



Qualys Context XDR (Extended Detection and Response)

Day 0 Enablement Guide

July 05, 2022

Copyright 2022 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

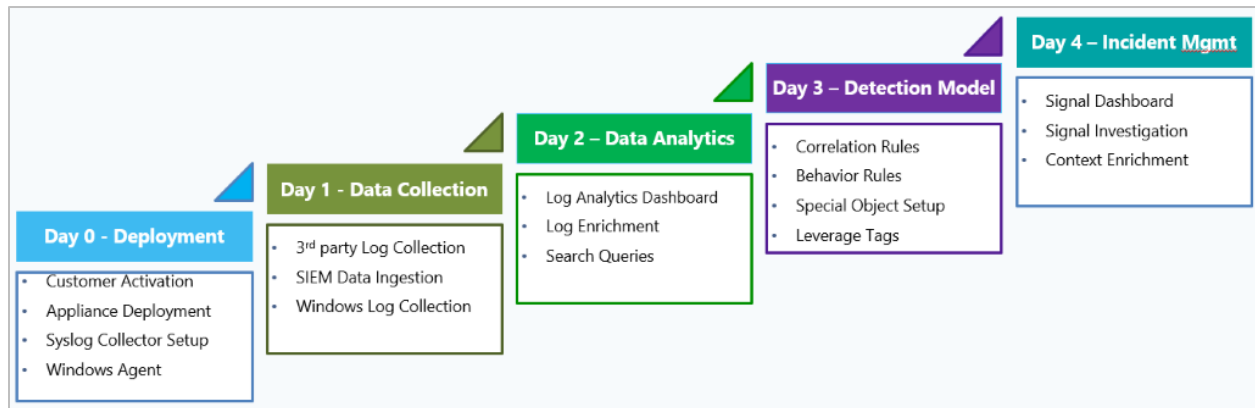
Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

Summary	4
Day 0 – Deployment	4
Appliance Deployment.....	5
Stage 1: Download the Appliance Image	5
Stage 2: Deploy and Verify the Appliance	6
Stage 3: Generate Activation Code	10
Stage 4: Apply Activation Code.....	11
Stage 5: Verify Activation	12
Collector Deployment.....	13
Syslog Collector.....	13
Active Directory Collector.....	16
Windows Agent Preparation	21
Install New Agent	21
Existing Agent	21
Enable XDR via a Configuration Profile.....	21
Activate Cloud Agents for XDR	23
What's Next.....	25
Appendix A – Appliance Deployment.....	26
Single-Site	26
Multi-Site	27
Appendix B - Windows Cloud Agent Requirements.....	28

Summary

The purpose of this guide is to provide a detailed overview of how to enable Qualys Context XDR (Extended Detection and Response). Qualys splits the enabling process over several phases. This guide covers the activities on Day 0, during which an appliance is deployed, and a collector is set up. This also covers information to set up the Qualys Windows Cloud Agent for XDR.



Day 0 - Deployment

On Day 0, we will walk you through the steps to:

1. [Deploy an appliance](#)
2. [Set up a collector](#)
3. [Prepare Qualys Cloud Agent for XDR](#)

Appliance Deployment

Deploying an appliance involves 5 stages:

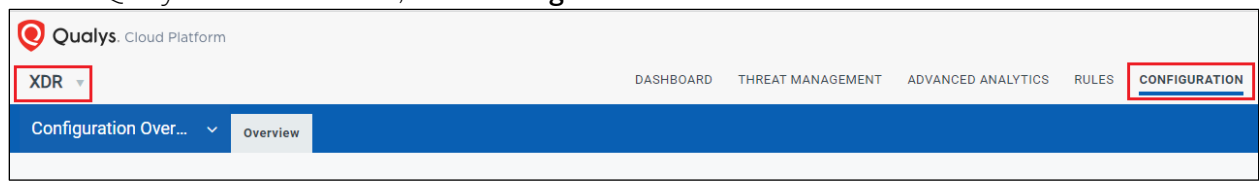
1. [Download the appliance image](#)
2. [Deploy and verify the appliance](#)
3. [Generate the registration code](#)
4. [Apply the registration code](#)
5. [Verify the activation](#)

To know more information on the appliance size requirements, refer to the [Appliance – Sizing calculations](#) section in the Online Help.

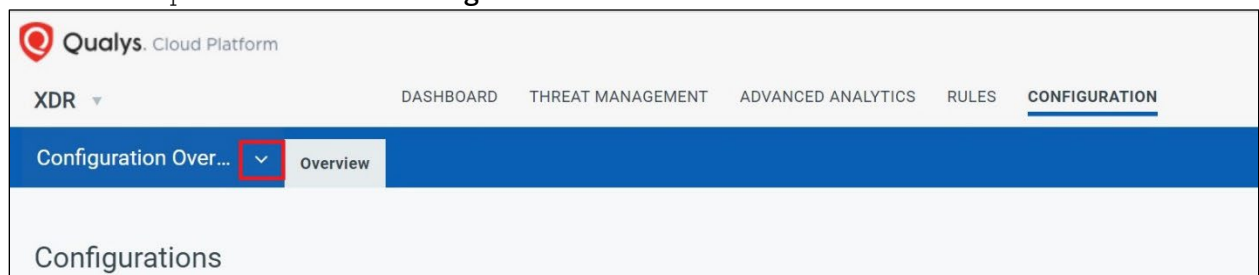
Stage 1: Download the Appliance Image

Qualys appliance image is available for download right from the Qualys Context XDR UI. Follow these steps to download the image:

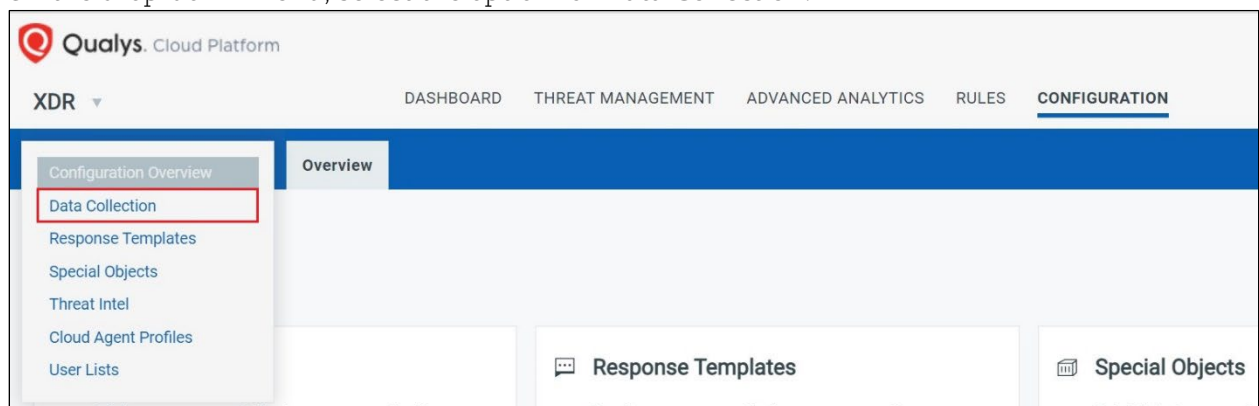
1. From the module picker, select XDR to access the Extended Detection and Response (XDR) module within the Qualys Cloud Platform.
2. On the Qualys Context XDR UI, click **Configuration**.



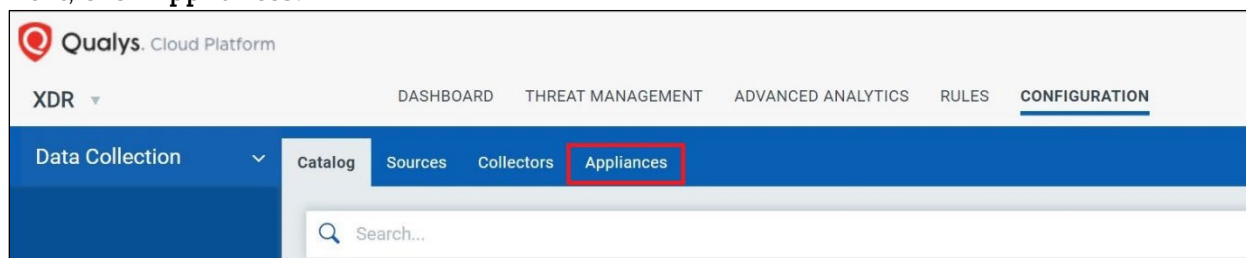
3. Click the drop-down box near **Configuration Overview**.



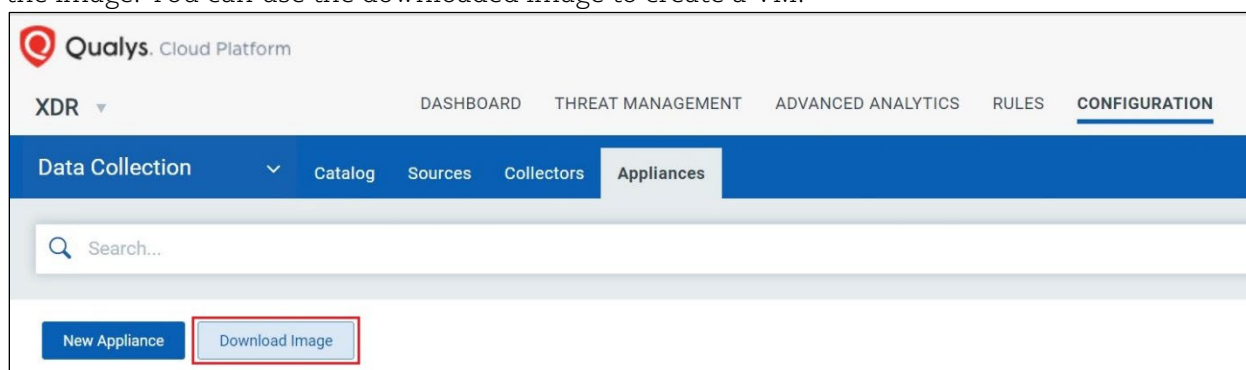
4. On the drop-down menu, select the option for **Data Collection**.



