

Getting Started with the Exalens Platform

Contents

Introduction	3
Platform Overview.....	3
Basic Connectivity Requirements	4
Exalens Host / Appliance Internet Access	4
“Air-Gapped” Exalens Deployments	4
Deployment Appliances	4
Installing Exalens Cortex as a Container	5
Prerequisites	5
Starting the Cortex Server	5
Accessing and Setting up the Cortex.....	6
Exalens Cortex UI First Login	6
Installing the Exalens License.....	6
Stopping and Starting the Cortex.....	7
Updating the Cortex	7
Reinstalling the Cortex (Factory Reset)	8
On Windows:.....	8
Changing the Cortex Web UI HTTPS Certificate	8
Backing Up Cortex Configurations and Data	10
Setting up and Configuring the Data Collector Probe (DCP).....	11
Configuring and Registering a DCP Virtual/Hardware appliance with a Cortex.....	11
Stopping the DCP Appliance	13
Updating the DCP	13
Reinstalling the DCP (Factory Reset).....	15
On Windows:.....	16
Deleting a DCP from the Cortex	16
Backing Up DCP Configurations and Data	16
Troubleshooting Data Collector Probe Connectivity	16
Failed Update via Cortex Web UI	17
Network Service Ports and Firewall Rules.....	17
Inbound Connectivity	17
Outbound Connectivity.....	17
Default Appliance User Credentials	17
Support Contact Information	17

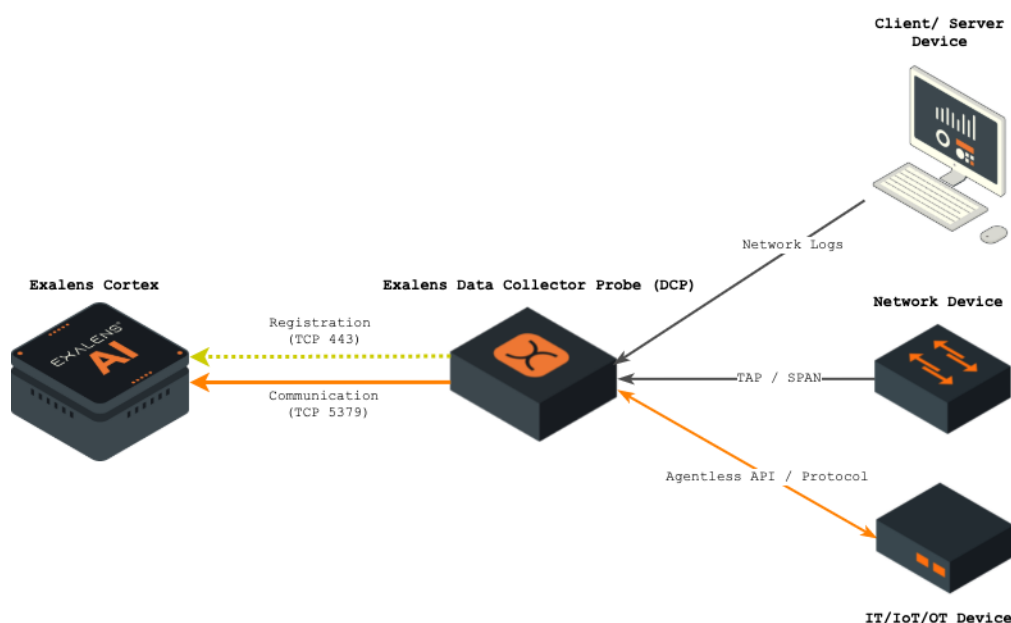
Introduction

The guide will provide basic information on how to get started on setting up the Exalens platform. This guide covers the basic deployment, network initial configuration requirements and settings. The guide is intended for and applicable to all platform deployment methods (On-premises, Cloud, Hybrid, Physical/Virtual appliances, etc.) based deployments, whether deployment is implemented by customers or partners.

This guide should be used in combination with other deployment guides which can be found on the Exalens website under the support section: <https://exalens.com/resources/resource-centre>.

Platform Overview

The following diagram provides a visual overview of a basic Exalens platform deployment, consisting of a single Exalens Cortex and a single Exalens Data Collector Probe (DCP). The Exalens Cortex is the central data analysis and AI component of the Exalens platform. The Cortex is the primary interface for end users, providing a Web-based UI for logging in and interacting with the Exalens platform. The DCP is primarily the data acquisition component of the Exalens platform that uses agentless methods to collect network, endpoint, and process data from systems in the deployment environment. For example, the DCP can passively capture network traffic data using a TAP or port mirroring (i.e., SPAN) on a network device, or directly via monitoring a network interface if deployed on an endpoint host. It can also monitor network, host, machine and process analytics from OT/IoT/IT devices by connecting to them via agentless APIs and Protocols commonly used by Controllers, Gateways, SCADA Servers and Data Historians (such as OPC-UA, MQTT, SNMP, MTconnect, etc.). The DCP also carries out initial data parsing, normalisation, analytics, before forwarding enriched log data to the Exalens Cortex for analysis. The DCP may also be configured to perform distributed functions (Note that this functionality is not enabled in the Exalens Community Edition).



