Migrate from ERA Proxy (Linux or Virtual Appliance) to Apache HTTP Proxy in ESET PROTECT (8.x)

Steef | ESET Nederland - 2020-12-10 - Reacties (0) - Legacy

Issue

- You have an ESET Remote Administrator (ERA) 6.x environment running with an ERA Proxy on a Virtual Appliance, and you want to upgrade to ESET PROTECT, which does not support ERA Proxy
- You want to enable an Apache HTTP Proxy on a Virtual Appliance to substitute the role of an ERA Proxy in ESET PROTECT
- Migrate from ERA Proxy (Windows) to Apache HTTP Proxy in ESET PROTECT

Details

ESET PROTECT introduces a new generation of the agent/server communication protocol. The new replication protocol uses TLS and HTTP2 protocols so it can go through proxy servers. There are also new self-recovery features and a persistent connection that improves overall communication performance.

> ERA Proxy 6.x users
> The new communication protocol does not support a connection using ERA Proxy 6.x.

ESET provides a pre-configured Apache installer. The user can also use other proxy solutions (besides Apache HTTP Proxy) that fulfill the following conditions:

- Can forwardSSLcommunications
- SupportsHTTP CONNECT
- Can work without authentication (the ESET Management Agent does not support authentication with proxy)

The configuration of other proxy solutions is not provided or supported by ESET. Other solutions may not support caching of ESET Dynamic Threat Defense (EDTD) communications.

The ESET PROTECT Virtual Appliance contains a correctly pre-configured Apache HTTP Proxy. We recommend you use the new appliance instead of upgrading the old one.

Solution

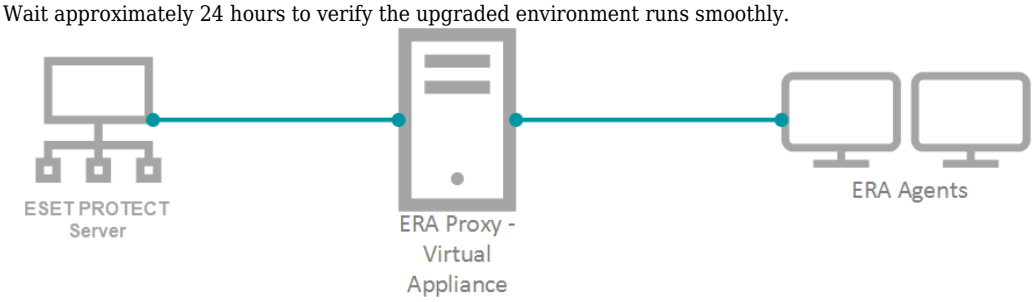
Connection limitations

- The ERA 6.x Proxy component is discontinued in ESET PROTECT.
- ERA 6.x Agents can connect to the ESET PROTECT Server.
- The ESET Management Agent 7 cannot connect to the ESET PROTECT Server via ERA Proxy or the ERA 6.x Server.
- Do not upgrade ERA 6.x Agents before a proper proxy solution is set up.
- It is not possible to run theAgent deployment taskon clients with an ESET PROTECT Server. The Agent deployment task can only reach the ESET PROTECT Server using Apache HTTP Proxy.

I. Prepare your ERA 6.x environment

1. Back up your ERA Server (for example,backup database,CAandcertificates).
2. Upgrade ESET Security Management Center to the latest ESET PROTECTvia an ESET **PROTECT Components Upgrade Task**. This task updates the server, agent and web console. When assigning a target for the task, only select the machine with the ERA Server.

3. Wait approximately 24 hours to verify the upgraded environment runs smoothly.



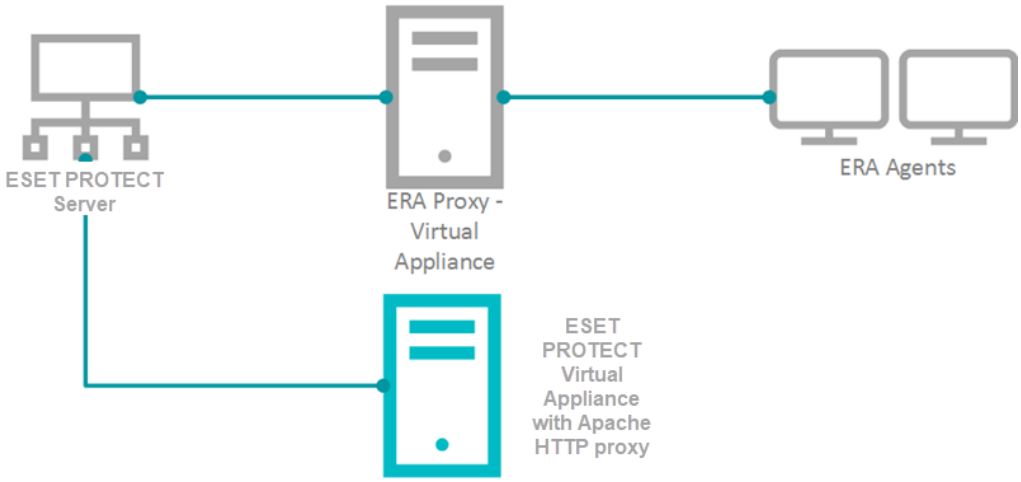
II. Deploy the new Virtual Appliance and connect it to your ESET PROTECT Server

To keep your proxy safe and well configured, replace your old ERA Proxy - Virtual Appliance with the new version. ESET PROTECT does not provide a stand-alone proxy configuration as ERA 6.x did. We recommend you deploy a new ESET PROTECT Server - Virtual Appliance. The new server is not used as an administrative server but as a proxy. The correctly configured Apache HTTP Proxy is included in the ESET PROTECT Virtual Appliance download.