- Next, click **Appliances**.



- On the Appliances tab, click the **Download Image** button to view available links to download the image. You can use the downloaded image to create a VM.

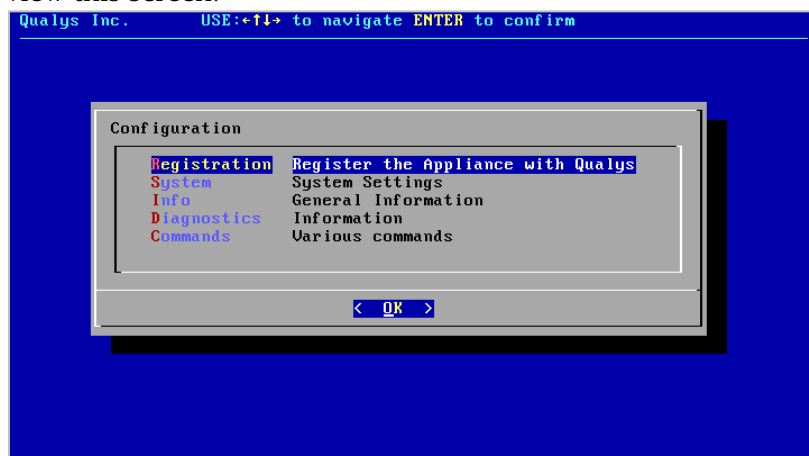


Stage 2: Deploy and Verify the Appliance

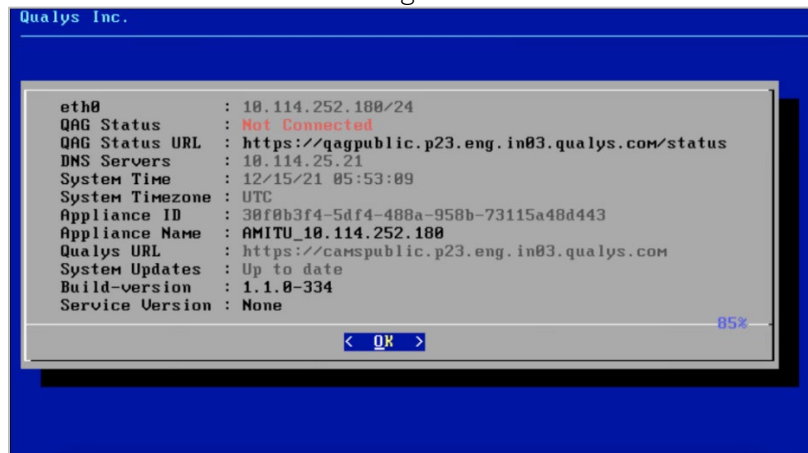
It is imperative to deploy the appliance within your environment such that there is network connectivity between the log sources and the appliance and between the appliance and the Qualys Cloud platform. See [Appendix A](#) for a few network diagrams on the recommended appliance deployment.

Note: If needed, consult your Solutions Architect for assistance.
Follow these steps to deploy the appliance:

- Deploy the image you downloaded. After deploying, the appliance may need 5-10 minutes to boot up the first time. After the appliance fully boots, console into the virtual machine to view this screen:

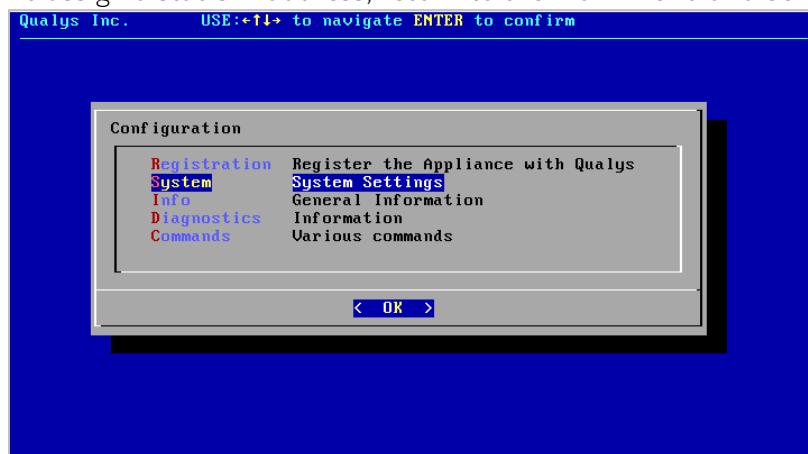


- By default, the appliance tries to automatically configure via DHCP. To verify the IP address, select Info to view the following screen:

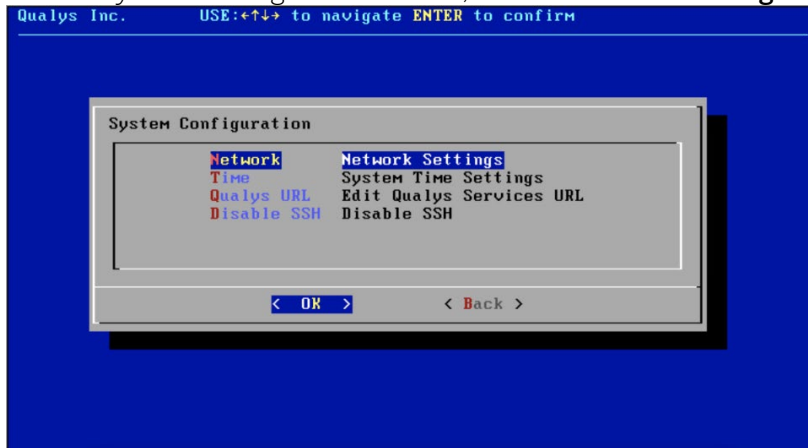


Note: XDR only supports a static IP address. If you need DHCP, contact Technical Account Manager (TAM).

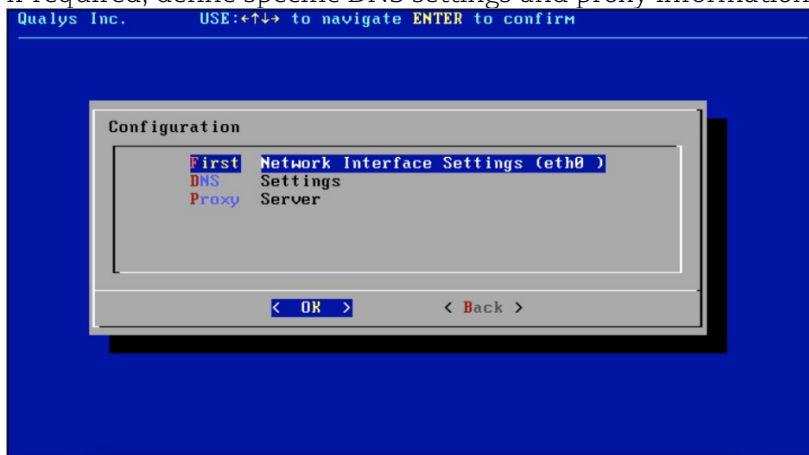
- To assign a static IP address, return to the main menu and Select **System Settings**.



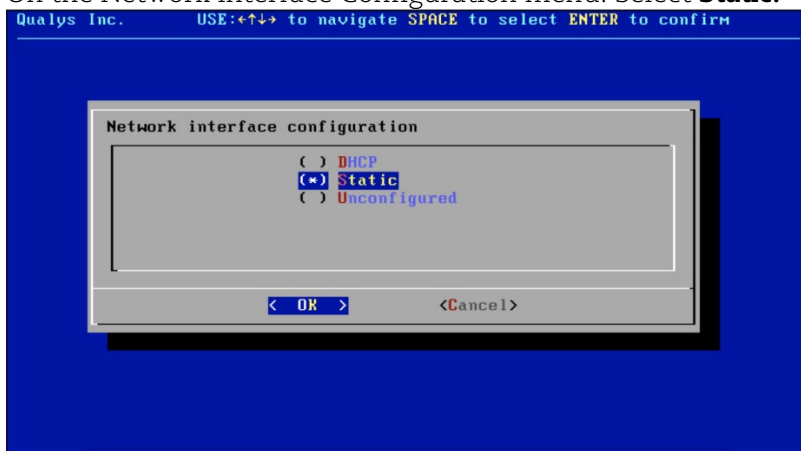
- On the System Configuration menu, Select **Network Settings**.



- On the Network Configuration menu, Select **Network Interface Settings**.
If required, define specific DNS settings and proxy information.

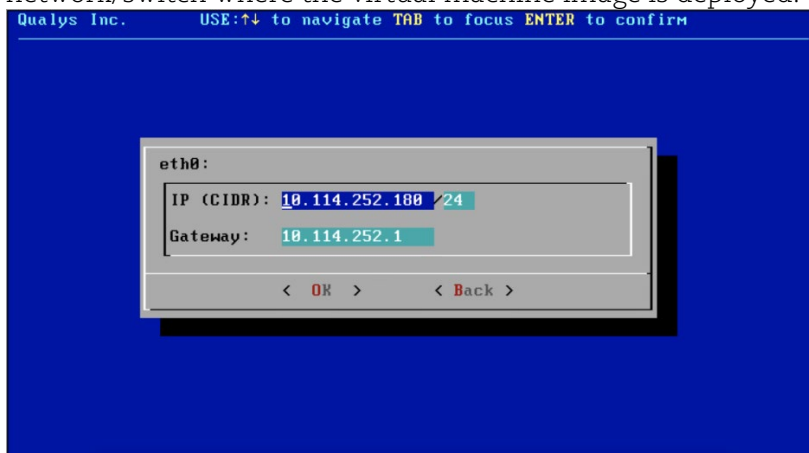


- On the Network interface Configuration menu. Select **Static**.