Basic Connectivity Requirements

Exalens platform deployment consists of a single Cortex server appliance connected to one or more DCPs. DCPs can only be connected to a single Cortex at a time and cannot be transferred to another Cortex without resetting their monitoring configurations. The Exalens platform uses several TCP/UDP ports for different communication purposes. DCPs communicate to Cortex appliances on TCP port 443 (HTTPS) for initial DCP to Cortex registration and configuration, and then, following successful registration and configuration, on TCP 5379 (TLS connection) for all further communication. Communication between the Cortex and DCP is initiated outbound from the DCP to the Cortex. There is no requirement for the Cortex to have direct inbound connectivity to a DCP, as all configuration communication issued from the Cortex to the DCP is retrieved by the DCP automatically via continuous call home functionality over TLS encrypted connections on TCP 5379.

Exalens Host / Appliance Internet Access

As the Exalens platform is a monitoring and security infrastructure platform, by default, it is recommended that Exalens appliances, or hosts running the Exalens platform are blocked from Internet access. Where required, inbound Internet access to Exalens appliances should only be granted from trusted authenticated sources and systems.

The Exalens platform requires Internet connectivity to automatically update software for normal operation. The Exalens platform requires Internet DNS access to resolve the IP addresses of external system hostnames for these requests. Both Public DNS servers on the Internet or internal DNS servers may be used.

“Air-Gapped” Exalens Deployments

In some organisations there may be a requirement to deploy the Exalens platform in a network that has restricted or no external network connectivity. The Exalens platform can be deployed with these “air-gapped” configurations, however, there are some limitations. In fully air gapped environments, where there is no Internet access, manual updates of Cortex and DCP appliances are required. To support manual updates of your Exalens appliance, you must contact the Exalens support team (See “Support Contact Information”) to receive offline updates and setup offline update functionality. Contacting Exalens support team is also required when performing an “offline” installation, so that offline image files can be supplied as part of the initial installation process.

Deployment Appliances

Exalens Cortex and DCPs can be deployed as a hardware or virtual appliance (i.e., Cortex and DCP installed on the same appliance host), or as separate appliances (i.e., Cortex or DCP installed on separate appliance hosts). Both the Cortex and DCP can also be supplied as Docker Containers (Note that this is the deployment method used for installing the Exalens Community Edition – it also provides greater flexibility in deployment operating system and host machine). Exalens Cortex and DCP Virtual and Hardware appliances are deployed on security hardened operating system images of Ubuntu LTS Linux maintained by Exalens. Whilst end users have the option to routinely update their appliance’s operating system image using the Internet or offline software packages, Exalens may issue notices and guidance at different times for critical operating system and software patches that have been released, as well recommendations on update paths for different operating system patches and Exalens Cortex and Probe software updates to prevent compatibility issues when performing system updates. Update guidance is provided in Exalens software release

notes and is published alongside support articles and other documentation on the Exalens website under: <https://exalens.com/resources/resource-centre>

A Virtual, Hardware appliance or container role can be selected by the user to be configured as a Cortex, as a DCP, or both. This requires that both the Cortex and DCP software is preinstalled on the appliance beforehand. When applying different roles, care should be taken to make sure the necessary system specifications can support these respective roles during deployment. Dedicated appliances or containers may come with specific resource specifications and limitations, with preinstalled Cortex or DCP software. In this case, it is possible to choose different roles, but depending on the deployment host resource limitations, certain roles may not be recommended and should be avoided (e.g., Cortex / Cortex + DCP). Moreover, a specific appliance may be preconfigured with a Cortex or DCP role. In these cases, it may not be possible to choose or change appliance role. For example, the Exalens Community Edition container comes preconfigured with the Cortex and DCP role. For support in selecting Cortex / DCP roles for a deployment system contact Exalens Support Team for further information.

Installing Exalens Cortex as a Container

This section will provide an overview of how-to setup Exalens Cortex using a container deployment method. This section can be skipped if you are deploying Exalens Virtual or Hardware appliances, as these appliances are preconfigured with Cortex and DCP roles.

On first launch, it will check Docker is installed, and then download the required Exalens Platform Docker images from Docker Hub. Once this is completed, the Exalens Cortex will automatically start. Note that the Cortex has a default DCP installed on the same host system as part of its automatic deployment that can be disabled later in the Cortex UI where required.

Prerequisites

Before starting, ensure you have the Docker installed on your host operating system:

- Docker (see instructions here: <https://docs.docker.com/engine/install/>)
- *** For Ubuntu Distributions Only***: Execute the script "install_docker.sh" that comes prepackaged with the Container deployment files to auto install Docker.

