your XDR Collector profile to a collector machine, you must use an XDR Collector policy. After you have created your profile, map it to a new or existing policy.

How to configure XDR Collector profiles

Filebeat profile

In the Filebeat Configuration File editor, you can define the data collection for your Elasticsearch Filebeat configuration file called `filebeat.yml`.

Cortex XSIAM provides YAML templates for DHCP, DNS, IIS, XDR Collector Logs, NGINX, and any templates added by the content packs installed from the XSIAM Marketplace.

1. In Cortex XSIAM, select Settings → Configurations → XDR Collectors → Profiles → +Add Profile → Windows.

2. Select Filebeat, then click Next.

3. Configure the General Information parameters.

    - Profile Name: Enter a unique name to identify the profile. The name can contain only letters, numbers, or spaces, and must be no more than 30 characters. The name that you enter here will be displayed in the list of profiles when you configure a policy.

    - (Optional) Add description here: To provide additional context for the purpose or business reason for your new profile, enter a profile description.

4. In the Filebeat Configuration File editing box, type or paste the contents of your configuration file, or use a template. To add a template, select one from the list, and click Add.

5. Cortex XSIAM supports all sections in the `filebeat.yml` configuration file, such as support for Filebeat fields and tags. You can use the "Add fields" processor to identify the product/vendor for the data collected by the XDR Collectors, so that the collected events go through the ingestion flow (Parsing Rules). To configure the product/vendor, ensure that you use the default `fields` attribute (do not use the target attribute), as shown in the following example:

```
processors:
  - add_fields:
      fields:
        vendor: <Vendor>
        product: <Product>
```

For more information about the "Add fields" processor, see Add_fields.

6. To finish creating your new profile, click Create.

   Your new profile will be listed under the applicable platform on the XDR Collectors Profiles page.

7. Apply profiles to XDR Collector machine policies by performing one of the following:

   - Right-click a profile, and select Create a new policy rule using this profile.

   - Launch the new policy wizard from XDR Collectors → Policies → XDR Collectors Policies.

Winlogbeat profile

In the Winlogbeat Configuration File editor, you can define the data collection for your Elasticsearch Winlogbeat configuration file called `winlogbeat.yml`.

Cortex XSIAM provides YAML templates for Windows Security, and any templates added by the content packs installed from the XSIAM Marketplace. To add a template, select it and click Add.

1. In Cortex XSIAM, select Settings → Configurations → XDR Collectors → Profiles → +Add Profile → Windows.

2. Select Winlogbeat profile, then click Next.

3. Configure the General Information parameters.

   - Profile Name: Enter a unique name to identify the profile. The name can contain only letters, numbers, or spaces, and must be no more than 30 characters. The name that you enter here will be displayed in the list of profiles when you configure a policy.

   - (Optional) Add description here: To provide additional context for the purpose or business reason for your new profile, enter a profile description.

4. In the Winlogbeat Configuration File editing box, type or paste the contents of your configuration file, or use the template. To add the template, click Select template, and then click Windows Security. Click Add.

5. Cortex XSIAM supports all sections in the `winlogbeat.yml` configuration file, such as support for Winlogbeat fields and tags. You can use the "Add fields" processor to identify the product/vendor for the data collected by the XDR Collectors, so that the collected events go through the ingestion flow (Parsing Rules). To configure the product/vendor, ensure that you use the default `fields` attribute (do not use the `target` attribute), as shown in the following example:

```
processors:
  - add_fields:
```

```
fields:
  vendor: <Vendor>
  product: <Product>
```

For more information about the "Add fields" processor, see Add_fields.

6. To finish creating your new profile, click Create.

   Your new profile will be listed under the applicable platform on the XDR Collectors Profiles page.

7. Apply profiles to XDR Collector machine policies by performing one of the following:

   - Right-click a profile, and select Create a new policy rule using this profile.

   - Launch the new policy wizard from XDR Collectors → Policies → XDR Collectors Policies.