1. Download the ESET PROTECT Virtual Appliance.
2. Deploy the ESET PROTECT Virtual Appliance on your hypervisor.
3. Configure the new Appliance as an ESET PROTECT Server.
   - You will be prompted for the new password later in the process.
   - Enable HTTP Forward Proxy during the configuration.
4. Reinstall the ESET Management Agent on the appliance and connect it to the main ESET PROTECT Server. Open the virtual machine with your ESET PROTECT Virtual Appliance → **Enter Management mode** → enter your password → **Login** → **Exit to terminal**.
5. The Agent installer is located at: `/root/eset_installers/Agent-Linux-x86_64.sh`
   We recommend you use the server-assisted installation. For example:

   ```
   /root/eset_installers/Agent-Linux-x86_64.sh \
   --skip-license \
   --hostname=10.1.179.36 \
   --port=2222 \
   --webconsole-user=Administrator \
   --webconsole-password=aB45$45c \
   --webconsole-port=2223
   ```

   Replace the hostname and password values with actual values from the main ESET PROTECT Server. For more information, refer to the Agent installation - Linux topic in the ESET PROTECT Online Help Guide.



6. If required, you can stop certain services on the new appliance to save resources.
   In the Terminal, run the applicable commands:

System V init	Systemd
`service eraserver stop`	`systemctl stop eraserver`
`service mysql stop`	`systemctl stop mysql`
`service tomcat stop`	`systemctl stop tomcat`

To prevent ESET PROTECT and MySQL services from starting after reboot, disable them:

Systemd
`systemctl disable eraserver`
`systemctl disable mysql`
`systemctl disable tomcat`

7. Modify the Apache HTTP Proxy configuration file */etc/httpd/conf.d/proxy.conf*. Use the **nano** editor in the Terminal or access the file using Webmin. For nano, use the following command:

   ```
   nano /etc/httpd/conf.d/proxy.conf
   ```

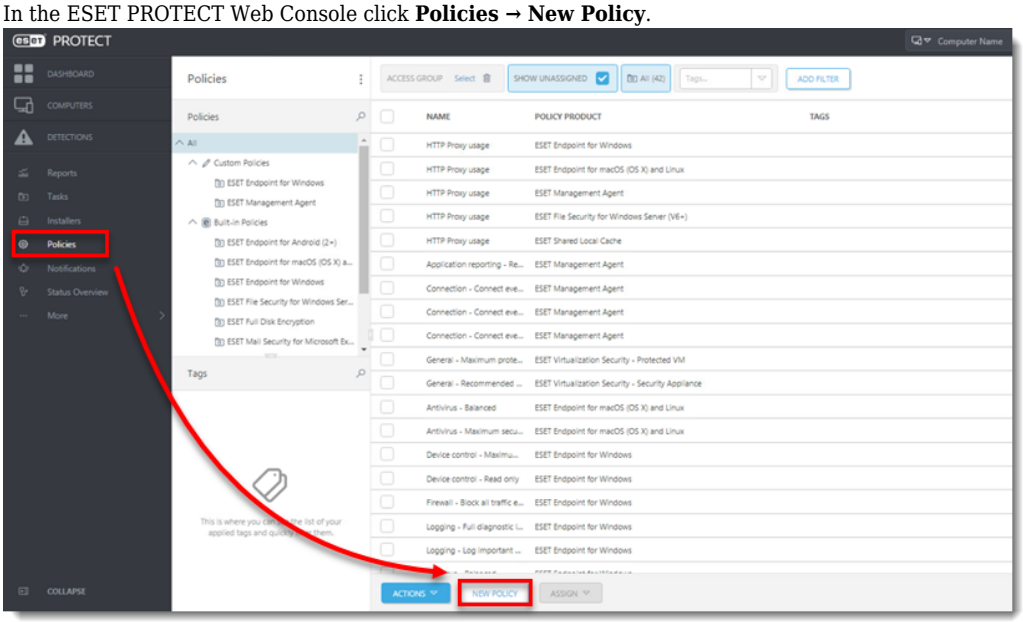
   1. If you have changed the default port (2222) for the agent, find the line `AllowCONNECT 443 2222` and change `2222` to the number of your port.
   2. Add the hostname or IP address of your ESET PROTECT Server to the configuration file. The hostname you add must be exactly the same as the hostname agents use to connect to the ESET PROTECT Server. You can also add a ProxyMatch expression.
   3. Close the file and save the changes.
   4. Restart the **Apache HTTP Proxy** service.