Starting the Cortex Server

To the services on Linux, navigate to the folder where the Docker setup files are located (when using the Exalens Community Edition, this is under the cloned repository or downloaded and extracted ZIP folder).

For Linux hosts, use the following script by executing the following command:

```
./retina-cortex.sh --start
```

For Windows hosts, use the following script by executing the following command:

```
.\retina-cortex.bat --start
```

When running the "--start" command for the first time, it will download the required Docker Container images from Exalens' Docker Hub which can take a few minutes depending on

EXALENS®

the speed of Internet connection that is available to the host machine. Once the required images are downloaded the Cortex server will automatically start.

Accessing and Setting up the Cortex

This section will provide an overview of how-to setup the Exalens Cortex for first time use, including registering new DCPs.

Once the Exalens Cortex is started and the service is running, to access the Exalens Cortex web UI, open a web browser and navigate to:

`https://[HOST_ADDRESS]`

Replace [HOST_ADDRESS] with the IP address or DNS hostname of the host machine where the Exalens Cortex is running.

Exalens Cortex UI First Login

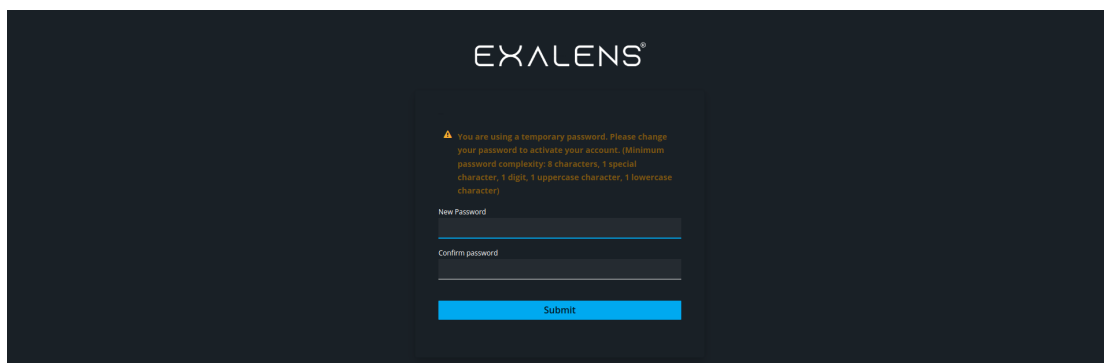
Upon first access to the Cortex UI, your browser may warn you about the security risk due to the use of a self-signed certificate. This is a common alert when using self-signed certificates. Please proceed by accepting the risk or adding an exception in your browser to continue. This process varies depending on the browser you are using. Once you proceed, the user login prompt for Exalens will appear.

Use the following default Exalens administrator user credentials to login:

Username: admin

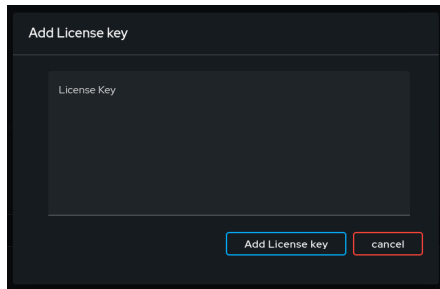
Password: @Dm1nadmin

A password change will be required at first logon (see below image), and after logging into the Exalens Cortex UI for the first time, the UI will prompt for a new password for the default administrator user account. This will change the password of the default administrative user. It recommended to change the default password to a suitable complex password. Multi-Factor Authentication can also be enabled for the default administrator account under “User Management”. Note that the Cortex Administrative user account is used for registering Exalens DCPs, therefore, the updated password should be used during DCP registration with the Cortex.



Installing the Exalens License

After logging into the Cortex UI and changing the default password, the UI will load the default dashboard and window popup prompting for a license key will appear (as shown in the image below). Note that the UI will not proceed beyond point without a valid license key, or Internet connectivity for the license to validate with Exalens license server(s).



Enter a valid license key supplied by the Exalens team and then accept the end-user license agreement and terms and conditions. Again, note the UI will not proceed beyond this point without accepting the agreement and terms and conditions.

Stopping and Starting the Cortex

To stop the Exalens Cortex this can be carried out both via the command line terminal or via the Cortex web UI. To stop the Cortex via the command line, use the retina-cortex script as before with the following command switch.

On Linux:

```
./retina-cortex.sh --stop
```

On Windows:

```
.\retina-cortex.bat --stop
```

To stop the Cortex via the web UI, navigate to top right of the user interface and select the username button to list system settings menu, and select the “Shutdown” menu option. Under this menu, the Cortex can also be restarted by selecting “Restart”

To restart the Cortex, this must be carried out via the command line console, by executing the following command.