Settings profile

You can configure automatic upgrades for XDR Collector releases. By default, this is disabled, and the Use Default (Disabled) option is selected. To implement automatic upgrades, follow these steps:

1. In Cortex XSIAM, select Settings → Configurations → XDR Collectors → Profiles → +Add Profile → Windows.

2. Select Settings profile, then click Next.

3. Configure the General Information parameters.

   - Profile Name: Enter a unique name to identify the profile. The name can contain only letters, numbers, or spaces, and must be no more than 30 characters. The name that you enter here will be displayed in the list of profiles when you configure a policy.

   - (Optional) Add description here: To provide additional context for the purpose or business reason for your new profile, enter a profile description.

4. Clear the Use Default (Disabled) checkbox.

5. For Collector Auto-Upgrade, select Enabled.

   Additional fields are displayed for defining the scope of the automatic upgrade.

6. Configure the scope of automatic upgrades:

- To ensure the latest XDR Collector release is used, leave the Use Default (Latest collector release) checkbox selected.
- To configure only a particular scope, perform the following steps:
    a. Clear the Use Default (Latest collector release) checkbox.

    b. For Auto Upgrade Scope, select one of the following options:

Option	**More Details**
Latest collector release	Configures the scope of the automatic upgrade to whenever a new XDR Collector release is available including maintenance releases and new features.
Only maintenance release	Configures the scope of the automatic upgrade to whenever a new XDR Collector maintenance release is available.
Only maintenance releases in a specific version	Configures the scope of the automatic upgrade to whenever a new XDR Collector maintenance release is available for a specific version. When this option is selected, you can select the specific Release Version.

7. To finish creating your new profile, click Create.

   Your new profile will be listed under the applicable platform on the XDR Collectors Profiles page.

8. Apply profiles to XDR Collector machine policies by performing one of the following:
    - Right-click a profile, and select Create a new policy rule using this profile.
    - Launch the new policy wizard from XDR Collectors → Policies → XDR Collectors Policies.

Additional XDR Collector profile management options

As needed, you can return to the XDR Collectors Profiles page to manage your XDR Collectors profiles. To manage a specific profile, right-click anywhere in an XDR Collector profile row, and select the desired action:

Option	More Details
Edit	Lets you edit the XDR Collector profile
Save As New	Copies the existing profile with its current settings, so that you can make modifications, and save it as a new profile with a unique name
Delete	Deletes the XDR Collector profile
View Collector Policies	Opens a new tab that displays the XDR Collectors Policies page, showing the policies that are currently associated with your XDR Collector profiles
Copy text to clipboard	Copies the text from a specific field in the row of a XDR Collector profile
Copy entire row	Copies the text from the entire row of a XDR Collector profile

2.2.1.1 | Ingest logs from Windows DHCP using Elasticsearch Filebeat

Abstract

Learn how to configure Cortex XSIAM to receive Windows DHCP logs.

You can extend visibility into logs from Windows DHCP, and enrich network logs with Windows DHCP data by using one of the following data collectors with Elasticsearch Filebeat :

- XDR Collector profile (recommended)
- Windows DHCP collector

When Cortex XSIAM begins receiving logs, it automatically creates a Windows DHCP dataset (`microsoft_dhcp_raw`). Cortex XSIAM uses Windows DHCP logs to enrich your network logs with hostnames and MAC addresses. Using XQL Search, you will be able to search for these items in the `microsoft_dhcp_raw` dataset.

> **NOTE:**
>
> Although this enrichment is available when configuring a Windows DHCP collector for a cloud data collection integration, we recommend configuring Cortex XSIAM to receive Windows DHCP

> logs with an XDR Collector Windows Filebeat profile, because it is simpler to set up.

Related information

- For more information about configuring the `filebeat.yml` file, see Elasticsearch Filebeat documentation.

Ingest Windows DHCP Logs with an XDR Collector Profile

When you add an XDR Collector Windows Filebeat profile using the Elasticsearch Filebeat default configuration file, called `filebeat.yml`, you can define whether the collected data undergoes follow-up processing in the backend for Windows DHCP data. You can further enrich network logs with Windows DHCP data by setting `vendor` to `“microsoft”`, and `product` to `“dhcp”` in the `filebeat.yml` file.