      ```
      systemctl restart httpd
      ```

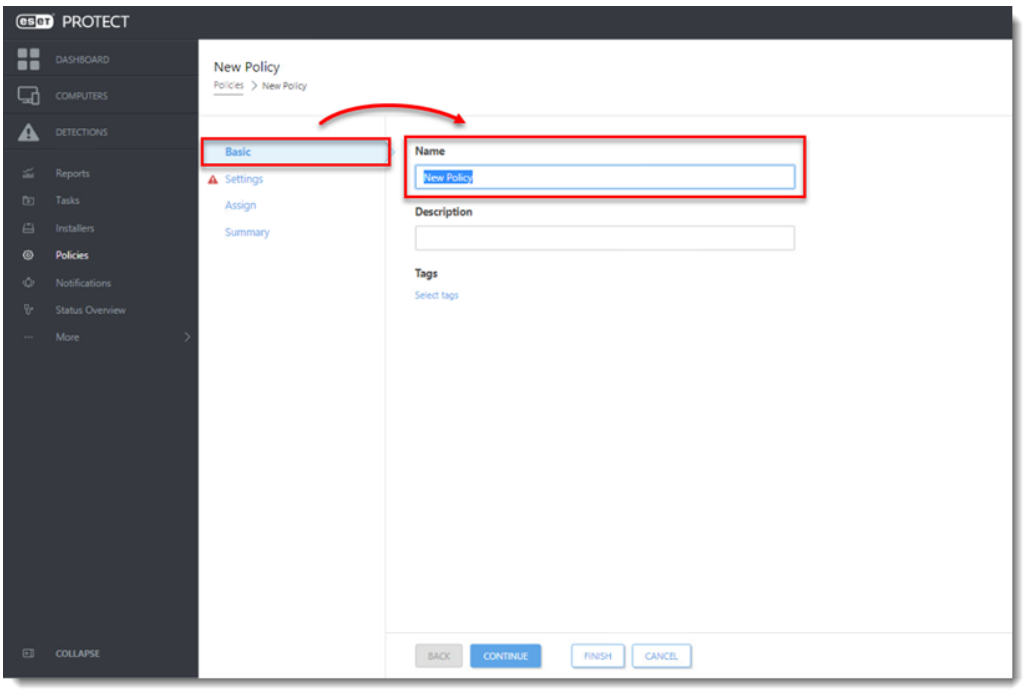
8. Open ESET PROTECT Web Console in your web browser and log in.
   If the new agent is connecting, use it for future maintenance of the proxy machine.

III. Assign a transition policy to a test client

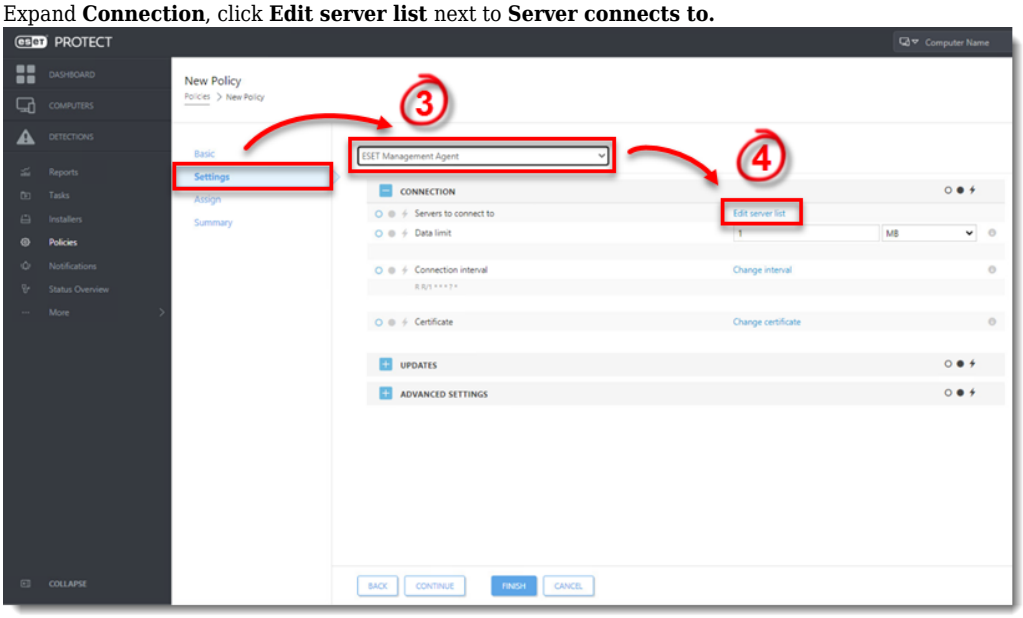
1. In the ESET PROTECT Web Console click **Policies → New Policy**.



