Advanced scenarios for ESET Bridge with ESET PROTECT (10.x and later)

Mitch | ESET Nederland - 2023-02-09 - Reacties (0) - ESET PROTECT

Issue

> Apache HTTP Proxy users
>
> ESET Bridge replaces Apache HTTP Proxy in ESET PROTECT version 10. All ESET product versions compatible with Apache HTTP Proxy are in Limited Support status. If you currently use Apache HTTP Proxy, we recommend that you migrate to ESET Bridge.

Details

Click to expand

- Download ESET Bridge for Windows
- Download ESET Bridge for Linux

These installers have the correct configuration necessary for the following:

- Forwarding ESET Management Agents' replication (communication with ESET PROTECT server)
- Caching ESET detection engine updates and installer files
- Caching ESET LiveGuard Advanced analysis results

See the instructions for ESET Bridge installation on Windows or ESET Bridge installation on Linux.

Solution

About ESET Bridge

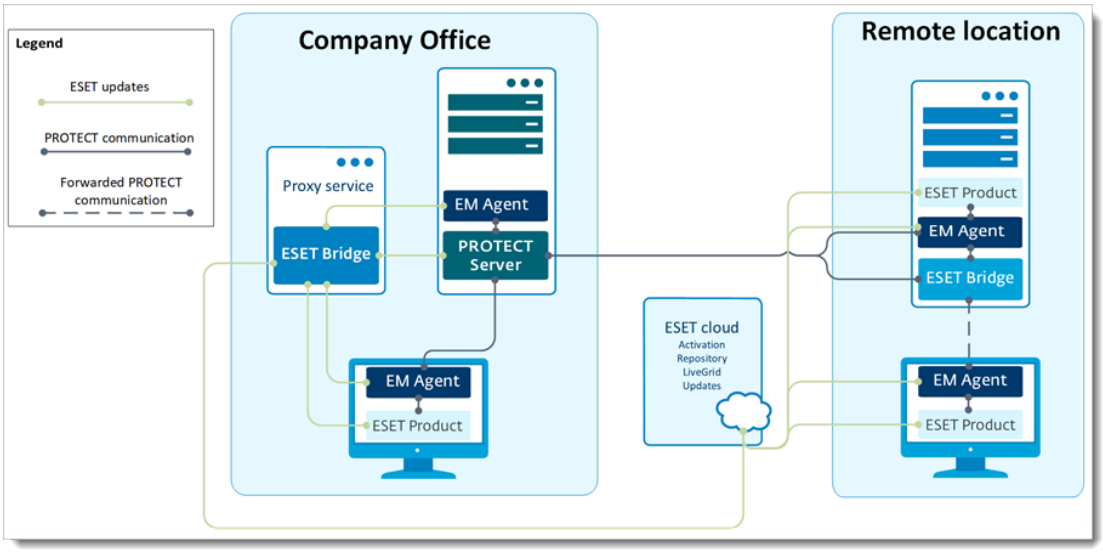
> HTTPS traffic caching is not supported
>
> ESET Bridge does not support HTTPS traffic caching for Windows Server/Linux/macOS security products.

ESET Bridge is a new ESET software based on the open-source nginx

software adjusted for the needs of ESET security solutions. ESET distributes ESET Bridge with ESET PROTECT 10.0 (and later) as a Proxy component replacing the former Apache HTTP Proxy.