> **NOTE:**
>
> Configuration activities include editing the `filebeat.yml` file. To avoid formatting issues in this file, use the template provided by Cortex XSIAM to make your customizations. We recommend that you edit the file inside the user interface, instead of copying it and editing it elsewhere. Validate the syntax of the YML file before you finish creating your profile.

Configure Cortex XSIAM to receive logs from Windows DHCP using an XDR Collector Windows Filebeat profile:

1. In Cortex XSIAM, select Settings → Configurations → XDR Collectors → Profiles → +Add Profile → Windows.

2. Select Filebeat, then click Next.

3. Configure the General Information parameters:

   - Profile Name: Enter a unique name to identify the profile. The name can contain only letters, numbers, or spaces, and must be no more than 30 characters. The name that you enter here will be displayed in the list of profiles when you configure a policy.

   - (Optional) Add description here: To provide additional context for the purpose or business reason for your new profile, enter a profile description.

4. In the Filebeat Configuration File editing box, select the DHCP template, and click Add.

   The template's content is displayed in the editing area.

5. Edit the template text as necessary for your system.

6. To finish creating your new profile, click Create.

   Your new profile will be listed under the applicable platform on the XDR Collectors Profiles page.

7. Apply profiles to XDR Collector machine policies by performing one of the following:

- Right-click a profile, and select Create a new policy rule using this profile.
- Launch the new policy wizard from XDR Collectors → Policies → XDR Collectors Policies.

Ingest Windows DHCP Logs with the Windows DHCP Collector

To receive Windows DHCP logs with this collector, you must configure data collection from Windows DHCP via Elasticsearch Filebeat. This is configured by setting up a Windows DHCP Collector in Cortex XSIAM and installing and configuring an Elasticsearch Filebeat agent on your Windows DHCP Server. Cortex XSIAM supports using Filebeat up to version 8.0.1 with the Windows DHCP Collector.

Certain settings in the Elasticsearch Filebeat default configuration file called `filebeat.yml` must be populated with values provided when you configure the Data Sources settings in Cortex XSIAM for the Windows DHCP Collector. To help you configure the `filebeat.yml` file correctly, Cortex XSIAM provides an example file that you can download and customize. After you set up collection integration, Cortex XSIAM begins receiving new logs and data from the source.

Windows DHCP logs are stored as CSV (comma-separated values) log files. The logs rotate by days (`DhcpSrvLog-<day>.log`), and each file contains two sections: `Event ID Meaning`, and the events list.

> **NOTE:**
>
> Configuration activities include editing the `filebeat.yml` file. To avoid formatting issues in this file, use the example file provided by Cortex XSIAM to make your customizations. Do not copy and paste the code syntax examples provided later in this procedure into your `filebeat.yml` file. Validate the syntax of the YML file before you finish creating your profile.

Configure Cortex XSIAM to receive logs from Windows DHCP via Elasticsearch Filebeat with the Windows DHCP collector:

1. In Cortex XSIAM, configure the Windows DHCP Collector.

   a. Select Settings → Data Sources.

   b. Click Add Instance to begin a new configuration.

   c. Search for `Windows DHCP`.

   d. In the Windows DHCP collector box, click Connect.

      The Enable Windows DHCP Log Collection dialog box is displayed.

   e. (Optional, but recommended) Download the example `filebeat.yml` file.

      To help you configure your `filebeat.yml` file correctly, Cortex XSIAM provides an example `filebeat.yml` file that you can download and customize. To download this file, click the filebeat.yml link provided in this dialog box.

f. In the Name field, specify a descriptive name for your log collection configuration.

g. Click Save & Generate Token. A key is displayed.

Click the copy icon next to the key, and save the copy somewhere safe. You will need to provide this key when you set the `api_key` value in the Elasticsearch Output section in the `filebeat.yml` file, as explained in Step #2. If you forget to record the key and close the window, you will need to generate a new key and repeat this process.

h. Click Done to close the dialog box.

i. Expand the Windows DHCP collector that you just created. Click the Copy api url icon, and save the copy somewhere safe. You will need to provide this URL when you set the `hosts` value in the Elasticsearch Output section in the `filebeat.yml` file, as explained in Step #2.