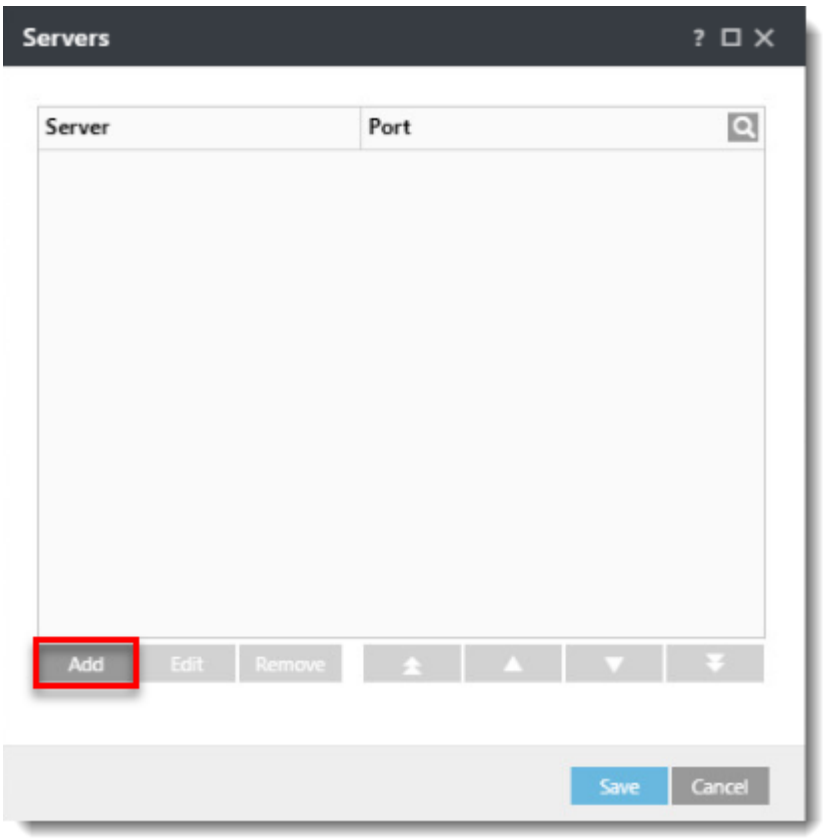
2. Type a **Name** for the policy.



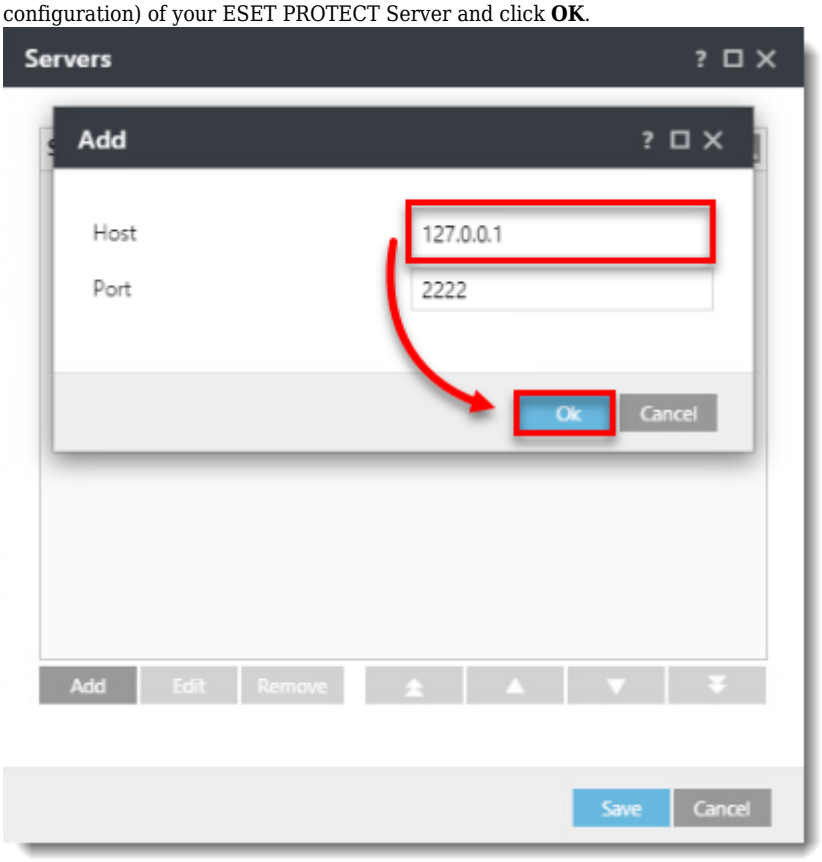
3. Click **Settings**, select **ESET Management Agent**.
4. Expand **Connection**, click **Edit server list** next to **Server connects to.**



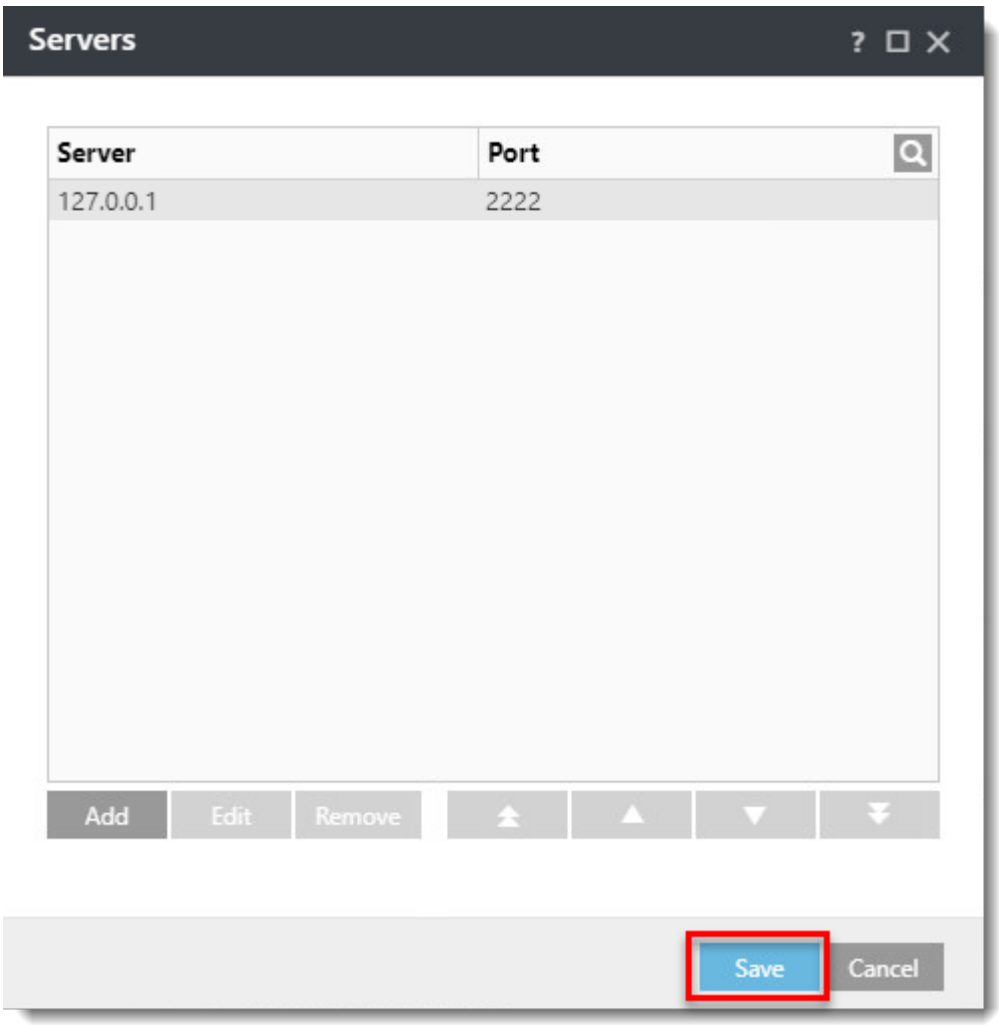
5. Click **Add**.