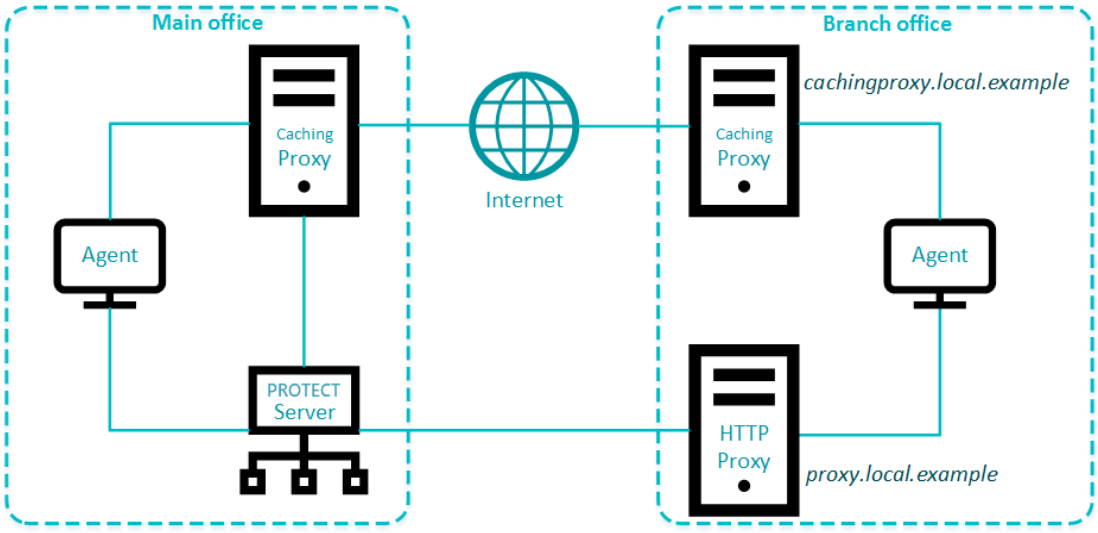
See the comparison of ESET Bridge and Apache HTTP Proxy. You can use ESET Bridge also with ESET PROTECT Cloud. You can connect up to 10,000 computers to ESET PROTECT using ESET Bridge.

Read more about ESET Bridge on ESET Online Help.



Use different proxy solutions for caching and replication

Users in some environments may need to use separate proxy solutions for caching and replication. In the example below, one branch office uses a separate proxy for caching and another for replication to the ESET PROTECT Server in the main office.