2. On your Windows DHCP Server, configure an Elasticsearch Filebeat agent.

a. Navigate to the Elasticsearch Filebeat installation directory, and open the `filebeat.yml` file to configure data collection with Cortex XSIAM. We recommend that you use the download example file provided by Cortex XSIAM.

b. Update the following sections and tags in the `filebeat.yml` file. The following code examples detail the specific sections to make these changes in the file.

- Filebeat inputs: Define the paths to crawl and fetch. The code in the example below shows how to configure the Filebeat inputs section in the `filebeat.yml` file with these paths configured.

  Example 150. Example

  ```
  # ============================== Filebeat inputs ===============================
  filebeat.inputs:
    # Each - is an input. Most options can be set at the input level, so
    # you can use different inputs for various configurations.
    # Below are the input specific configurations.
    - type: log
      # Change to true to enable this input configuration.
      enabled: true
      # Paths that should be crawled and fetched. Glob based paths.
      paths:
        - c:\Windows\System32\dhcp\DhcpSrvLog*.log
  ```

- Elasticsearch Output: Set the `hosts` and `api_key`, where both of these values were obtained when you configured the Windows DHCP Collector in Cortex XSIAM, as explained in Step #1. The following code example shows how to configure the Elasticsearch Output section in the `filebeat.yml` file, and indicates which settings need to be obtained from Cortex XSIAM.

  Example 151. Example

  ```
  # ---------------------------- Elasticsearch Output ----------------------------
  output.elasticsearch:
    enabled: true
    # Array of hosts to connect to.
    hosts: ["OBTAIN THIS URL FROM CORTEX XDR"]
    # Protocol - either `http` (default) or `https`.
    protocol: "https"
    compression_level: 5
    # Authentication credentials - either API key or username/password.
    api_key: "OBTAIN THIS KEY FROM CORTEX XDR"
  ```

- Processors: Set the `tokenizer` and add a `drop_event processor` to drop all events that do not start with an event ID. The code in the example below shows how to configure the Processors section in the `filebeat.yml` file and indicates which settings need to be obtained from Cortex XSIAM.

  > **NOTE:**
  >
  > The `tokenizer` definition is dependent on the Windows server version that you are using, because the log format differs.

> - For platforms earlier than Windows Server 2008, use "`%{id},%{date},%{time},%{description},%{ipAddress},%{hostName},%{macAddress}`"
>
> - For Windows Server 2008 and 2008 R2, use "`%{id},%{date},%{time},%{description},%{ipAddress},%{hostName},%{macAddress},%{userName},%{transactionID},%{qResult},%{probationTime},%{correlationID}`"
>
> - For Windows Server 2012 and later, use "`%{id},%{date},%{time},%{description},%{ipAddress},%{hostName},%{macAddress},%{userName},%{transactionID},%{qResult},%{probationTime},%{correlationID},%{dhcid},%{vendorClassHex},%{vendorClassASCII},%{userClassHex},%{userClassASCII},%{relayAgentInformation},%{dnsRegError}`"

Example 152. Example

```
# ================================= Processors =================================
processors:
  - add_host_metadata:
    when.not.contains.tags: forwarded
  - drop_event.when.not.regexp.message: "^[0-9]+,.*"
  - dissect:
    tokenizer: "%{id},%{date},%{time},%{description},%{ipAddress},%{hostName},%
{macAddress},%{userName},%{transactionID},%{qResult},%{probationTime},%{correlationID},%
{dhcid},%{vendorClassHex},%{vendorClassASCII},%{userClassHex},%{userClassASCII},%
{relayAgentInformation},%{dnsRegError}"
  - drop_fields:
    fields: ["message"]
  - add_locale: ~
  - rename:
      fields:
        - from: "event.timezone"
          to: "dissect.timezone"
      ignore_missing: true
      fail_on_error: false
  - add_cloud_metadata: ~
  - add_docker_metadata: ~
  - add_kubernetes_metadata: ~
```

3. Verify the status of the integration.

   Return to the integrations page in Cortex XSIAM, and view the statistics for the log collection configuration.

4. After Cortex XSIAM begins receiving logs from Windows DHCP via Elasticsearch Filebeat, you can use XQL Search to search for logs in the new `microsoft_dhcp_raw` dataset.