On Linux:

```
./retina-cortex.sh --start
```

On Windows:

```
.\retina-cortex.bat --start
```

Updating the Cortex

To update the Exalens Cortex this can be carried out both via the command line terminal or via the Cortex web UI. To stop the Cortex via the command line, use the retina-cortex script as before with the following command switch.

On Linux:

```
./retina-cortex.sh --update
```

On Windows:

```
.\retina-cortex.bat -- update
```

To update the Cortex via the web UI, navigate to top right of the user interface and select the username button to list system settings menu, and select the “Update” menu option.

Reinstalling the Cortex (Factory Reset)

Normally factory resetting the Cortex software should not be required, however, under exceptional circumstances the Cortex software can be reinstalled to a “Factory Reset” state. This can be carried out by running a clean reinstall process.

First stop the Cortex and perform a factory reset reinstallation by executing the following commands.

On Linux:

```
./retina-cortex.sh --stop  
./retina-cortex.sh --clean-install
```

On Windows:

```
.\\retina-cortex.bat --stop  
\\.\\retina-cortex.bat --clean-install
```

Changing the Cortex Web UI HTTPS Certificate

By default, the Exalens Cortex Web UI uses self-signed certificates that will generate a certificate validation warning when accessed by a modern browser. This is because the browser cannot check the validity of the certificate as it has not been signed by a trusted certificate authority. A certificate validation warning may also be caused when there is a mismatch between the Cortex hostname and the subject name in the Cortex certificate. To remove these warnings, third party certificates can be installed by generating a certificate signing request (CSR) on the Exalens Cortex and sending this to a trusted third-party certificate authority to sign and return a valid certificate and keys.

The following instructions describe how to create a certificate signing request, and then replace existing certificates and keys in the Exalens Cortex with those provided by a third-party certificate authority on a host running a Linux operating system. The exact steps for this will be different for hosts running Windows operating systems. Note that it is planned in a future version to migrate this functionality to the Cortex UI for both Linux and Windows deployments.

To install a third-party certificate for use with the Exalens Cortex UI web server. The following actions should be completed (note the certificate key algorithm and key complexity may change from provided instructions based on third-party certificate signing requirements).

```
openssl req -new -newkey rsa:2048 -nodes -keyout mydomain.key -out mydomain.csr
```

A prompt to answer a series of questions will be generated - complete the required certificate sections as specified by the third-party certificate authority requirements (below

an explanation of each section is provided).

Country Name - This is the two-letter abbreviation for your country. For example, United States would be US and Great Britain would be GB.

State or Province Name - This is the full name of the state your organization operates from. For example, this might be "California" or "Michigan".

Locality Name - Name of the city your organization operates from. Examples might include "Lansing" or "Phoenix". Don't use abbreviations in this field. For example, "St. Helena" should be "Saint Helena"

Organization Name - The name of your organization. If you are a business, use must use your legal name. If you are applying as an individual, you use your full name instead.

Organizational Unit Name - If applying as a business, you can enter your "Doing Business As" (DBA) name here. Alternately, you can use a department name here. For example, "IT Department" or "Web Administration".

Common Name - The domain name that you are purchasing a SSL certificate for. This must be a fully qualified domain name (FQDN). An example might be mydomain.com.

Email Address - An email address that can be used as a point of contact for your domain. Be sure the address is valid.

Challenge password - An optional password to further secure your certificate. Be sure to remember this password if you choose to use it. It must be at least 4 characters long. You can skip this step if you like.

Company name - Another optional step. Fill in your company name if you wish. This is not required for web SSL certificates.

The CSR will now be generated within the local directory in which the request was made. Check the contents of your local working directory and validate that two new files ending with ".key" and ".csr" exist. Note that the key file should be kept private on your server as it will be to copy over existing private keys later. The .csr file is your certificate signing request and can be sent to a Certificate Authority. You can inspect the contents of the CSR by using the "cat" command. Here is an example of the CSR generated:

```
ls -ls
-rw-r--r--. 1 root root 1082 Jan 31 12:10 mydomain.csr
-rw-----. 1 root root 1704 Jan 31 12:10 mydomain.key
cat mydomain.csr
```