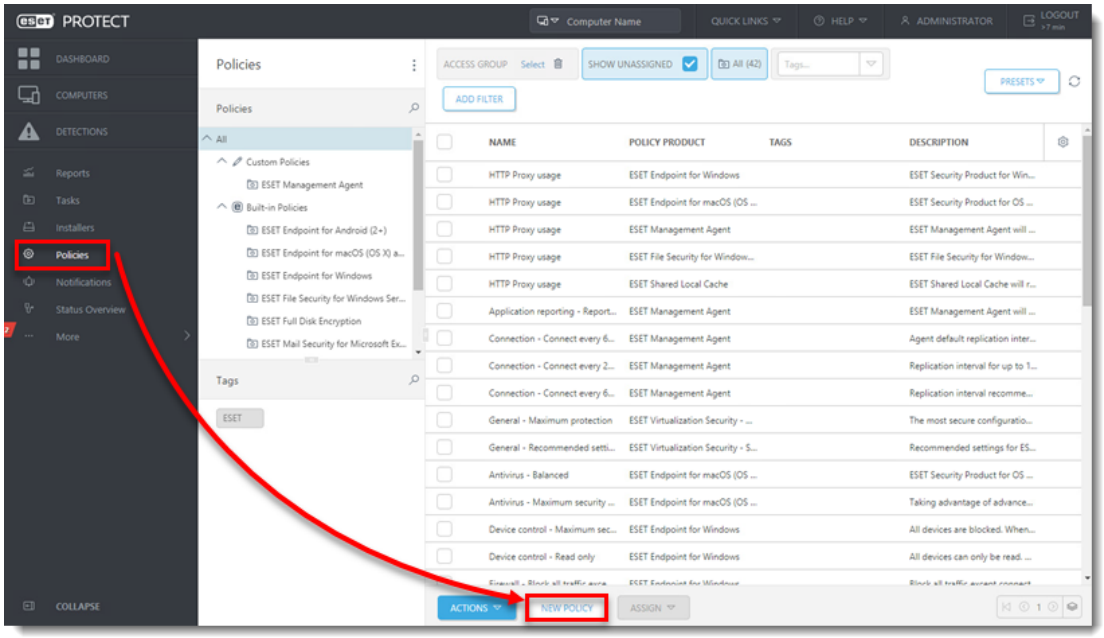


Configure an Agent to use different proxies

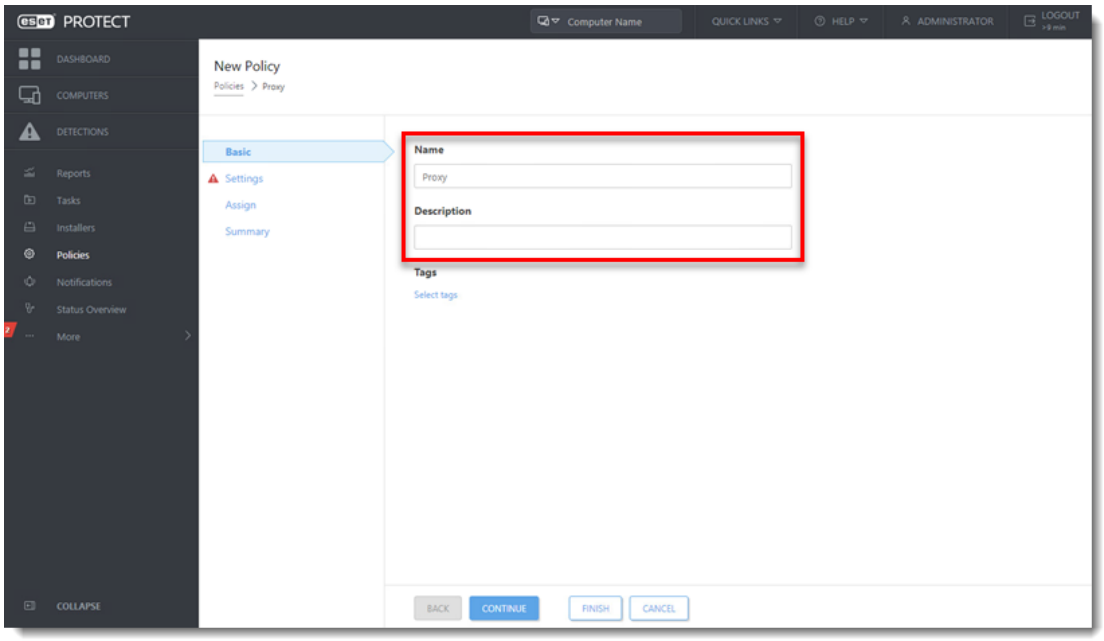
The proxy settings are located in the Agent policy. To configure them, create a new Agent policy or modify an existing one. You can also create multiple Agent policies with different proxy setups and assign them to computers using dynamic groups. When a client machine is moved to a different dynamic group, it will automatically use the appropriate proxy setup.

To set up different proxies follow these steps:

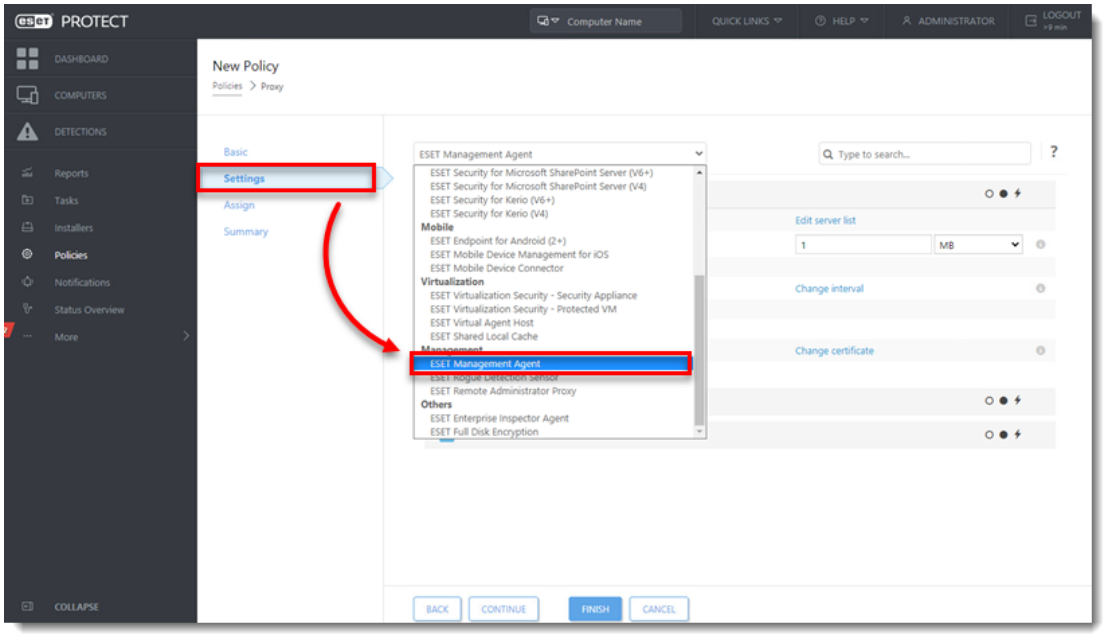
1. Open the ESET PROTECT Web Console in your web browser and log in.
2. Click Policies → New Policy.



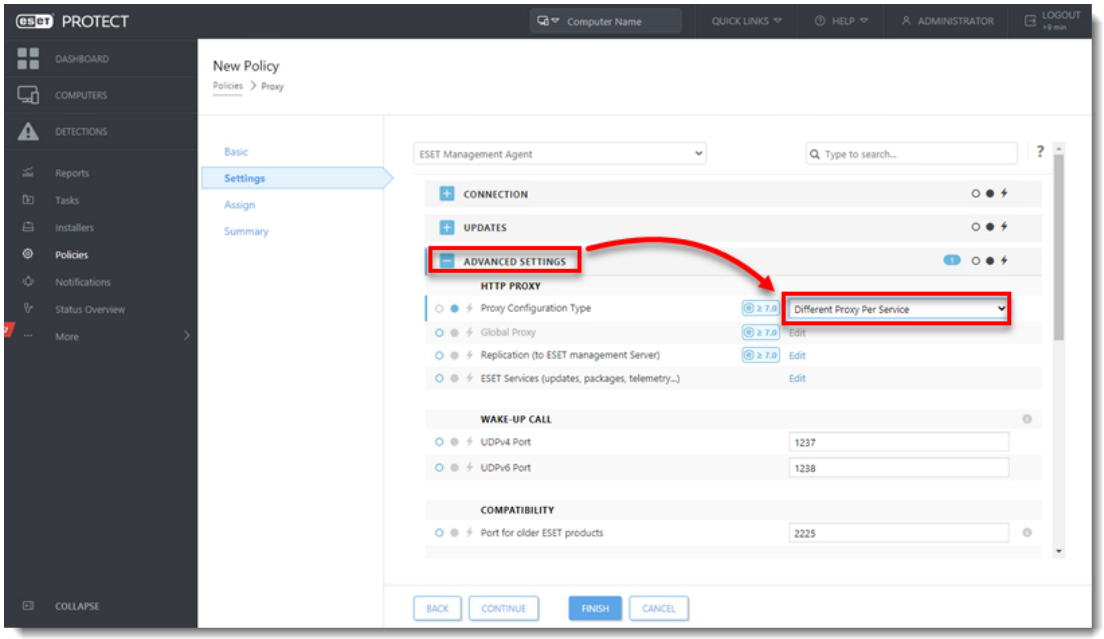
1. In the **Basic** section, type a **Name** and **Description** (the **Description** field is optional).