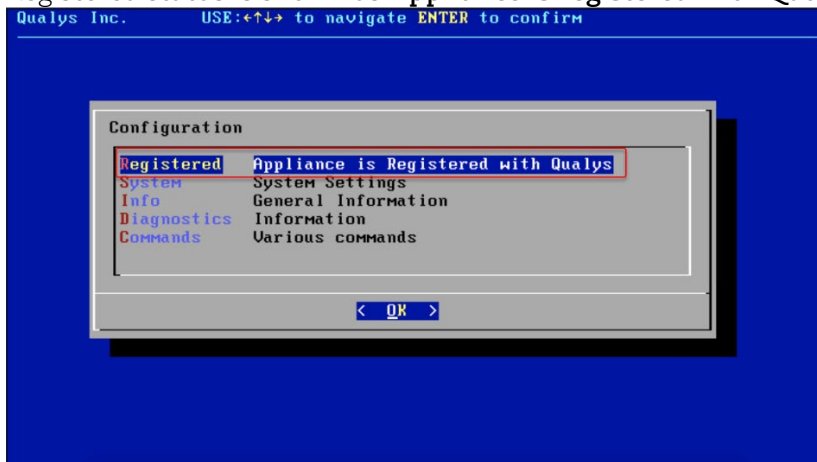


Note: XDR only supports a static IP address. If you need DHCP, contact Technical Account Manager (TAM).

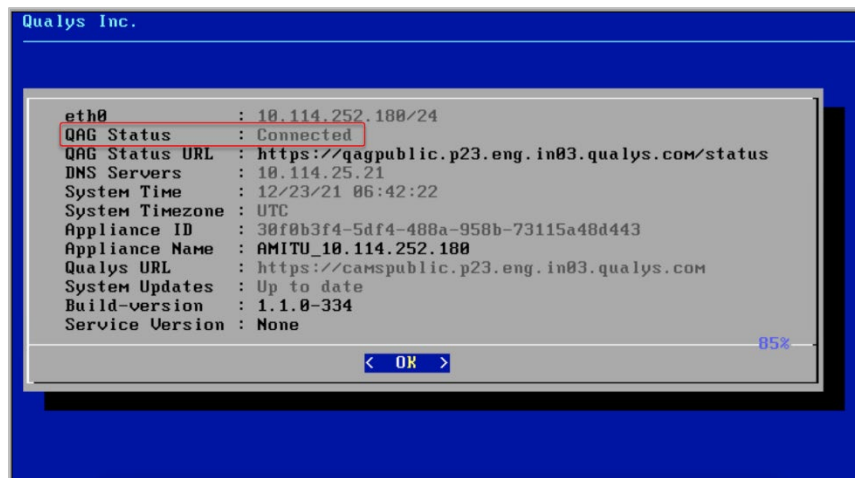
- Enter the IP address and Gateway to configure the interface that conforms to the virtual network/switch where the virtual machine image is deployed.



8. Once the network is successfully configured, return to the main menu and see if the Registered status is shown as **Appliance is registered with Qualys**.



9. Also, if the network is successfully configured, QAG Status should show as **Connected** on the Info screen under the **General information** of main menu.



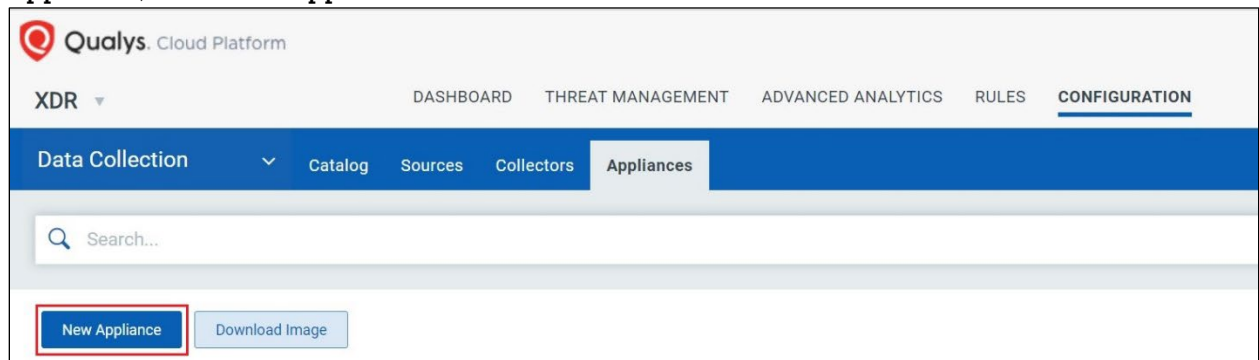
The initial stages of the appliance setup are considered as verified when the QAG Status is Connected. You can now proceed to generate an activation code from the XDR UI.

Stage 3: Generate Activation Code

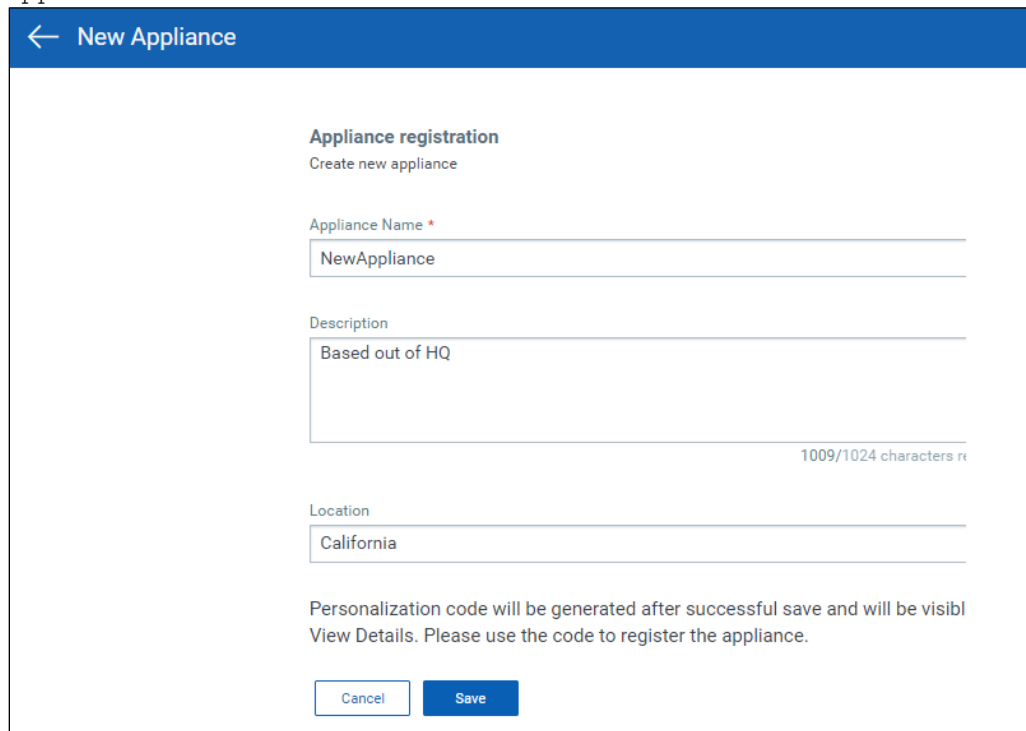
After you have deployed an appliance, you need to bind it with the Qualys Cloud Platform. Qualys uses an activation code for this purpose.

Follow these steps to generate an activation code:

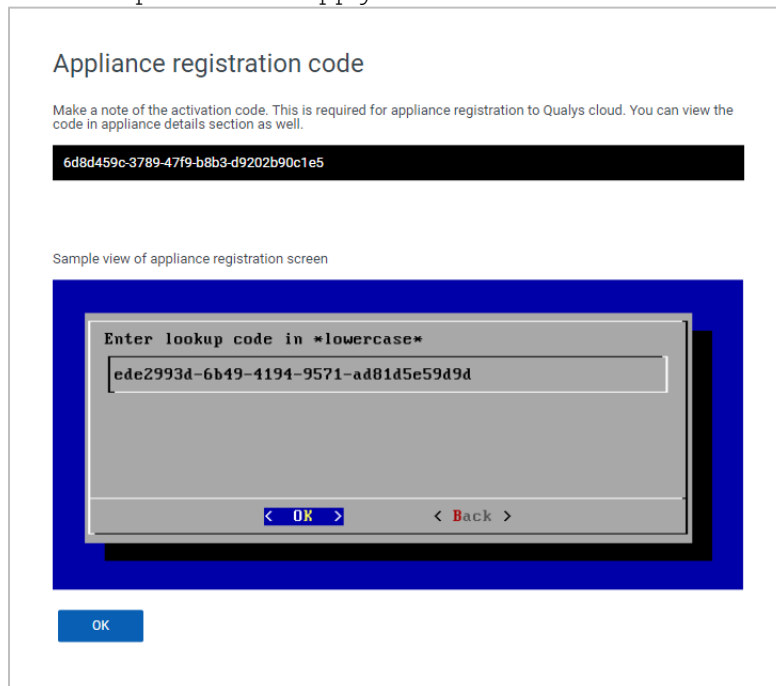
1. On the Qualys Cloud Platform, under **XDR > Configuration > Data Collection > Appliance**, click **New Appliance**.