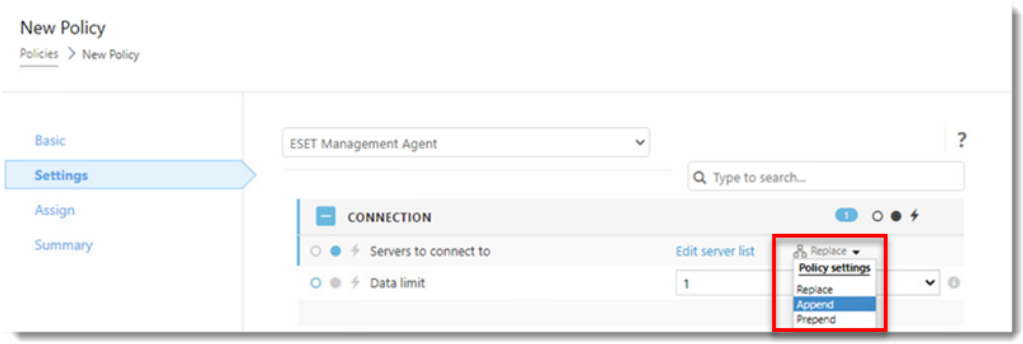
6. In the **Host** field, type the applicable address (the address must match what the agent uses in the configuration) of your ESET PROTECT Server and click **OK**.



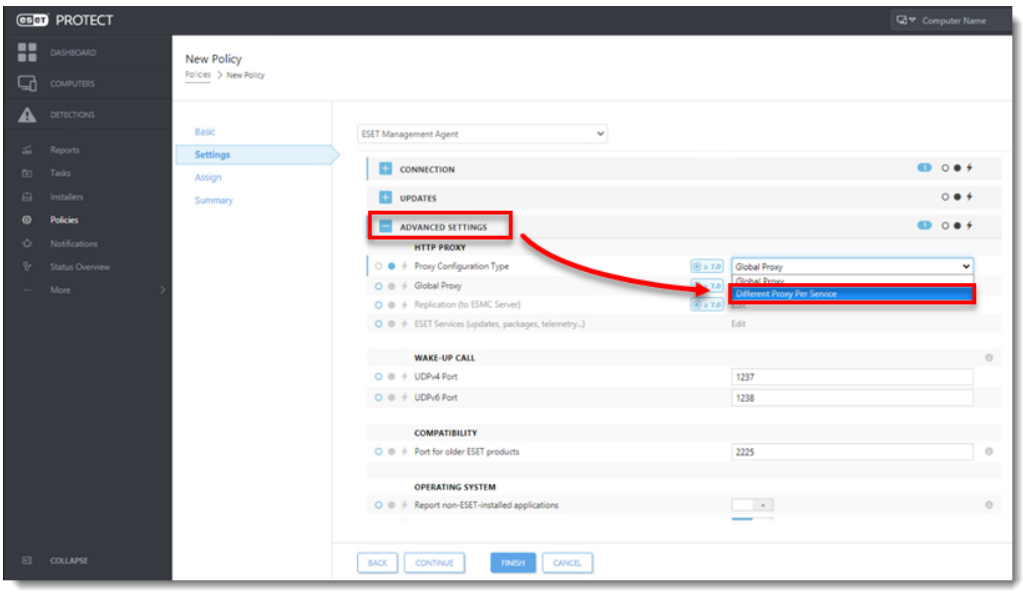
7. Click **Save**.