2.2.1.2 | Ingest Windows DNS debug logs using Elasticsearch Filebeat

Abstract

Extend Cortex XSIAM visibility into Windows DNS Debug logs using Elasticsearch Filebeat with an XDR Collectors profile.

Extend Cortex XSIAM visibility into Windows DNS Debug logs using an XDR Collector Windows Filebeat profile.

During configuration of an XDR Collector Windows Filebeat profile, you can configure the profile to enrich network logs with Windows DNS Debug log data. You do this by editing the Elasticsearch Filebeat default configuration file called `filebeat.yml`. In this file, you can define whether the collected data undergoes follow-up processing in the backend for Windows DNS Debug log data. Cortex XSIAM uses Windows DNS Debug logs to enrich network logs. These logs can be searched, using XQL Search. You can search the Windows DNS Debug Cortex Query Language dataset (`microsoft_dns_raw`) for raw data, and the normalized stories using the `xdr_data` dataset with the preset called `network_story`.

1. Enable DNS debug logging in your Windows DNS server settings:

    a. In Windows, open DNS Manager, right-click your Windows DNS Server, and select Properties.

    b. Select Debug Logging → Log packets for debugging, and keep the settings that are automatically configured for collecting regular Windows DNS logs in the Packet direction and Packet contents sections.

    c. (Optional) To collect detailed Windows DNS logs, under the Other options section, select Details.

    > **NOTE:**
    >
    > Detailed logs are significantly larger, because more information is added to the logs.

    d. In the Log file section, for File path and name , enter the file path and log name of your Windows DNS logs, such as `c:\Windows\System32\dns\DNS.log`. This path will also be configured in your `filebeat.yml` file, as explained in a later step (see Example 153, “Example”).

    e. Click OK.

2. In Cortex XSIAM, go to Settings → Configurations → XDR Collectors → Profiles → +Add Profile → Windows.

3. Select Filebeat, then click Next.

4. Configure the General Information parameters:

   - Profile Name: Enter a unique name to identify the profile. The name can contain only letters, numbers, or spaces, and must be no more than 30 characters. The name that you enter here will be displayed in the list of profiles when you configure a policy.

   - (Optional) Add description here: To provide additional context for the purpose or business reason for your new profile, enter a profile description.

5. In the Filebeat Configuration File editing box, select the DNS template of your choice (detailed, or non-detailed). If you configured detailed collection in the Windows DNS Manager, select the detailed DNS template here. Click Add.

   The template's content is displayed in the editing area.

6. Configure the `filebeat.yml` file to collect Windows DNS Debug log data.

   a. In the `filebeat.inputs:` section of the file, for `paths:`, configure the file path to your Windows DNS Debug logs. This file path must be the same as the one configured in your Windows DNS server settings, as explained in an earlier step.

   b. Set `vendor` to “`microsoft`” and `product` to “`dns`”.

   The following examples show how to configure the `filebeat.yml` file to normalize Windows DNS Debug logs with an XDR Collector.

   > **NOTE:**
   >
   > To avoid formatting issues in your `filebeat.yml` file, we recommend that you validate the syntax of the file.

   Example 153. Example

   Example for non-detailed (regular) Windows DNS log collection:

```
filebeat.inputs:
- type: filestream
  enabled: true
  paths:
    -  c:\Windows\System32\dns\DNS.log
  processors:
    - add_fields:
        fields:
          vendor: "microsoft"
          product: "dns"
```

   Example 154. Example

   Example for detailed Windows DNS log collection:

```
filebeat.inputs:
- type: log
  enabled: true
  paths:
    -  c:\Windows\System32\dns\DNS.log
  multiline.type: pattern
  multiline.pattern: '^(?:\d{1,2}\/){2}\d{4}\s(?:\d{1,2}\:){2}\d\d\s(?:AM|PM)'
  multiline.negate: true
  multiline.match: after
  processors:
    - add_fields:
        fields:
          vendor: "microsoft"
          product: "dns"
```

7. To finish creating your new profile, click Create.

   Your new profile will be listed under the applicable platform on the XDR Collectors Profiles page.