2. Enter the Appliance Name, Description, and Location details you want to use for the appliance and click **Save**.

A screenshot of the 'New Appliance' form in the Qualys Cloud Platform. The form has a blue header bar with a back arrow and the text 'New Appliance'. The main content area is titled 'Appliance registration' with the subtitle 'Create new appliance'. It contains three input fields: 'Appliance Name' (with a red asterisk) containing the text 'NewAppliance', 'Description' containing 'Based out of HQ', and 'Location' containing 'California'. A character count '1009/1024 characters' is visible next to the description field. Below the input fields, a message states: 'Personalization code will be generated after successful save and will be visible in View Details. Please use the code to register the appliance.' At the bottom of the form are two buttons: 'Cancel' and 'Save'.

3. An Appliance registration code is generated when the appliance is saved. This registration code is required in the Apply Activation Code section.



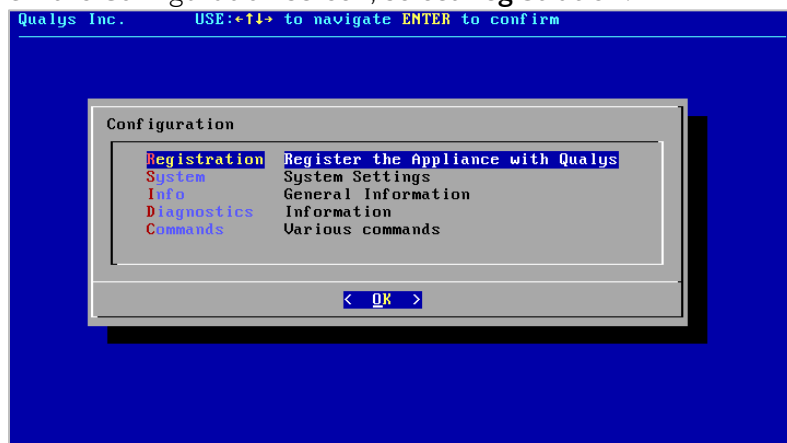
The appliance is visible on the Appliances tab with the **Unregistered** status.

Stage 4: Apply Activation Code

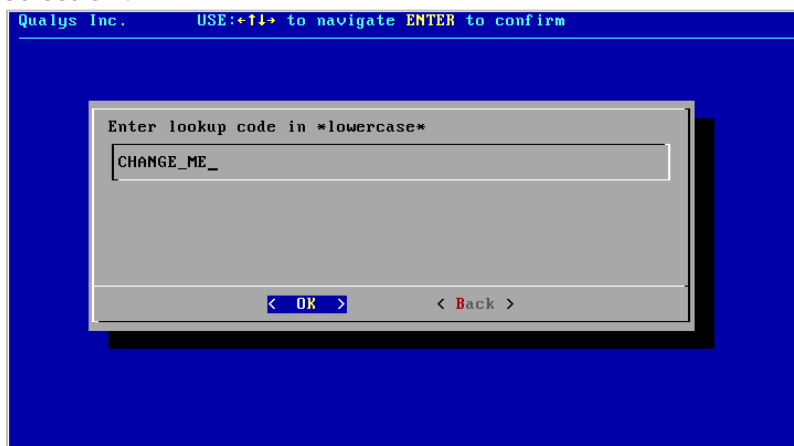
To bind the virtual machine appliance deployed in the Deploy and Verify the Application section with the Qualys Cloud Platform, you need to register the appliance with the registration code generated in stage 3.

Follow these steps to register your appliance:

1. Access the appliance deployed and verified in the Deploy and Verify the Application section via the console.
2. On the Configuration screen, select **Registration**.



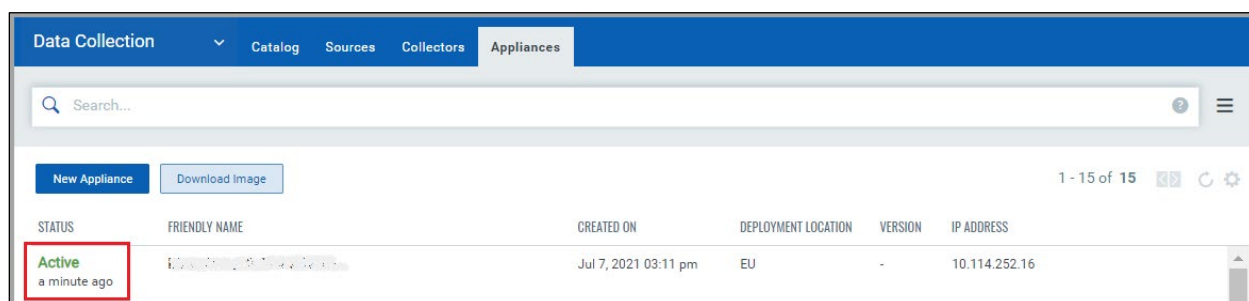
- Next, enter the registration code generated in the Generate Registration Code section and select **OK**.



TIP: Some consoles do not allow copy-paste. You might have to manually type in the registration code on such consoles.

Stage 5: Verify Activation

The final step in deploying an appliance is verifying the deployment. To verify the deployment, on the Qualys UI, navigate to **Configuration > Data Collection > Appliance**. The appliance you deployed should be displayed with the status as **Active**.



If the status does not update or continues to show 'Unregistered' after 10 minutes, contact your Solutions Architect for assistance.

Collector Deployment

After the new application is deployed, you can deploy and prepare log collectors for ingestion to the Qualys Context XDR Platform. Depending on your initial scope, you can deploy a syslog collector and/or perform Windows Agent activation (WLC logging profile will be on Day 1).

IMPORTANT: To continue, validate your XDR appliance is successfully registered and the status appears as **Active**.

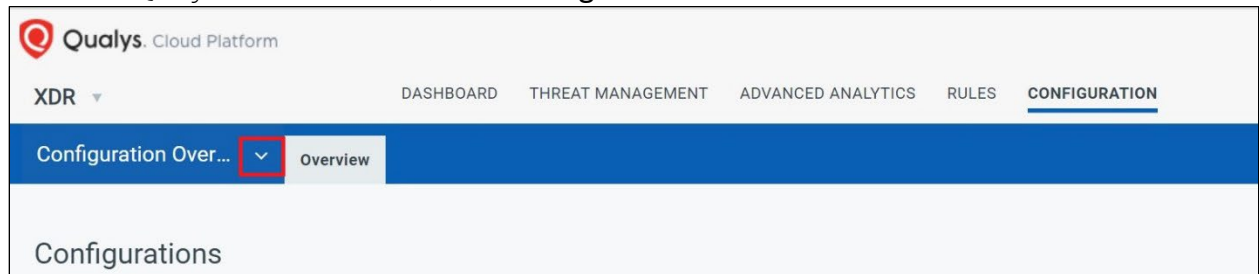
You can deploy the following collectors:

- [Syslog Collector](#)
- [Active Directory Collector](#)

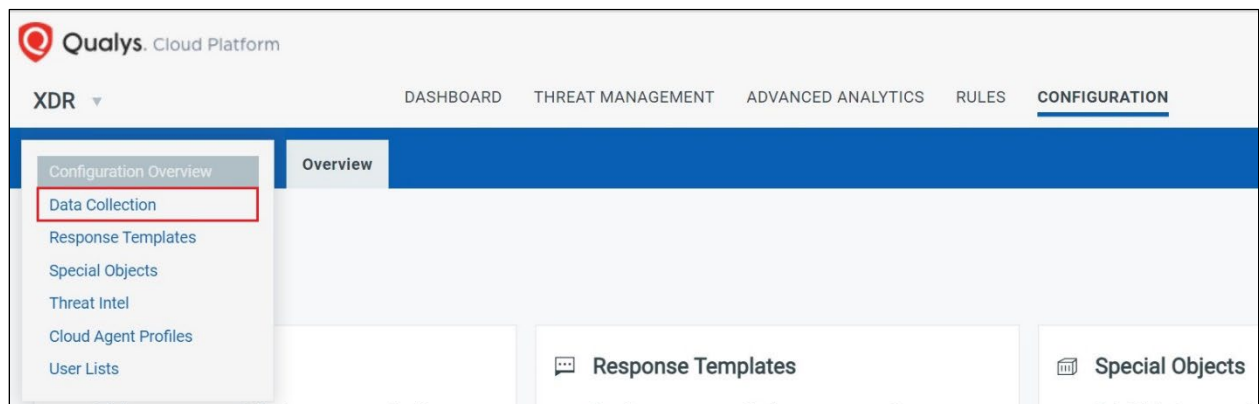
Syslog Collector

Follow these steps to configure a Syslog collector:

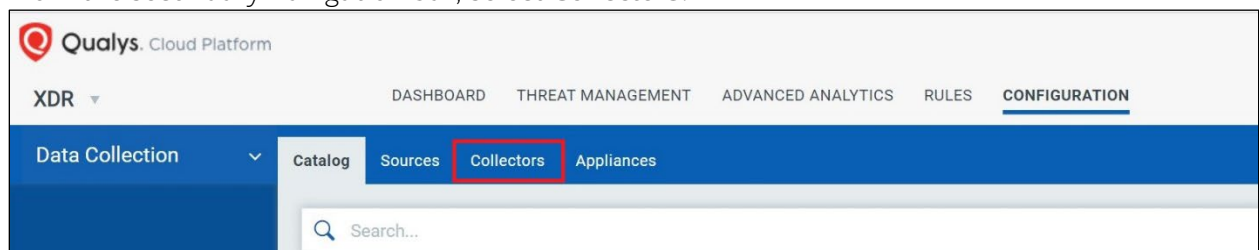
1. From the Qualys Context XDR UI, click **Configuration**.