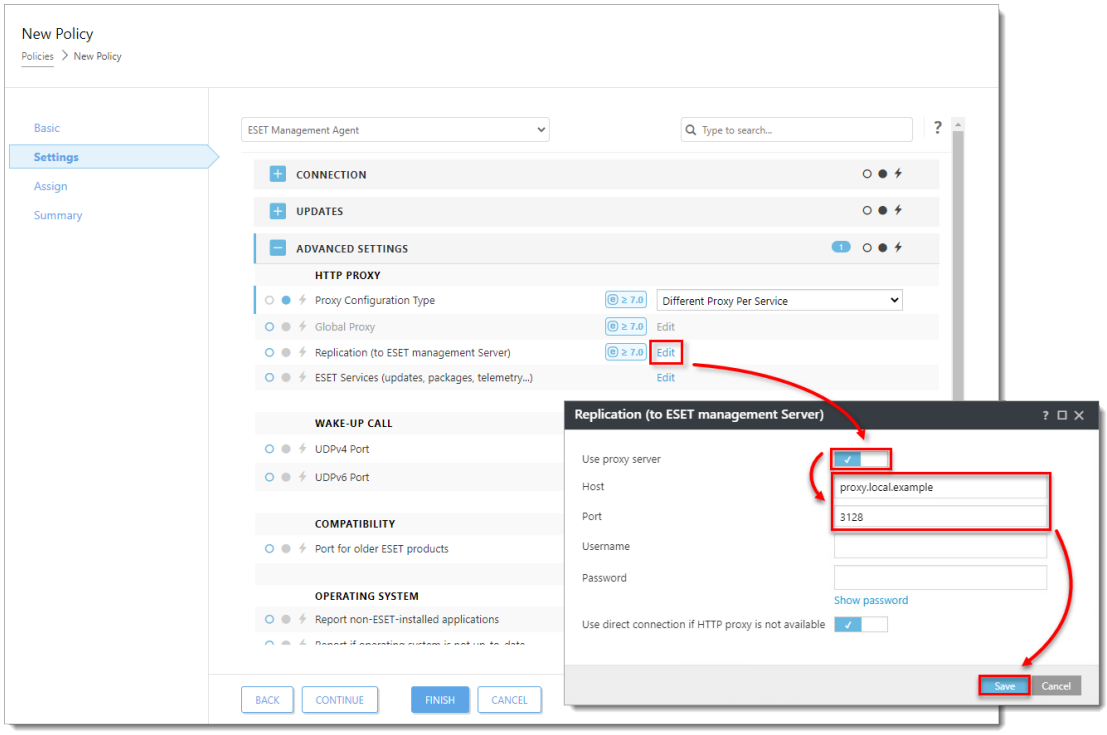
1. Click **Settings** and select **ESET Management Agent** from the drop-down menu.