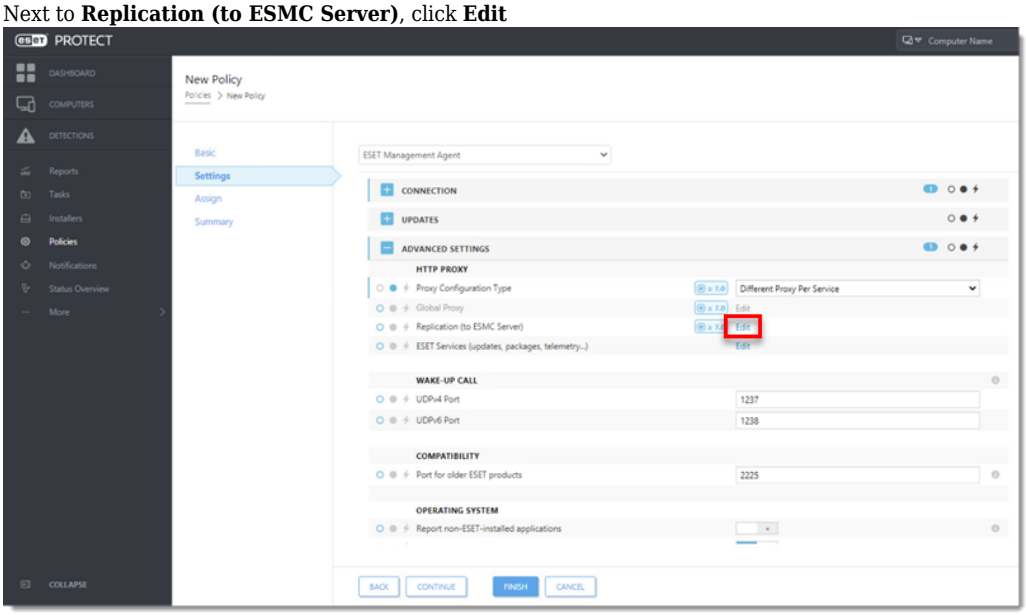
8. In the **Policy settings** drop-down menu, select **Append**.



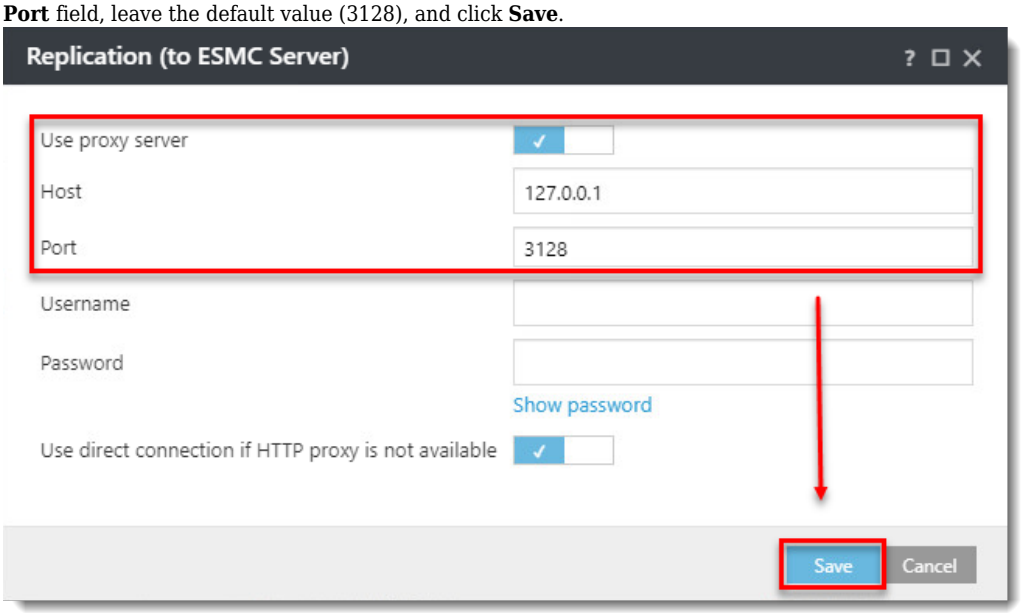
9. Expand **Advanced Settings**. In the **HTTP Proxy** section, select **Different Proxy Per Service** from the **Proxy Configuration** drop-down menu.