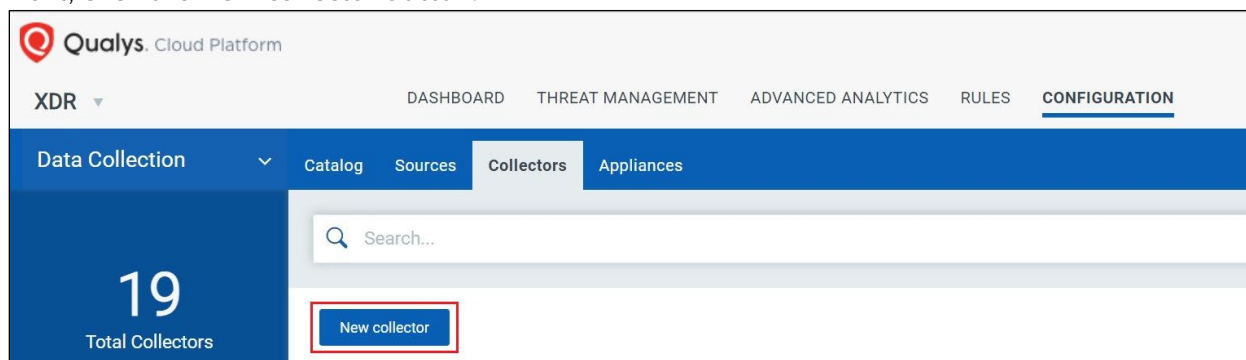
2. From the **Configuration Overview** menu, select **Data Collection**.



3. From the secondary navigation bar, select **Collectors**.



- Next, click the **New collector** button.



- Enter a **Name** and **Description** for the collector.
In our example, we chose a naming convention that will quickly give us the information.

The screenshot shows the 'Collector Details' form. It has the following fields:

- Name ***: A text input field containing 'USL-SYSLOG'.
- Description ***: A text area containing 'This is a syslog collector'. A character count '998/1024 characters remaining' is shown at the bottom right of the text area.
- Type ***: A dropdown menu with the placeholder text 'Select type of collector'.
- Appliance ***: A dropdown menu with the placeholder text 'Select appliance'.
- HeartBeat Interval ***: A dropdown menu with the placeholder text 'Select HeartBeat interval in minutes'.

At the bottom of the form are two buttons: 'Cancel' and 'Save'.

- Next, from the **Type** dropdown list, choose **Syslog**.
- The **Appliance** drop-down lists all the active appliances you have already deployed. Select the appliance you want to deploy this Syslog collector on.

8. When you set the Type to SYSLOG, additional details will open up. Define the protocol and port number you want the collector to listen on and then click **Save**.

Collector Configuration

Port *

514

Protocol *

UDP

9. After a few minutes, when the collector binds successfully, the collector status appears as **Active** under the Collectors tab.

Catalog Sources Collectors Appliances				
Search...				
New collector 1 - 19 of 19				
STATUS	COLLECTOR NAME	TYPE	LAST COLLECTION	NEXT COLLECTION
Active 4 minutes ago	SYSLOG_10.114.252.173 SYSLOG_10.114.252.173	SYSLOG	Not applicable	Not applicable

If the status does not show Active, try the following:

- Recheck the parameters and verify the credentials.
- Attempt configuring the collector on a different port.

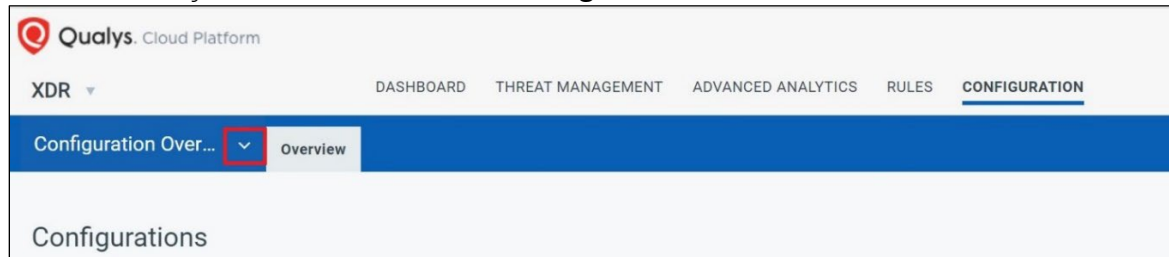
If the status does not change to Active, contact your Qualys Technical Account Manager (TAM) or Solution Architect. You can also contact Qualys Support to resolve your issue.

Active Directory Collector

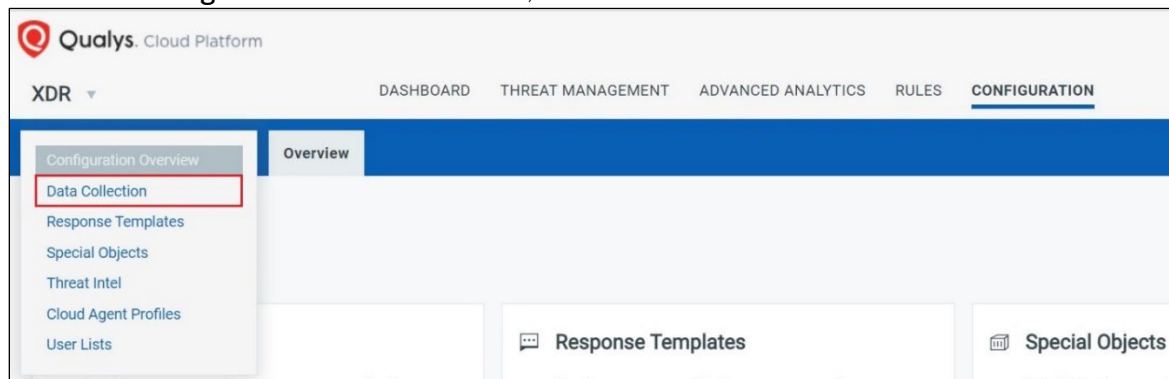
An Active Directory collector allows you to import your organization's user directory and user attributes into Qualys Context XDR. XDR uses this user data to enrich data from other log sources.

Follow these steps to configure an Active Directory collector:

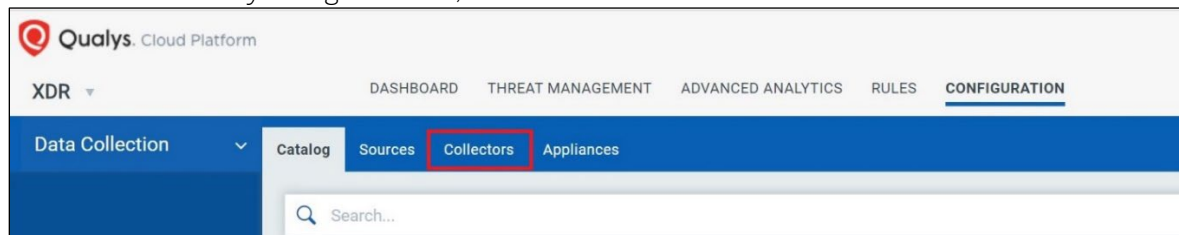
1. From the Qualys Context XDR UI, click **Configuration**.



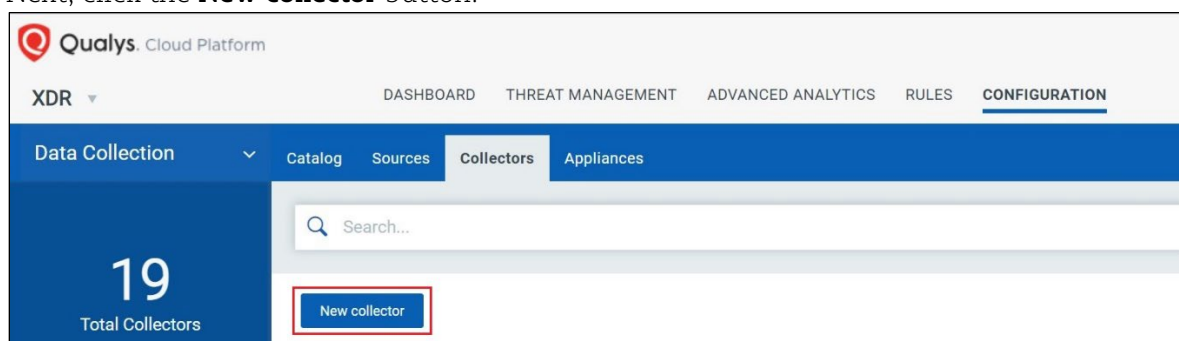
2. From the **Configuration Overview** menu, select **Data Collection**.



3. From the secondary navigation bar, select **Collectors**.



4. Next, click the **New collector** button.



5. Enter a **Name** and **Description** for the collector.

Collector Details

Name *

Description *

This is an Active Directory collector

987/1024 characters remaining

Type *

Select type of collector ▼

Appliance *

Select appliance ▼

HeartBeat Interval *

Select HeartBeat interval in minutes ▼

Cancel

Save

6. From the **Type** drop-down, select **AD** as your collector.

Collector Details

Name *

Description *

This is an Active Directory collector

987/1024 characters remaining

Type *

AD ▼

7. The **Appliance** drop-down lists all the active appliances you have already deployed. Select the appliance you want to deploy this Active Directory collector on.
8. After selecting the appliance, define the heartbeat interval for this collector.
NOTE: Qualys recommends a heartbeat interval of 5m.

9. When you set the Type to AD, additional details will open up. You can now choose to configure this collector as **LDAP** or **LDAPS**.

A. **LDAP**

Follow these steps to configure your collector as LDAP:

- a) Define the **Host** and **Port** for this collector.

NOTE: The port is typically set as 636.

The screenshot shows the 'Collector Configuration' form with the 'LDAP' radio button selected. The form includes fields for Host, Port, BindDN, Password, Refresh frequency in minutes, Base Context, and Filter. Each field has a placeholder text and a character count indicator.