An example CSR output is shown below:

```
-----BEGIN CERTIFICATE REQUEST-----
JBgNVBAYTAITMRAwDgYDVQQIDAdBcmI6b25hMRAwMIIC5jCCAcCAQAwgaAxCzA
DgYDVQQHDAdQaG9lbml4MRswGQYDVQQKDBJNeSBBD2Vzb21lIENvbXBuYXkxJAU
BgNVBAsMDUIUIERlIGFydG1lbnQxFTATBgNVBAMMDG15ZG9tYWluLmNvbTEhMB8G
CSqGSIlb3DQGEJARYSYWRtaW5AbXlkb21haW4uY29tMIIBljANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAsNljF8u2vvTGisYStD/+4elnQnWIB30o38hWnF+bi6ZS
MmraeigL/HrSoKfUti/z96PVeK9CFo0AZ12Tq9lBzXtqxSjbolc9r9lZvrycrEYR
qsepF8M18Y0jyBfDzXIY13o5Sjnd4e0H7gZCldxy930Lj1JQC0o4XAbxHd8k7A3
976uh2r6MPdnnQ65UG2vKnMa1MGft9XTD6dQjj3ZpTqbdG4TnOPFIG4TNXu2zSYI
CX7XHjBKBGx5r/ohQBCqAYFpAMs/7E+gSbkK4jv9Mr8W1gC0CHSJkpT0tqcn+8Lj
1vMi3ysDed6bObC/OMBXAZY2lpALbHvny2NJP RPjwIDAQABoAAwDQYJKoZIhvcN
AQELBQADggEBABuUSRgBnv4R1k4UHGngmvQ63jjaZhO6URhQbFzb1e+XHeqou1F8
YSP17A8w23hLfXxs/NC0hQZan9cFbBGy6dajqMjsCF3timGXHitsmUyswpG3k+dl
```

```
bWlsRaJPMsOoz9Hcl7ztvN1zs6iiMCZkpI4G+9J5wBqddgXSH+/w5bCViqj0855O
APFUYUEFSB5jS5/e132F5zhcZV5vQ2bato8Zy58gzz5t+q5rn6uuzqc05kmBtDG8
B12RIUt2lBbl6sxQDKQbsM6snwn50H3Xszgn8kyR1VuXOqaKf1X1cCKRTSzyZtUp
FeKV0mMwoC9XxX6YCz8eQy66RMVSm3hGI2Y=
-----END CERTIFICATE REQUEST-----
```

The entire contents of the CSR file need to be copied (including “BEGIN CERTIFICATE REQUEST” and “END CERTIFICATE REQUEST”) and sent to a third-party Certificate Authority.

Once the signed certificate is received from the third-party certificate authority. They need to be copied over to Exalens Cortex Nginx and Keycloak directories.

The replacement certificates and key (generated by the CSR and stored locally on your machine in the same location as the CSR file) will replace existing ones used by Exalens Nginx and Keycloak. First backup the existing Nginx and Keycloak certificates in case of required regression. To backup the existing Certificate and Key Files for Nginx and Keycloak using the following commands:

```
sudo cp ~/.exalens/retinaCortex/conf/nginx/certs/sslCert.pem
/[BACKUP_PATH]/cert/sslCert.pem.bak

sudo cp ~/.exalens/retinaCortex/conf/nginx/certs/sslKey.pem
/[BACKUP_PATH]/cert/sslKey.pem.bak
```

Copy and rename the Certificate and Key Files to the Nginx and Keycloak directories:

```
sudo cp /[PATH_TO_NEW_CERT]/NewCert.pem
~/.exalens/retinaCortex/conf/nginx/certs/sslCert.pem

sudo cp /[PATH_TO_NEW_KEY]/NewPrivateKey.pem
~/.exalens/retinaCortex/conf/nginx/certs/sslKey.pem

sudo cp /[PATH_TO_NEW_CERT]/NewCert.pem
~/.exalens/retinaCortex/conf/keycloak/certs/sslCert.pem

sudo cp /[PATH_TO_NEW_KEY]/NewPrivateKey.pem
~/.exalens/retinaCortex/conf/keycloak/certs/sslKey.pem
```

Set the Certificate Permissions:

```
sudo chmod 655 ~/.exalens/retinaCortex/conf/nginx/certs/*
sudo chmod 655 ~/.exalens/retinaCortex/conf/keycloak/certs/*
```

Restart the Exalens Cortex using the following commands:

```
./retina-cortex.sh --stop
./retina-cortex.sh --start
```

The Exalens Cortex Web UI should now be using the newly installed certificate.

Backing Up Cortex Configurations and Data

It is recommended to periodically back up Cortex install and data in the event of a system fault requiring reinstallation, or before updating the Cortex version in case of a required regression to an earlier Cortex version.

To do this manually, first stop the Cortex with the following command.

In Linux:

```
./retina-cortex.sh --stop
```

In Windows:

```
./retina-cortex.bat --stop
```

Below are examples command to backup the Cortex to a local directory, or remotely via SCP (SSH) to a remote system.

Backup Cortex to a local directory:

```
cp -r ~/.exalens [DESTINATION_DIRECTORY_PATH]
```

Below is a command to backup the Cortex to a remote system via SCP (SSH):

```
scp -r ~/.exalens username@hostname:/path/to/remote
```

Depending on the host operating system being used (Linux / Windows), different backup options may be available. Backing up the Cortex preserves the Cortex data and instance configuration only, which can be reimported by copying ~/.exalens and overwriting existing the existing ~/.exalens directory.