8. Apply profiles to XDR Collector machine policies by performing one of the following:

   - Right-click a profile, and select Create a new policy rule using this profile.

   - Launch the new policy wizard from XDR Collectors → Policies → XDR Collectors Policies.

2.2.2 | Add an XDR Collector profile for Linux

Abstract

Add a Cortex XDR Collector profile, which defines the data that is collected from a Linux collector machine, and defines automatic XDR Collector upgrade settings.

> **NOTE:**
>
> Ingestion of log events larger than 5 MB is not supported.

An XDR Collector Linux profile defines the data that is collected from a Linux collector machine. For Linux, you can configure a Filebeat profile and a Settings profile.

The Filebeat profile uses a configuration file in YAML format. To facilitate the configuration of the YAML file, you can use out-of-the-box collection templates, and templates added by the content packs installed from the XSIAM Marketplace. Templates save you time, and don't require previous knowledge of configuration file generation. You can edit and combine the provided templates, and you can add your own collection settings to the configuration file.

- Use an XDR Collector Linux Filebeat profile to collect file and log data using the Elasticsearch Filebeat default configuration file, called `filebeat.yml`.

  Cortex XSIAM supports using Filebeat version 8.15 with the operating systems listed in the Elasticsearch Support Matrix that conform with the collector machine operating systems supported by Cortex XSIAM. Cortex XSIAM supports the input types and modules available in Elasticsearch Filebeat.

  > **NOTE:**
  >
  > - Fileset validation is enforced. You must enable at least one fileset in the module, because filesets are disabled by default.
  > - Cortex XSIAM collects all logs in either an uncompressed JSON or text format. Compressed files, such as the gzip format, are not supported.
  > - Cortex XSIAM supports logs in single line format or multiline format. For more information about handling messages that span multiple lines of text in Elasticsearch Filebeat, see Manage Multiline Messages.

  Related Information

  - Elasticsearch Filebeat Overview Documentation
  - Configure Filebeat Inputs in Elasticsearch
  - Configure Filebeat Modules in Elasticsearch
  - Elasticsearch Support Matrix
  - XDR Collector machine requirements and supported operating systems

- Use an XDR Collector Settings profile to configure automatic upgrade settings for XDR Collector releases.

To map your XDR Collector profile to a collector machine, you must use an XDR Collector policy. After you have created your profile, map it to a new or existing policy.

How to configure XDR Collector profiles

Filebeat profile

In the Filebeat Configuration File editor, you can define the data collection for your Elasticsearch Filebeat configuration file called `filebeat.yml`.

Cortex XSIAM provides YAML templates for XDR Collector Logs, Linux (RHEL/CentOS), NGINX (Linux), Linux (Debian/Ubuntu), and any templates added by the content packs installed from the XSIAM Marketplace.

1. In Cortex XSIAM, select Settings → Configurations → XDR Collectors → Profiles → +Add Profile → Linux.
2. Select Filebeat, then click Next.

3. Configure the General Information parameters.

    - Profile Name: Enter a unique name to identify the profile. The name can contain only letters, numbers, or spaces, and must be no more than 30 characters. The name that you enter here will be displayed in the list of profiles when you configure a policy.

    - (Optional) Add description here: To provide additional context for the purpose or business reason for your new profile, enter a profile description.

4. In the Filebeat Configuration File editing box, type or paste the contents of your configuration file, or use a template. To add a template, select one from the list, and click Add.

5. Cortex XSIAM supports all sections in the `filebeat.yml` configuration file, such as support for Filebeat fields and tags. You can use the "Add fields" processor to identify the product/vendor for the data collected by the XDR Collectors, so that the collected events go through the ingestion flow (Parsing Rules). To configure the product/vendor, ensure that you use the default `fields` attribute (do not use the target attribute), as shown in the following example:

    ```
    processors:
      - add_fields:
          fields:
            vendor: <Vendor>
            product: <Product>
    ```

    For more information about the "Add fields" processor, see Add_fields.

6. To finish creating your new profile, click Create.

    Your new profile will be listed under the applicable platform on the XDR Collectors Profiles page.