10. Next to **Replication (to ESMC Server)**, click **Edit**

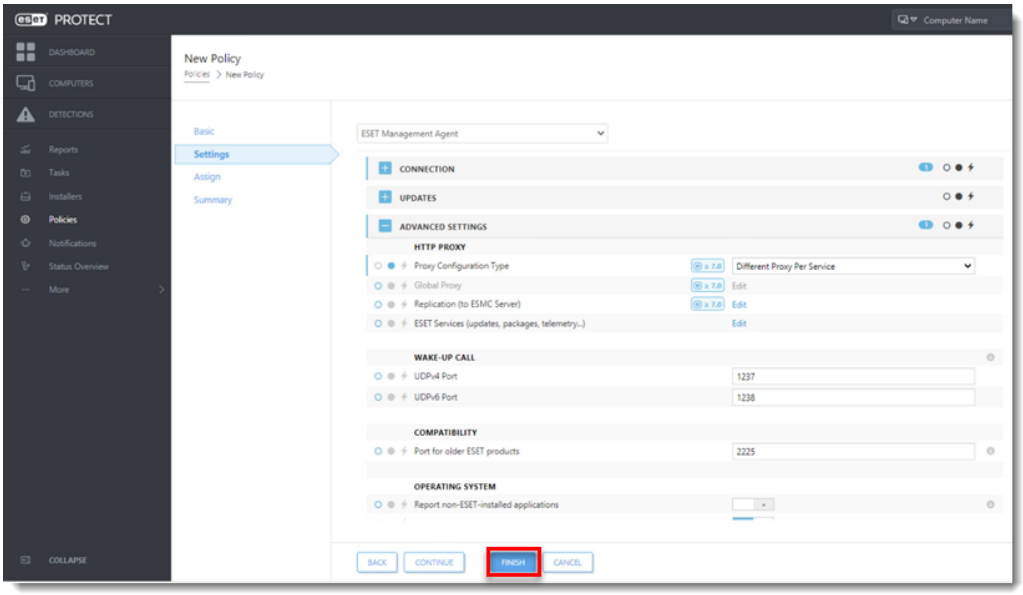


11. Enable the **Use proxy server.** In the **Host** field, type the IP address of the proxy machine. In the **Port** field, leave the default value (3128), and click **Save**.



12. Click **Finish** to save the policy. Do not assign it to a computer yet.

> **IP Addresses**
> It is necessary to have both IP addresses in one list applied to the client. If the agent does not have this information in the policy, it is unable to connect to the proxy and the ESET PROTECT Server after the upgrade. Such an agent must be fixed manually by running a repair installation and using the correct ESET PROTECT Server address. If the HTTP Proxy setting is not applied in the policy, the agent is able to connect to the ESET PROTECT Server.



13. Choose one computer that is connected via ERA Proxy and assign the new policy to that test client.
14. After a few minutes, verify the computer is still connecting to the ESET PROTECT Server.

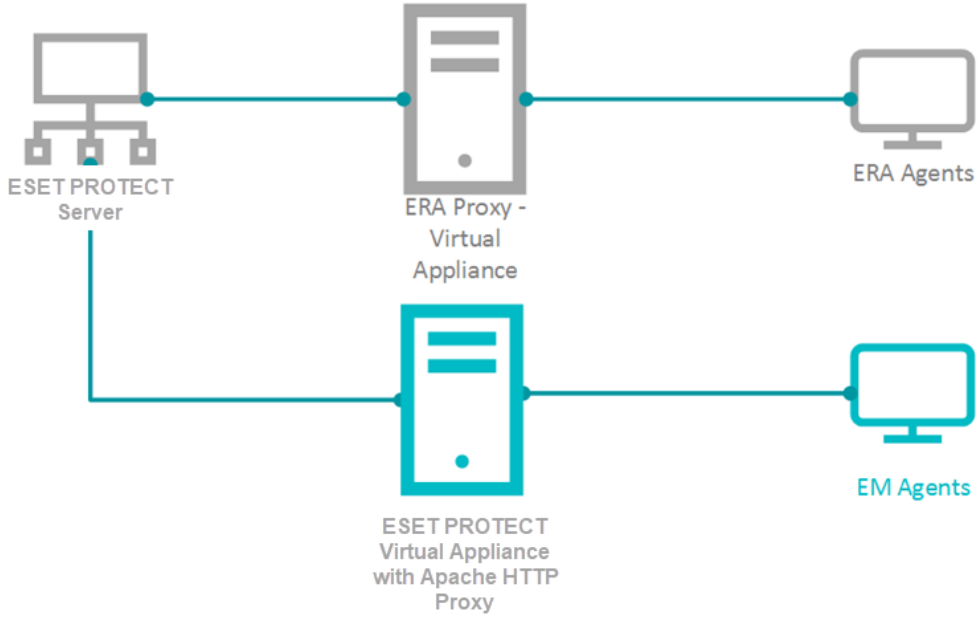
IV. Upgrade ERA Agents on client computers

1. Run an ESET PROTECT Components Upgrade Task.

2. Verify the client is connected to the ESET PROTECT Server. Continue upgrading the remaining clients.

> **Upgrades and troubleshooting**
> If you have a more extensive network, begin the upgrade with departments that include IT experienced users or those who are physically closer to their computers to make troubleshooting easier.

3. Apply the policy from part III to the other computers connected via the ERA Proxy.



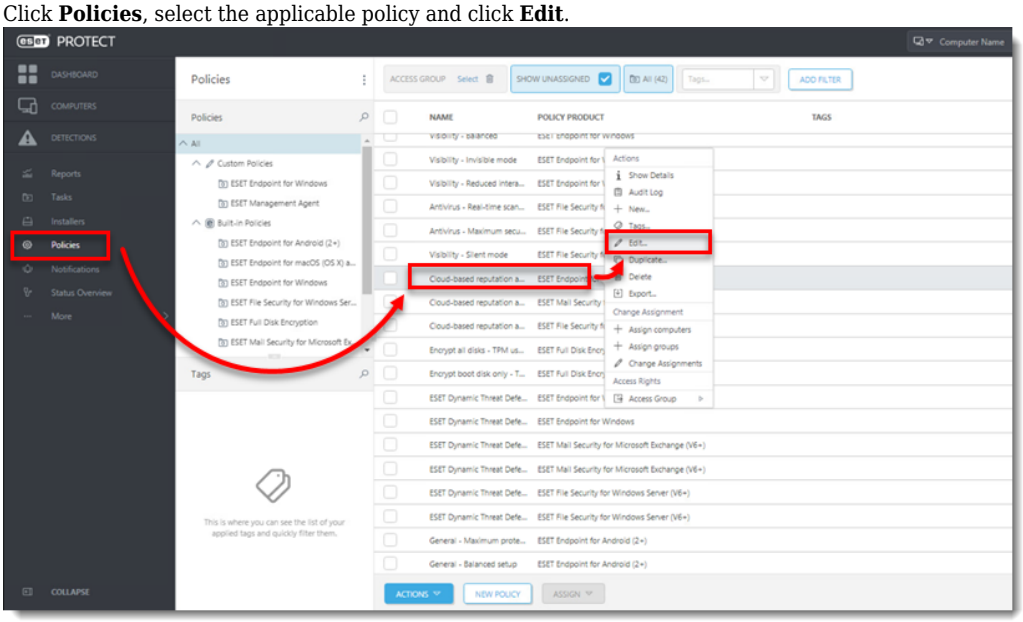
4. After the policy is applied, verify all clients are connecting to the ESET PROTECT Server.
5. Run an **ESET PROTECT Components Upgrade Task**.
6. If all clients are connecting to the ESET PROTECT Server after the upgrade is finished, proceed to