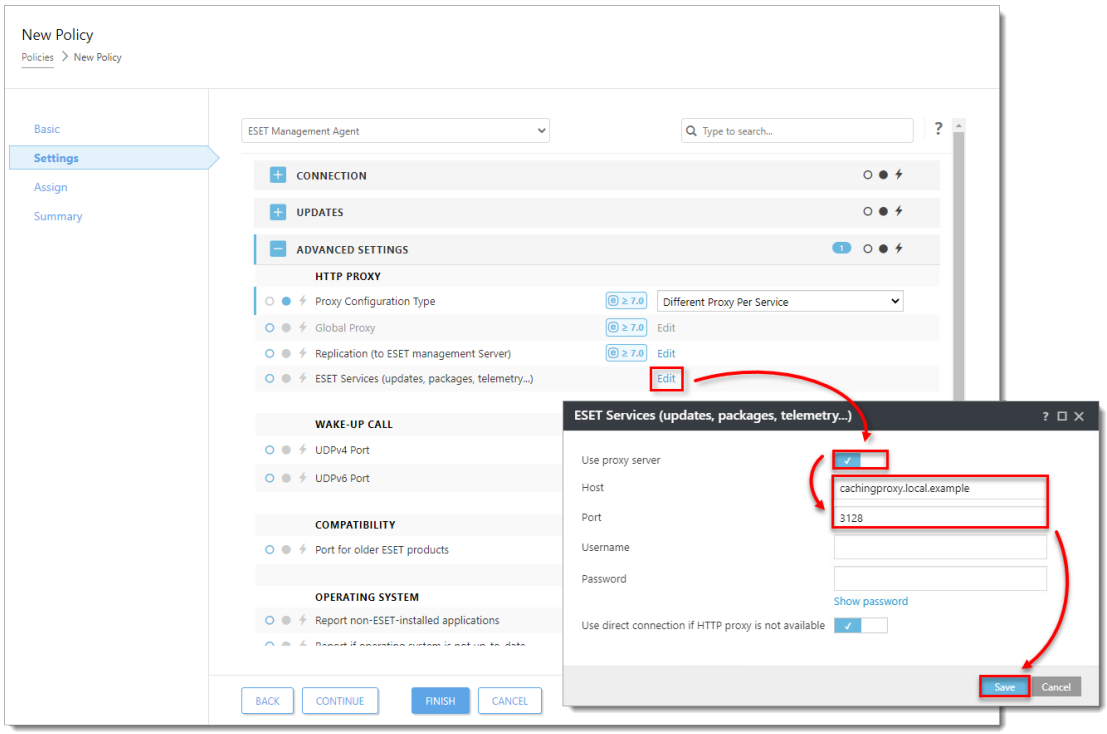
1. Expand **Advanced Settings**. In the **HTTP Proxy** section, change the **Proxy Configuration Type** to **Different Proxy Per Service**.



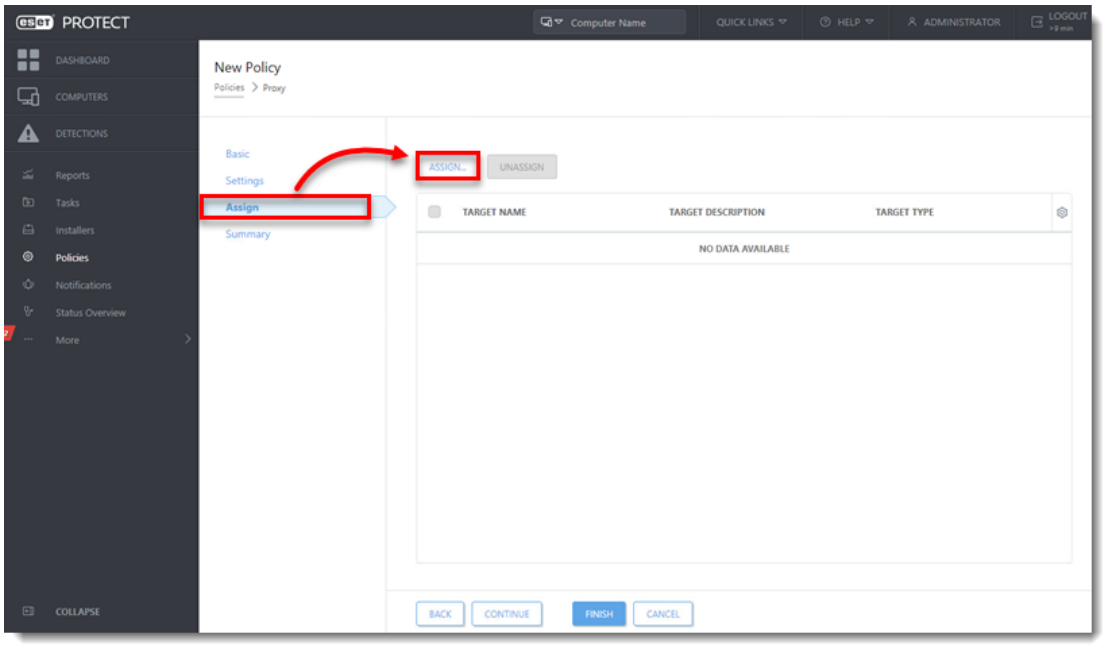
1. Click **Edit** next to **Replication (to ESET Management Server)**. Click the toggle next to **Use proxy server** to enable it and type the **Host** value. **Port** is set to 3128 by default. **Host** is the hostname or IP address of the machine where the proxy is running. Do not type a **Username** or **Password**. Click **Save**.