Collector Configuration

☒ LDAP ☐ LDAPS

Host * Port *

BindDN * 1024/1024 characters remaining

Password *

Refresh frequency in minutes ⓘ *

Base Context * 1024/1024 characters remaining

Filter *

- b) Next, configure the **BindDN** and enter the password.

- c) You can then define the refresh frequency in minutes.

NOTE: Qualys recommends a refresh frequency of 1440 minutes.

- d) Next, add the base context for this collector.

- e) Finally, define the filter you want to set for this collector.

NOTE: Qualys recommends this filter – (&(objectCategory=person)(objectClass=user))

B. **LDAPS**


Follow these steps to configure this collector as LDAPS:

- a) Choose your **Certificate Type**.

Collector Configuration

☐ LDAP ☒ LDAPS

Certificate type *
X.509

 Drop file here to attach or [browse](#)

Host *
Add host for this collector

Port *
Add port for this collector

BindDN *
for example: CN=Jon Wiesly,OU=Dev,DC=corp,DC=xyz,DC=com
1024/1024 characters remaining

Password *
Enter password

Refresh frequency in minutes ⓘ *
Frequency

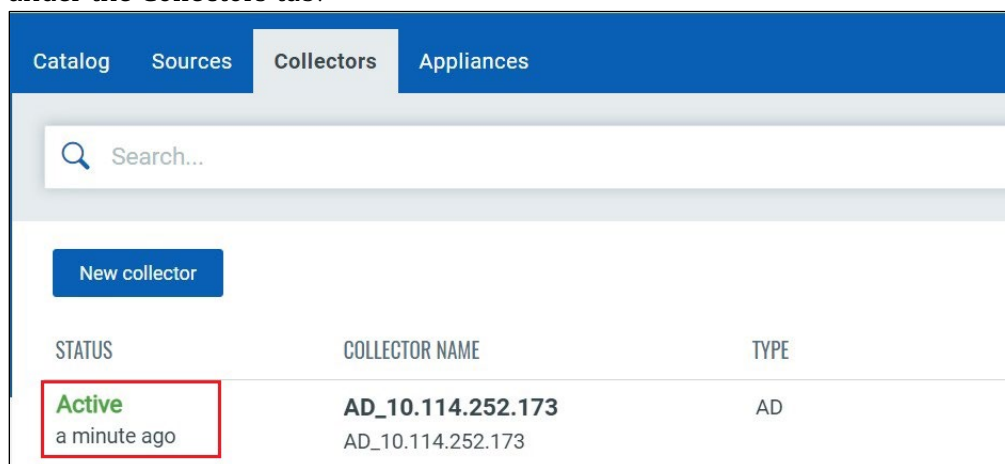
Base Context *
For example: OU=CorpUsers,DC=corp,DC=xyz,DC=com
1024/1024 characters remaining

Filter *
Add pattern to filter out logs for this collector. For example: (&(objectCategory=person)(objectClass=user))
1024/1024 characters remaining

- b) Drag and drop or browse and select your certificate to attach it.
- c) Next, add the base context for this collector.
- d) You can then define the refresh frequency in minutes.
NOTE: Qualys recommends a refresh frequency of 1440 minutes.
- e) Next, configure the **BindDN** and enter the password.
- f) Now, define the **Host** and **Port** for this collector.
NOTE: The port is typically set as 636.
- g) Finally, define the filter you want to set for this collector.
NOTE: Qualys recommends this filter – (&(objectCategory=person)(objectClass=user)).

10. Finally, click **Save** to configure your Active Directory collector.

After a few minutes, when the collector binds successfully, the collector status appears as **Active** under the Collectors tab.



The screenshot shows the Qualys interface with the 'Collectors' tab selected. At the top, there are tabs for 'Catalog', 'Sources', 'Collectors', and 'Appliances'. Below the tabs is a search bar labeled 'Search...'. A 'New collector' button is visible. The main content area displays a table with the following data:

STATUS	COLLECTOR NAME	TYPE
Active a minute ago	AD_10.114.252.173 AD_10.114.252.173	AD

If the status does not show Active, try the following:

- Recheck the parameters and verify the credentials.
- Verify the connection between the appliance and the directory host.
- If you are trying to configure your collector using LDAPS, ensure your Active Directory server is set up to allow LDAPS.
- Attempt configuring the collector on port 389 instead of 636.
- Ensure you have used FQDN or IP address to reduce name resolution errors.

After trying these steps, if the status does not change to Active, contact your Qualys Technical Account Manager (TAM) or Solution Architect. You can also contact Qualys Support to resolve your issue.

Windows Agent Preparation

Qualys Context XDR allows you to leverage existing Qualys Cloud Agents (Windows only) to collect event logs from assets on which agents are deployed. You can also deploy fresh agents and configure them to collect logs for XDR.

The Windows Cloud Agents used for Extended Detection and Response (XDR) must be assigned a Configuration Profile with XDR enabled. The Windows Cloud Agent must also be activated for XDR (see 'Existing Agent' below).

Install New Agent

For new Windows hosts without an existing Qualys Cloud Agent, refer the [Qualys Cloud Agent Getting Started Guide](#) for details.

Existing Agent

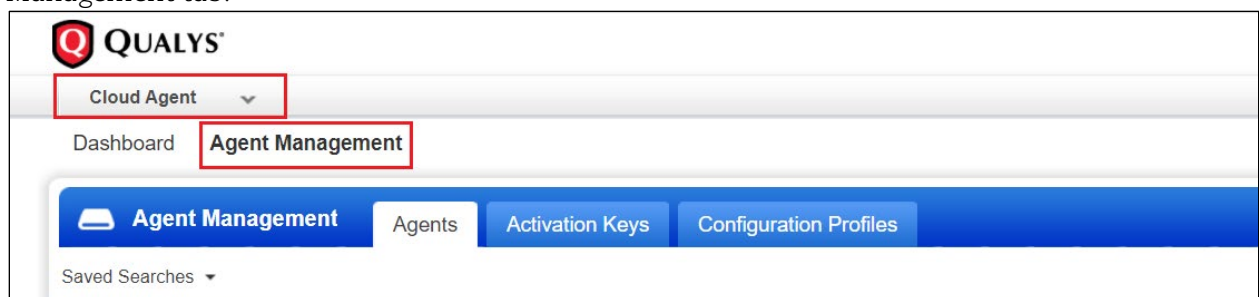
For Windows hosts with an existing Qualys Cloud Agent installed, first enable Extended Detection and Response (XDR) within the correct Configuration Profile and then activate the XDR license for each Cloud Agent to support XDR.

Enable XDR via a Configuration Profile

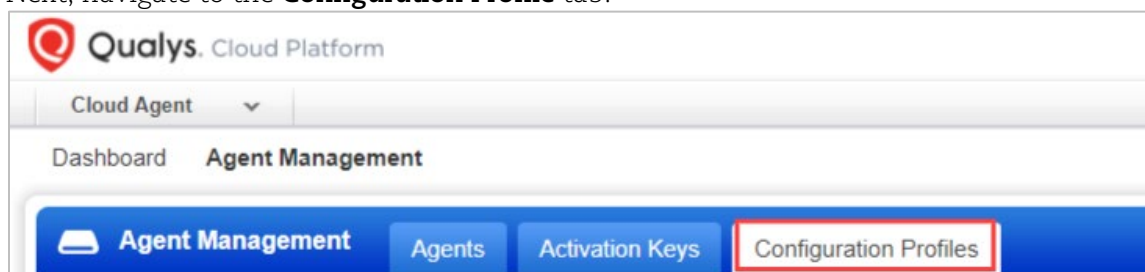
Before collecting event logs from assets using the Windows Cloud Agent, you first need to enable XDR for these agents by either updating an existing configuration profile or by creating a new configuration profile.

Follow these steps to enable XDR through a configuration profile:

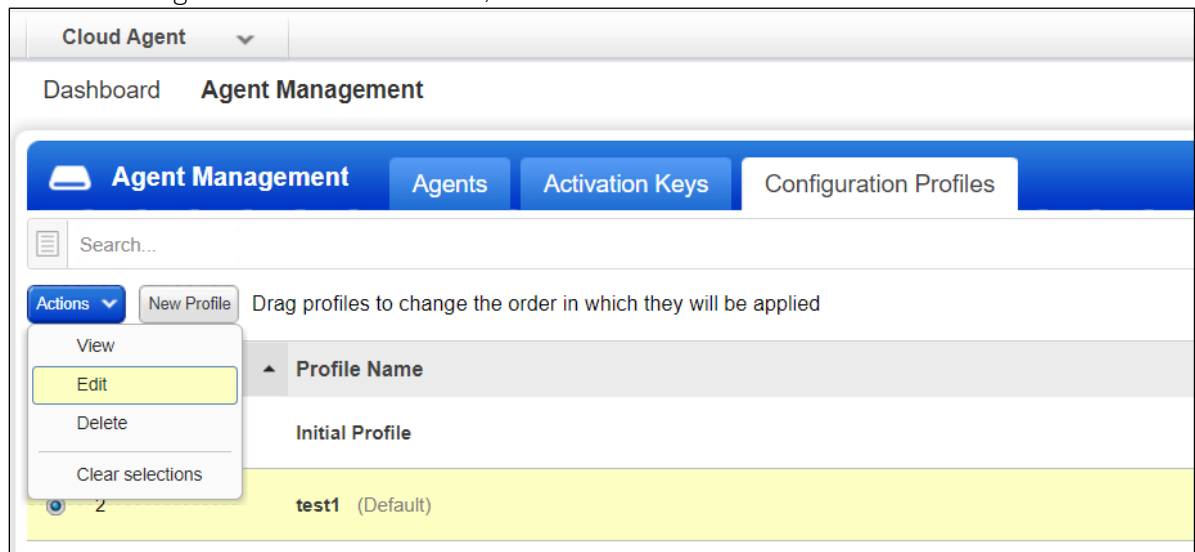
1. Navigate to **Cloud Agent** module within Qualys Cloud Platform and move to the Agent Management tab.