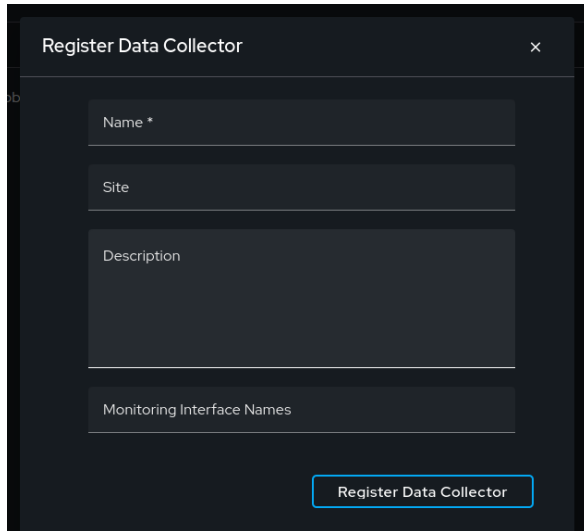
Setting up and Configuring the Data Collector Probe (DCP)

This section will provide an overview of how-to setup the Exalens DCP.

Configuring and Registering a DCP Virtual/Hardware appliance with a Cortex

*** Note that the Exalens Community Edition comes preinstalled with a DCP “CortexProbe” when deploying the Cortex Docker Container. Therefore, these configuration steps are not applicable to Exalens Community Edition installation and setup. ***

To register a new DCP with a Cortex, the DCP must be first registered via the Cortex UI under “System Administration – Data Collectors”. Select the “Register Data Collector” button and a pop-up UI window will appear requesting the user to provide the following information (see image below): DCP (Probe) Name, Site, and Description, and the name of any network interfaces on the host machine that should be used for passive network monitoring; it is important to provide the exact name of the interface name as shown on the host. Note that “Monitoring Interfaces Names” is only applicable to Docker Container installations, Virtual or Hardware appliances network monitoring interfaces are preconfigured. After completing the required input, click on the “Register Data Collector” button.



Register Data Collector

Name *

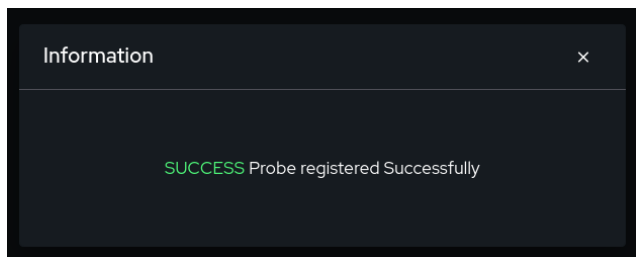
Site

Description

Monitoring Interface Names

Register Data Collector

When the DCP is registered with the Cortex will provide a prompt as shown below:



The registered DCP will then be added to the Data Collector list as shown:

Data Collectors						
Action	Name	CPU Usage	Memory Usage	Disk Usage	Last Activity (UTC)	Status
	Q	Q	Q	Q	≤	Q
<div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>	DCP1				21/12/2023 14:49:21	Registered
<div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>	CortexProbe	0.8%	61.9%	67.9%	21/12/2023 14:50:18	Connected

Once this step is completed, return to the DCP host, and execute the following command to connect the DCP to the Cortex.

In Linux:

```
./retina-probe.sh --start
```

In Windows:

```
.\retina-probe.bat --start
```

If no prior Cortex configuration has been created, a prompt will appear requesting the user to input the Hostname/IP Address of the Cortex to connect, and then the username and password of a Cortex administrator user.

EXALENS[®]

A user with Administrator access (Administrator group), or the default Administrator credentials should be used for this step. The default account is the default administrator account of the Cortex. Once the credentials are entered, upon successful authentication, the DCP will download its registration configuration and confirm successful connectivity with the Cortex (as shown below), and then auto start DCP services.

```
Please enter your credentials:
[?] Enter username: admin
[?] Enter password: *****
Probe configured successfully
exalens@probe:~$
```

Once the DCP starts, the DCP status under “System Administration - Data Collectors” will change from “Registered” to “Connected”. This means the DCP is now fully started and can be used for network and endpoint / process monitoring.

Data Collectors						
Action	Name	CPU Usage	Memory Usage	Disk Usage	Last Activity (UTC)	Status
	🔍	🔍	🔍	🔍	📅	🔍
🔄 📄 ⏻ ⏻ ⚙️ ⬇️	CortexProbe	82.4%	59.1%	59.1%	20/12/2023 12:16:52	Connected

Stopping the DCP Appliance

To stop the Exalens DCP, this can be carried out both via the command line terminal on the DCP console or via the Cortex web UI with which the DCP is registered. To stop the DCP via the command line, execute the following command:

On Linux:

```
./retina-probe.sh --stop
```

On Windows:

```
.\retina-probe.bat -- stop
```

To stop the Cortex via the web UI, navigate to top right of the user interface and select the username button to list system settings menu, then under “System Administration – Data Collectors” select the “Shutdown” button for the respective DCP (see image below)

Updating the DCP

To update the DCP, it is recommended to stop any active Endpoint / Process Monitors and Datasource plugins on the Exalens Cortex. Whilst Cortex will attempt to close any active datasources and monitors that are running when notified by a DCP that it is shutting down or being updated, failing to stop these via the Cortex may result in unexpected behaviour after DCP updates have completed and the DCP restarts.