section V below.

V. Remove the ERA Proxy address from the list of servers

1. Open ESET PROTECT Web Console in your web browser and log in.

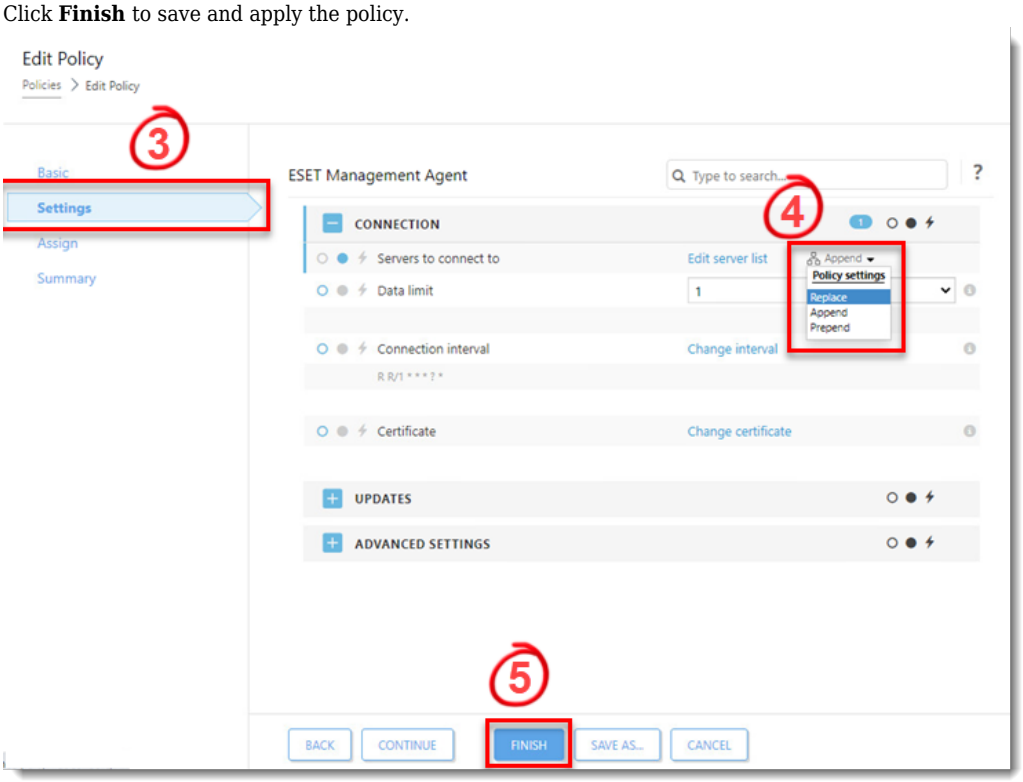
2. Click **Policies**, select the applicable policy and click **Edit**.



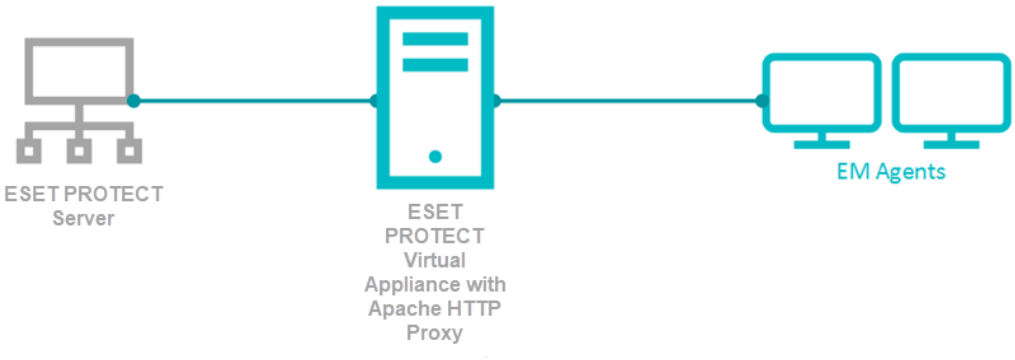
3. Click **Settings**.

4. **In the Policy settings drop-down menu, select Replace.**

5. Click **Finish** to save and apply the policy.



6. Remove the ERA Proxy Virtual Appliance (remove the virtual machine from the hypervisor).


ESET PROTECT
Server
ESET
PROTECT
Virtual
Appliance with
Apache HTTP
Proxy
EM Agents