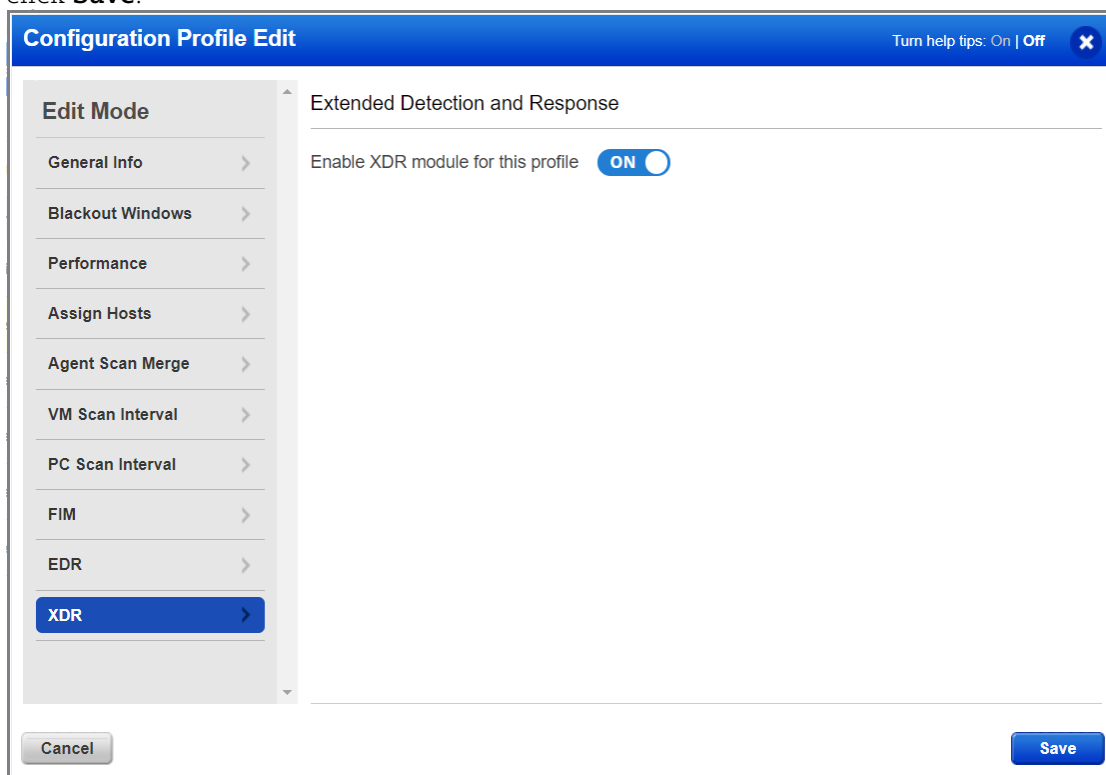
2. Next, navigate to the **Configuration Profile** tab.



- Choose an existing Configuration Profile (should already be assigned to the hosts) or create a new Configuration Profile.
- For the Configuration Profile selected, click **Edit** from the **Actions** menu.



- Scroll to the section for XDR and toggle the slider to **Enable XDR module for this profile** and click **Save**.



NOTE: When selecting a configuration profile, ensure the profile is assigned to the correct hosts. You can view and modify the hosts assigned to the profile, navigate to the **Assign Hosts** tab from the left pane of the Configuration Profile pop-up.

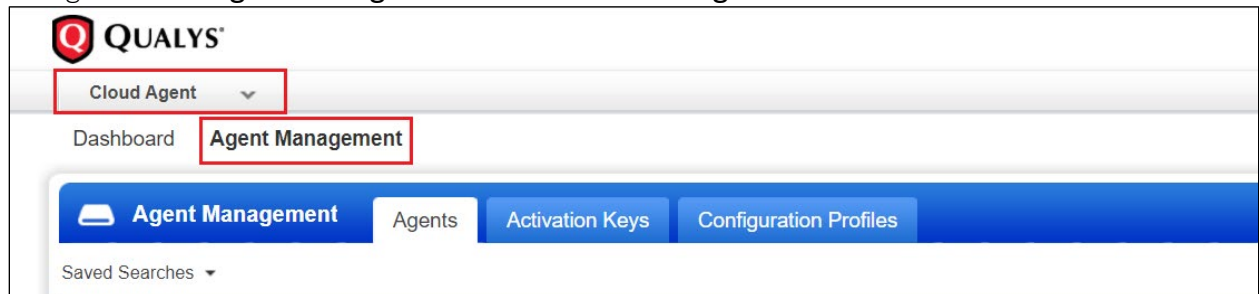
All hosts using this configuration profile are now enabled for XDR.

Activate Cloud Agents for XDR

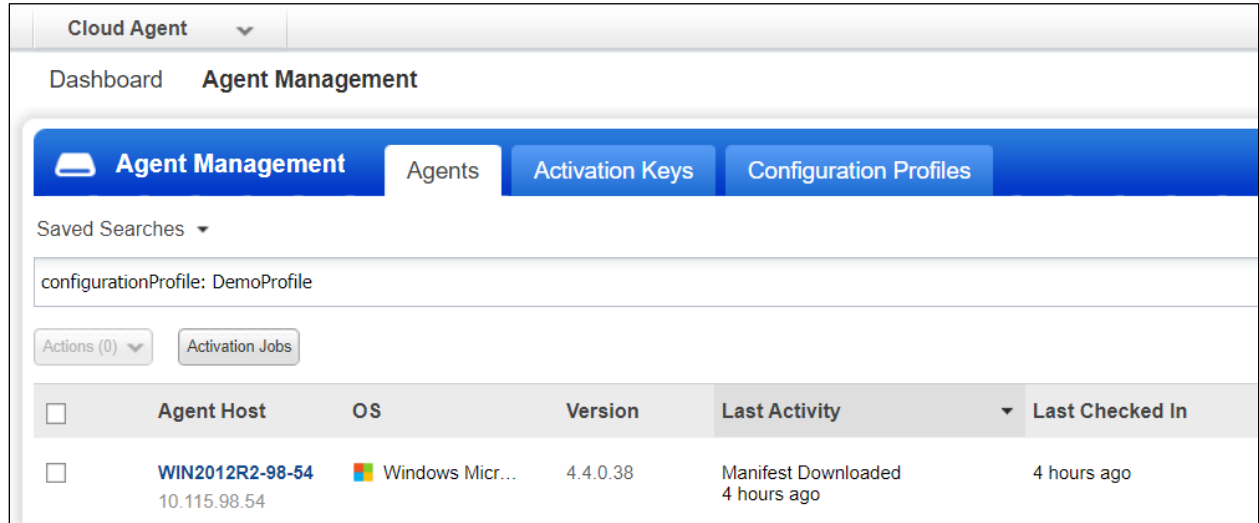
After you have enabled XDR via the configuration profile, ensure that your agents are activated for XDR.

Follow these steps to activate the Windows Cloud Agents for XDR:

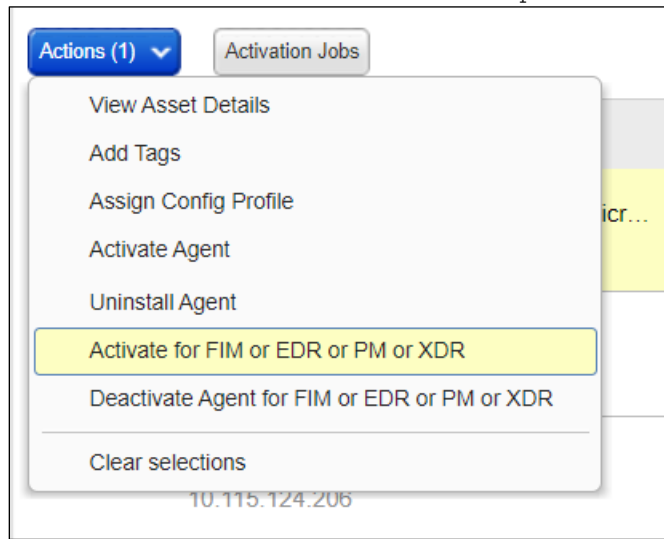
1. Navigate to the **Agent Management** tab of the **Cloud Agent**.