Datasource plugins can be stopped by navigating to “Datasources” under the main navigation menu, and selecting the specific datasource plugin type, followed by selecting the stop button for configured and running datasources. Endpoint / Process Monitors can be stopped by navigating to “Monitors” under the main navigation menu, followed by selecting the stop button for configured and running Endpoint and Process Monitors.

To update the DCP via the DCP console on the appliance command line, login via a local terminal or SSH and run the following command:

On Virtual / Hardware appliances and Linux:

```
./retina-probe.sh --update
```

On Windows:

```
.\retina-probe.bat --update
```

Once the update has completed, the DCP will automatically restart. Once DCP has successfully restarted, its connectivity status should appear as “Connected” under the “System Administration” in the Cortex Web UI. If for any reason the DCP has not restarted successfully, manually stop and start the DCP again. If this does not resolve the issue, contact Exalens Support Team to troubleshoot further.

It is also possible to update the DCP via the Cortex Web UI under “System Administration – Data Collectors”, by selecting the update button under the “Actions” column of the Data Collectors list (see image below).



After successful DCP update via the Cortex Web UI, a confirmation popup will appear stating that the DCP has been successfully updated.

Configuring DCP Network and Endpoint / Process Monitoring Roles

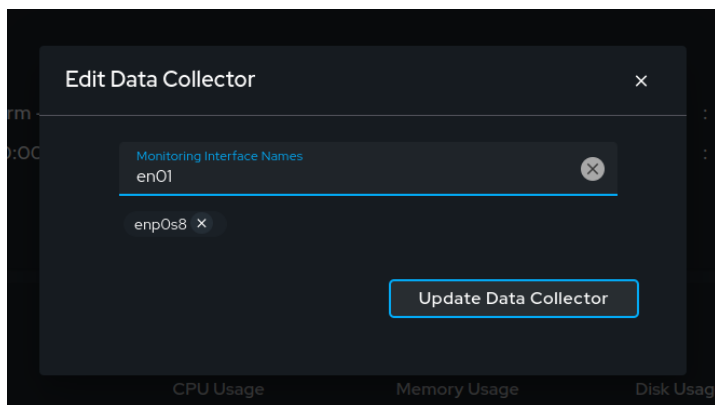
A DCP appliance can be configured with multiple data collection roles so that it performs network and or endpoint / process monitoring. A DCP can be configured solely a network monitor (passively monitoring a network SPAN or TAP or on host monitoring host network interfaces), an agentless endpoint / process monitor, or both simultaneously. This option is configurable in both Virtual / Hardware appliance and Docker container deployments.

For Virtual or Hardware appliances, no configuration is necessary for activating these roles as dedicated virtual or physical interfaces are preconfigured for network monitoring and endpoint / process monitoring. Network monitoring will not be activated until a SPAN / TAP interface is connected to the appliance. Endpoint / Process monitoring will not be activated until the user configures a Datasource to use a specific DCP in the Exalens Cortex – this notifies the Exalens Cortex to instruct the DCP to create a Datasource client for Endpoint / Process monitoring.

For Docker Container deployments, the network monitoring feature is available only for Linux host machines currently. To monitor the network interface using the Exalens platform on a Linux host, carry out the following steps:

1. Following the DCP registration process as defined earlier in “Configuring and Registering a DCP Virtual/Hardware appliance with a Cortex”, and during the DCP registration process, add the network interface names that should be used for passive network monitoring under “Monitoring Network Interfaces”, before clicking on “Register Data Collector”.

2. For existing registered and connected DCPs, navigate to “System Administration” by clicking on the menu located in the top right corner (default admin). Select “System Administration” from the dropdown menu. Select the “Data Collector” menu tab at the top of in the System Administration page. Under the “Data Collector” section, select a DCP, and select the “Edit” button. Note the DCP status should be set as “Connected”, otherwise enabling network monitoring will fail. This because the Exalens Cortex will not be able to communicate with the DCP without a “Connected” state. On selecting “Edit”, a pop-up menu will appear prompting to input the name of the host interface to be monitored. More than one interface name can be specified in this configured, however, take care to use the exact name and case of the interface name as shown under the host interface configuration (e.g., when using “ifconfig” to list interfaces on Debian Linux). See image below for an example:



Once the desired network interfaces have been added, click “Update Data Collector” to save the DCP configuration. This will configure the DCP to start monitoring the specified network interface specified, however, it can take up to 5 minutes for the configuration to take effect. Please be aware that this configuration only updates the Docker Container configuration and does not set any monitoring configuration on the underlying hosts network interface. When setting a network monitoring interface in a Linux host Docker Container deployment, it is recommended to turn on promiscuous mode on the host interface, turn off broadcast, unicast, multicast, and ARP functions, as well as using ebtables / mac address filters to prevent outbound layer 2 frames. The configuration for these interface settings, as well as network interface monitoring optimisation (e.g., checksum offloading, packet rings, etc.) differ between Linux operating system distributions. For support in configuring these settings on host machines using Docker Containers for DCP deployment, contact the Exalens Support Team.