7. Apply profiles to XDR Collector machine policies by performing one of the following:

    - Right-click a profile, and select Create a new policy rule using this profile.

    - Launch the new policy wizard from XDR Collectors → Policies → XDR Collectors Policies.

Settings profile

You can configure automatic upgrades for XDR Collector releases. By default, this is disabled, and the Use Default (Disabled) option is selected. To implement automatic upgrades, follow these steps:

1. In Cortex XSIAM, select Settings → Configurations → XDR Collectors → Profiles → +Add Profile → Linux.

2. Select Settings profile, then click Next.

3. Configure the General Information parameters.

- Profile Name: Enter a unique name to identify the profile. The name can contain only letters, numbers, or spaces, and must be no more than 30 characters. The name that you enter here will be displayed in the list of profiles when you configure a policy.
- (Optional) Add description here: To provide additional context for the purpose or business reason for your new profile, enter a profile description.

4. Clear the Use Default (Disabled) checkbox.
5. For Collector Auto-Upgrade, select Enabled.

   Additional fields are displayed for defining the scope of the automatic upgrade.

6. Configure the scope of automatic upgrades:
   - To ensure the latest XDR Collector release is used, leave the Use Default (Latest collector release) checkbox selected.
   - To configure only a particular scope, perform the following steps:
     a. Clear the Use Default (Latest collector release) checkbox.

     b. For Auto Upgrade Scope, select one of the following options:

Option	More Details
Latest collector release	Configures the scope of the automatic upgrade to whenever a new XDR Collector release is available including maintenance releases and new features.
Only maintenance release	Configures the scope of the automatic upgrade to whenever a new XDR Collector maintenance release is available.
Only maintenance releases in a specific version	Configures the scope of the automatic upgrade to whenever a new XDR Collector maintenance release is available for a specific version. When this option is selected, you can select the specific Release Version.

7. To finish creating your new profile, click Create.

   Your new profile will be listed under the applicable platform on the XDR Collectors Profiles page.

8. Apply profiles to XDR Collector machine policies by performing one of the following:
    - Right-click a profile, and select Create a new policy rule using this profile.
    - Launch the new policy wizard from XDR Collectors → Policies → XDR Collectors Policies.

Additional XDR Collector profile management options

As needed, you can return to the XDR Collectors Profiles page to manage your XDR Collectors profiles. To manage a specific profile, right click anywhere in an XDR Collector profile row, and select the desired action:

Option	More Details
Edit	Lets you edit the XDR Collector profile
Save As New	Copies the existing profile with its current settings, so that you can make modifications, and save it as a new profile with a unique name
Delete	Deletes the XDR Collector profile
View Collector Policies	Opens a new tab that displays the XDR Collectors Policies page, showing the policies that are currently associated with your XDR Collector profiles
Copy text to clipboard	Copies the text from a specific field in the row of a XDR Collector profile
Copy entire row	Copies the text from the entire row of a XDR Collector profile

2.3 | XDR Collector datasets

Abstract

After Cortex XSIAM begins receiving data from your XDR Collectors configuration, the app automatically creates an XQL dataset.

After Cortex XSIAM begins receiving data from your XDR Collectors configuration that are dedicated for on-premises data collection on Windows and Linux machines.

- For Filebeat, the app automatically creates an Cortex Query Language (XQL) dataset of event logs using the vendor name and the product name specified in the configuration file section of the Filebeat profile. The dataset name follows the format `<vendor>_<product>_raw`. If not specified, Cortex XSIAM automatically creates a new default dataset in the format `<module>_<module>_raw` or `<input>_<input>_raw`. For example, if you are using the NGINX module, the dataset is called `nginx_nginx_raw`.
- For Winlogbeat, the app automatically creates an XQL dataset of event logs using the vendor name and the product name specified in the configuration file section of the Winlogbeat profile. The dataset name follows the format `<vendor>_<product>_raw`. If not specified, Cortex XSIAM automatically creates a new default dataset, `microsoft_windows_raw`, for event log collection. Winlogbeat data is also normalized to `xdr_data` (and thus the `xdr_event_log` preset).

After Cortex XSIAM creates the dataset, you can search for your XDR Collector data using XQL Search.