1. Click **Edit** next to **ESET Services (updates, packages, telemetry...)**. Click the toggle next to **Use proxy server** to enable it and type the **Host** value. **Port** is set to 3128 by default. **Host** is the hostname or IP address of the machine where the proxy is running. Click **Save**.



1. Click **Assign** → **Assign**. Select a group or multiple machines that will use the new proxy setting.

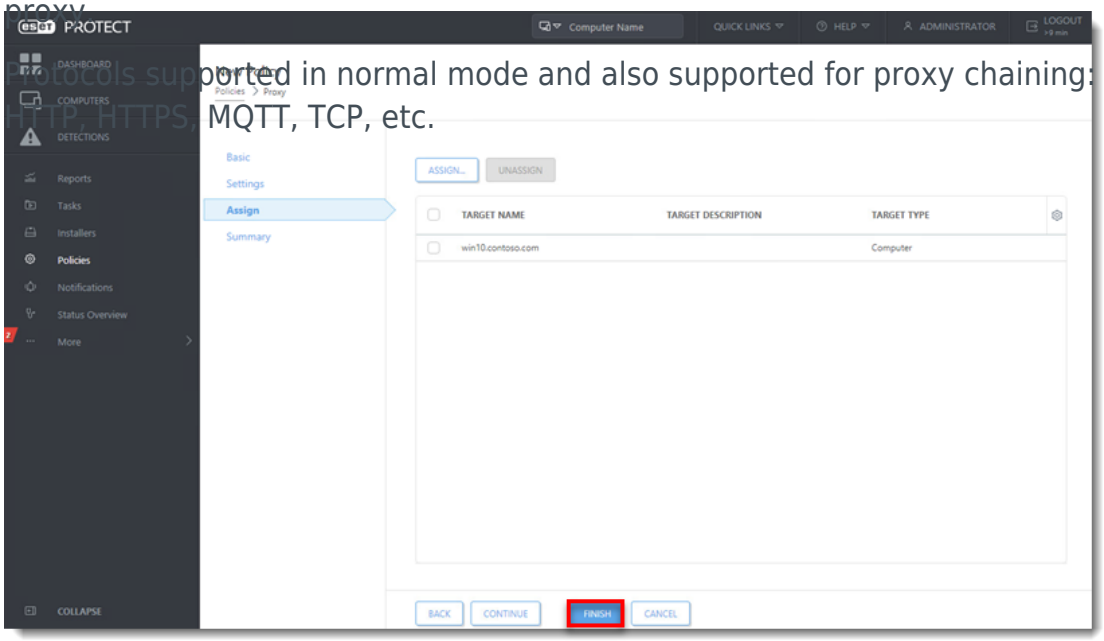


1. Click **Finish** to apply the policy.

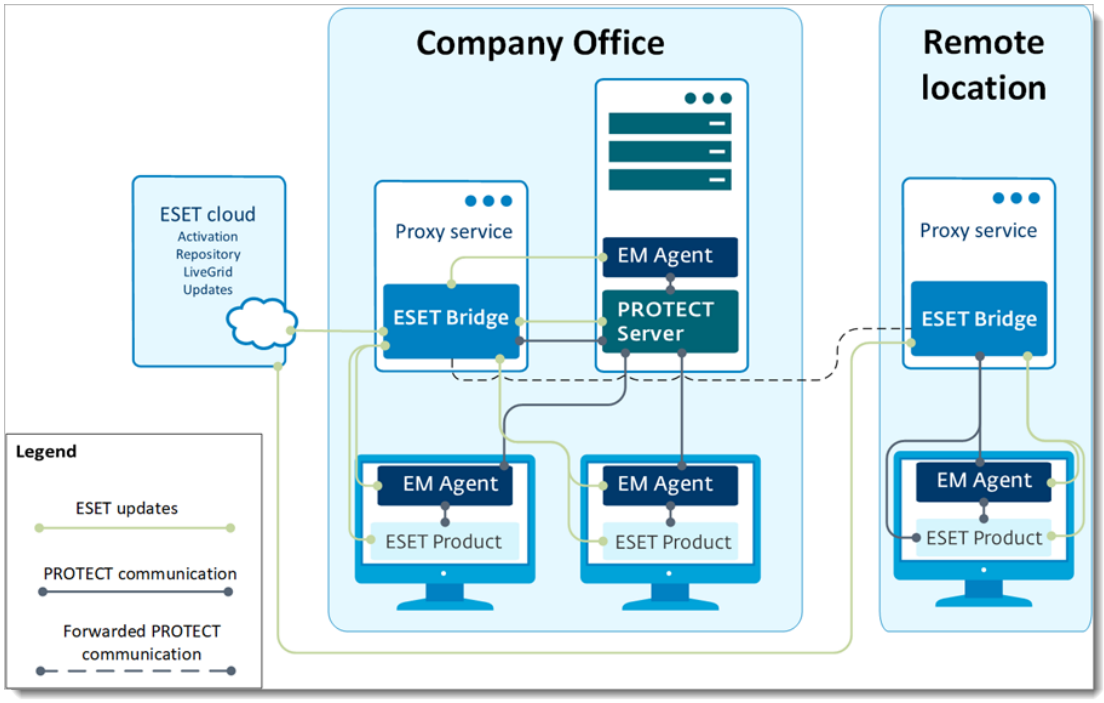
Set up a proxy chain

> Caching is not supported in proxy chaining mode
>
> The proxy chaining mode does not support caching.
>
> This limitation will be removed in the next ESET Bridge release.

ESET Bridge supports proxy chaining—it can forward the traffic to a remote proxy.



Protocols supported in normal mode and also supported for proxy chaining: HTTP, HTTPS, MQTT, TCP, etc.



See the instructions for setting ESET Bridge in the proxy chaining mode.

ESET Bridge in an environment with DMZ

In a more complex infrastructure, with a subnet that separates an internal LAN from untrusted networks (DMZ), it is recommended to deploy the ESET PROTECT server out of the DMZ. Figure 5-1 illustrates one deployment scenario.

When setting up an environment such as this, we recommend adhering to the following guidelines:

- Use hostnames instead of IP addresses in ESET PROTECT component settings.
- If client machines can leave the intranet (roaming clients): use dynamic groups and policies to make sure roaming clients use the server hostname resolvable from the internet only when they are outside of the intranet. Clients that cannot leave the intranet should use a hostname that is resolvable only inside the intranet, to be sure their connection is not routed via the internet.
- ESET Bridge (when used for replication) does not aggregate connections from Agents and does not save bandwidth. Use ESET Bridge for replication only if necessary.

- Using ESET Bridge for caching updates and installers is recommended. Roaming agents should not use caching proxy when outside of the intranet. This can be achieved by using a hostname for caching proxy which is not resolvable outside of the intranet and allowing a direct connection.

- Firewall: open only necessary ports (see the list of used ports) for selected hostnames.