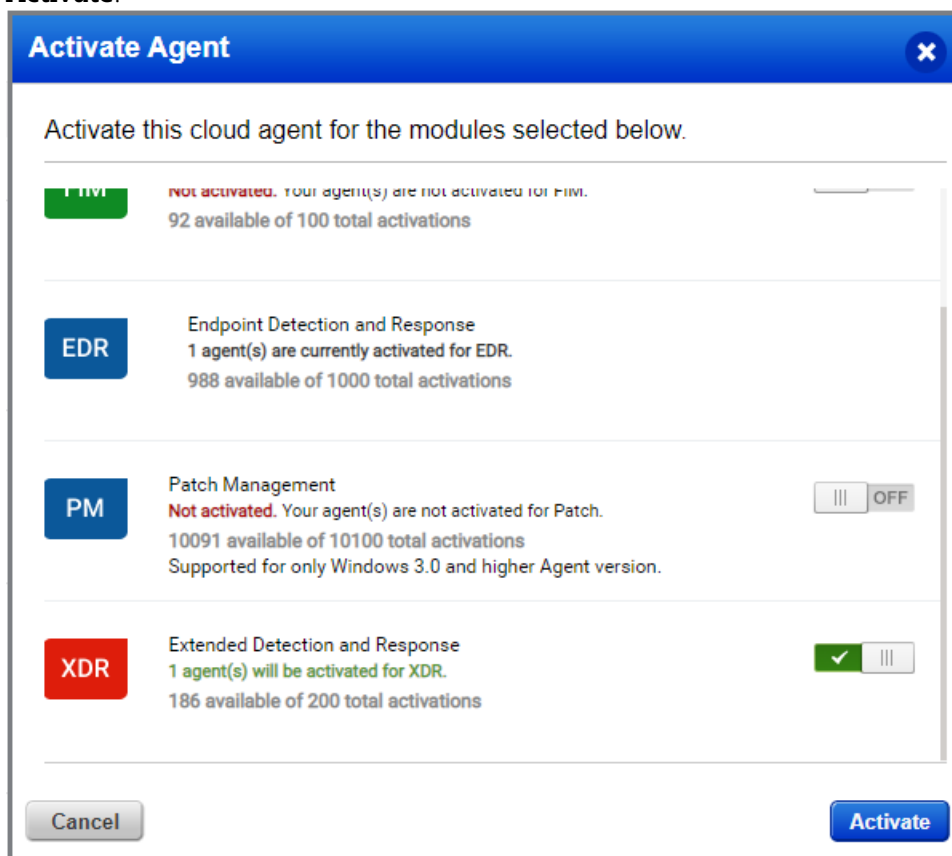
2. On the Agents sub-tab, search for the configuration profile that you enabled XDR on. This displays the Agents assigned to this configuration profile. For example, we search for the configuration profile named 'DemoProfile'.



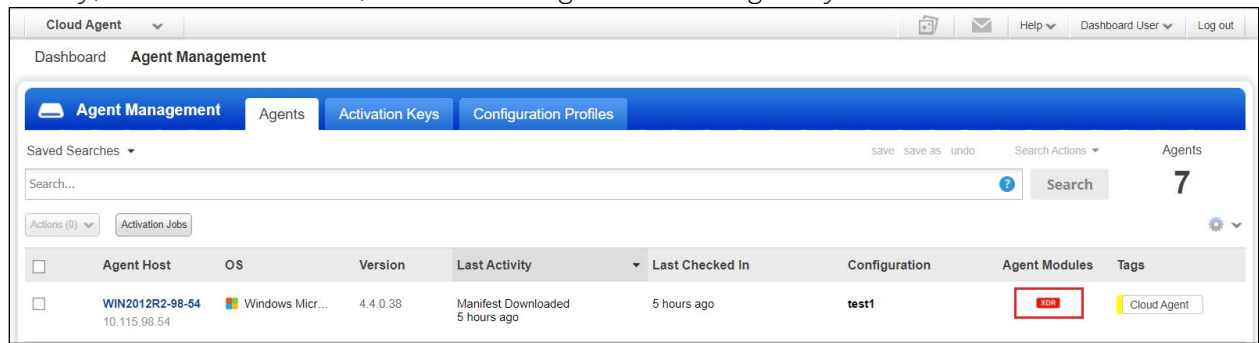
3. Select all agents using this configuration profile and click the **Actions** menu. Next, click the **Activate for FIM or EDR or PM or XDR** option.



4. On the Activate Agents pop-up, toggle the slider to activate the agent for XDR and click **Activate**.



5. Finally, after a few minutes, XDR is listed against all the agents you had selected.



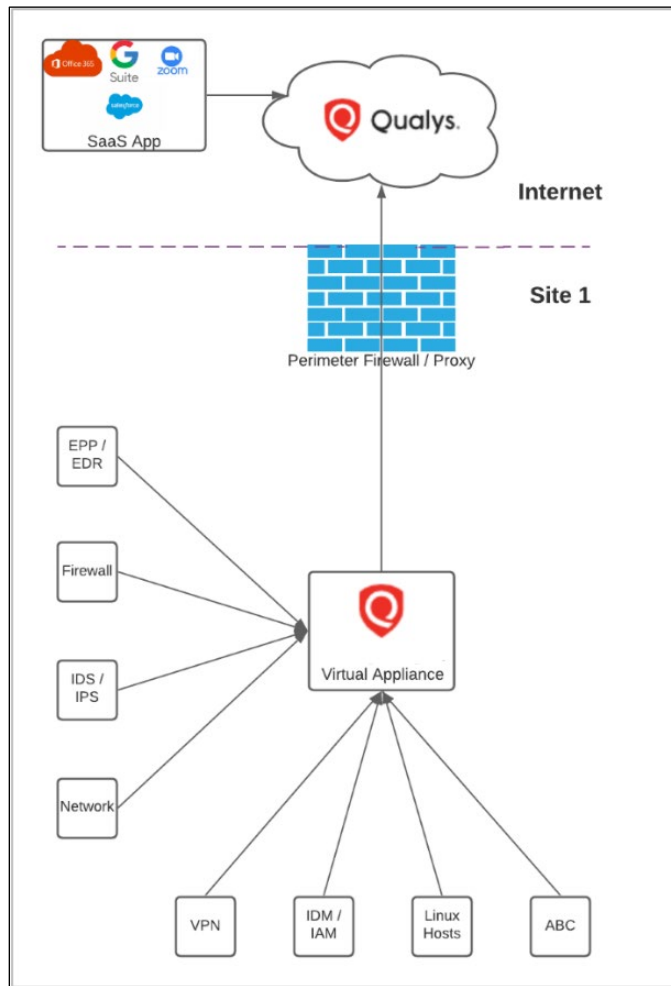
What's Next

Contact your Solution Architect for details on 'Day 1 – Data Collection'.

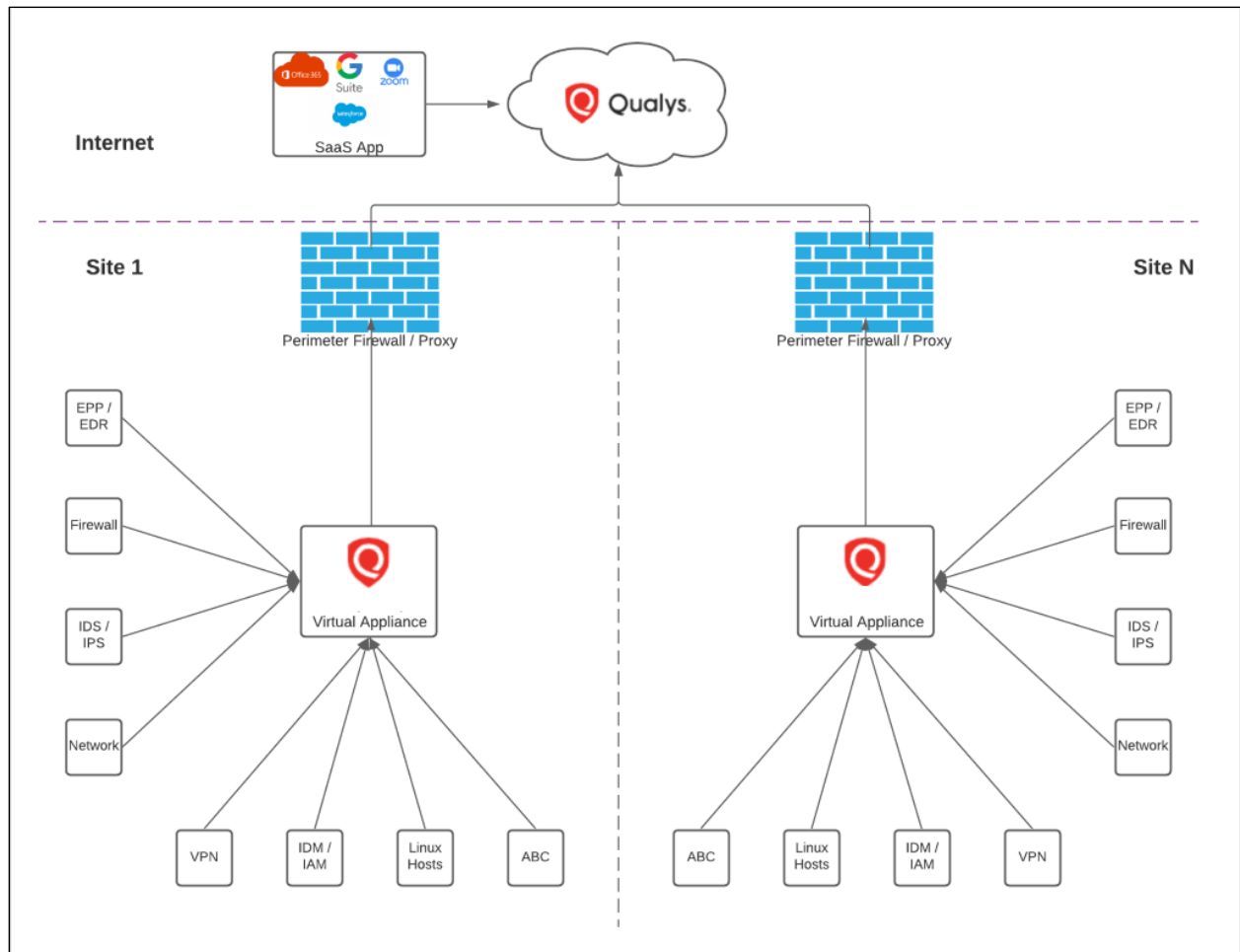
Appendix A – Appliance Deployment

Virtual Machine Deployment

Single-Site



Multi-Site



Appendix B - Windows Cloud Agent Requirements

Click [Cloud Agent Platform Availability Matrix \(PAM\)](#) to view the agent versions and their supported platforms.

Qualys certifies the two latest Agent releases for new operating systems and their updates. While not explicitly certified, all Agent versions that are not End-of-Service should also support these operating systems.