Reinstalling the DCP (Factory Reset)

Normally factory resetting the DCP software should not be required, however, under exceptional circumstances the DCP software can be reinstalled to a “Factory Reset” state. This can be carried out by running a clean reinstall process.

First stop the DCP and perform a factory reset reinstallation by executing the following commands.

On Linux:

```
./retina-probe.sh --stop  
./retina-probe.sh --clean-install
```


On Windows:

```
.\retina-probe.bat --stop  
.\retina-probe.bat --clean-install
```

Deleting a DCP from the Cortex

To delete a DCP that has been registered with a Cortex, this must be conducted via the Cortex Web UI under “System Administration”. Note that a DCP cannot use the existing network and process endpoint monitoring configuration of another DCP on a Cortex once the other DCP has been removed. So, when a DCP is removed from a Cortex, its network and process endpoint monitoring configuration on the Cortex are removed as well. Therefore, care should be taken when reconfiguring and removing DCPs from a Cortex instance to avoid losing configurations and data, especially for Endpoint / Process Monitors, as they are active configurations that are synchronised between the Cortex and corresponding DCP that performs process endpoint data acquisition.

Backing Up DCP Configurations and Data

It is recommended to periodically back up DCP install and data in the event of a system fault requiring reinstallation.

Below are examples command to backup the DCP to a local directory, or remotely via SCP (SSH) to a remote system. Enter the following command backup DCP to a local directory:

```
cp -r ~/.exalens/retinaProbe [DESTINATION_DIRECTORY_PATH]
```

Below are examples command to backup the DCP to a local directory, or remotely via SCP (SSH) to a remote system:

```
scp -r ~/.exalens/retinaProbe username@hostname:/path/to/remote
```

Troubleshooting Data Collector Probe Connectivity

DCP Connection Status

If the DCP connection status under “System Administration – Data Collectors” says: “**Registered**”, this indicates that the DCP has registered with the Cortex, but it is not yet started, or may have been stopped and therefore requires a restart.

If the DCP connection status under “System Administration – Data Collectors” says: “**ConnectionLost**”, this indicates that the DCP is no longer connecting and calling home to the Cortex. These DCP statuses can usually be resolved by selecting the restart button under the Data Collectors “Action” column. However, if DCP restart fails via the Cortex Web UI, login into the DCP and run the following command to start the DCP:

On Virtual / Hardware appliances and Linux:

```
./retina-probe.sh --start
```

On Windows:

```
.\retina-probe.bat --start
```


Failed Update via Cortex Web UI

Should for any reason a DCP update via the Cortex Web UI fail, then it is recommended that DCP update is conducted via the DCP command line console. Network connectivity should be validated in case updates via console are also failing.

Network Service Ports and Firewall Rules

The following ports are required for the Exalens Cortex and DCPs to communicate correctly over the network for normal operation. Please ensure these services are enabled in your firewall and access control policies.

Inbound Connectivity

To	From	Ports	Description
Cortex	DCP	TCP 443, TCP 5379	DCP Registration and Communication
Cortex	Admin systems	TCP 443	Web UI access
Cortex	Admin systems	TCP 22	SSH console management
DCP	Network SPAN/TAP interface	ALL	Networking Monitoring
DCP	Admin systems	TCP 22	SSH console management

Outbound Connectivity

From	To	Ports	Description
Cortex	ALL	TCP 443	Updates & Patches
Cortex	NTP servers	UDP 123	Time synchronisation
Cortex	DNS servers	UDP 53, TCP 53	Hostname resolution
DCP	ALL	TCP 443	Updates & Patches
DCP	NTP servers	UDP 123	Time synchronisation
DCP	DNS servers	UDP 53, TCP 53	Hostname resolution
DCP	Specific monitored endpoint devices	ALL	Agentless endpoint monitoring (read-only)

Default Appliance User Credentials

From	Username	Password
Exalens Appliance	exalens	exalens
Cortex Web UI (First Login)	admin	@Dm1nadmin

Support Contact Information

Technical Resources: <https://www.exalens.com/resources/resource-centre>

Slack Workspace: exalens.slack.com

Email: support@exalens.com (preferred method)