ESET Tech Center

Migrate from ERA Proxy (Linux or Virtual Appliance) to Apache HTTP Proxy in ESMC 7

Anish | ESET Nederland - 2020-07-13 - Reacties (0) - 6.x

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 Security Management Center (ESMC) 7, 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 ESMC7
- Are you using an ERA Proxy on a Windows host?

Details

ESMC 7 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 ESMC 7 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 ESMC 7.
- ERA 6.x Agents can connect to the ESMC 7 Server.
- The ESET Management Agent 7 cannot connect to the ESMC 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 ESMC Server. The Agent deployment task can only reach the ESMC 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 your ERA Server to ESMC 7via aRemote Administrator 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.

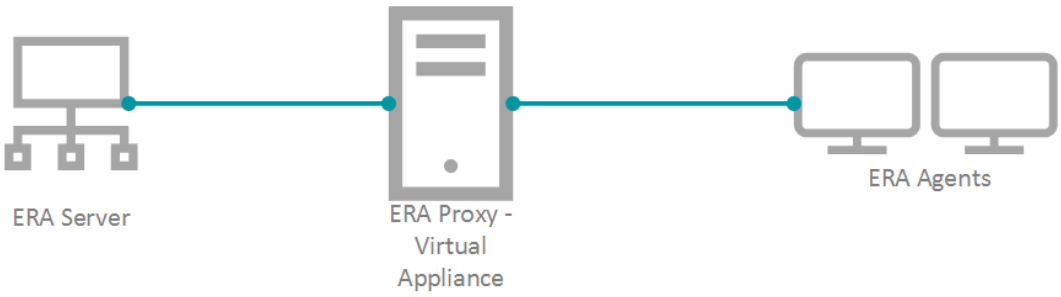

Figure 1-1

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

To keep your proxy safe and well configured, replace your old ERA Proxy - Virtual Appliance with the new version. ESMC 7 does not provide a standalone proxy configuration as ERA 6.x did. We recommend you deploy a new ESMC Server - Virtual Appliance. The new server is not used as an administrative server, but a proxy. The correctly configured Apache HTTP Proxy is included in the ESMC 7 Virtual Appliance download.

1. Download the ESMC 7 Virtual Appliance.
2. Deploy the ESMC 7 Virtual Appliance on your hypervisor.
3. Configure the new Appliance as an ESMC Server.

-
    - You will be prompted for the new password later in the process.
    - Enable HTTP Forward Proxy during the configuration.

1. Reinstall the ESET Management Agent on the appliance and connect it to the main ESMC Server. Open the virtual machine with your ESMC Virtual Appliance → Enter Management mode→ enter your password →Login→ Exit to terminal.
2. 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 ESMC Server. For more information, refer to theAgent installation - Linuxtopic in the ESMC Online Help Guide.

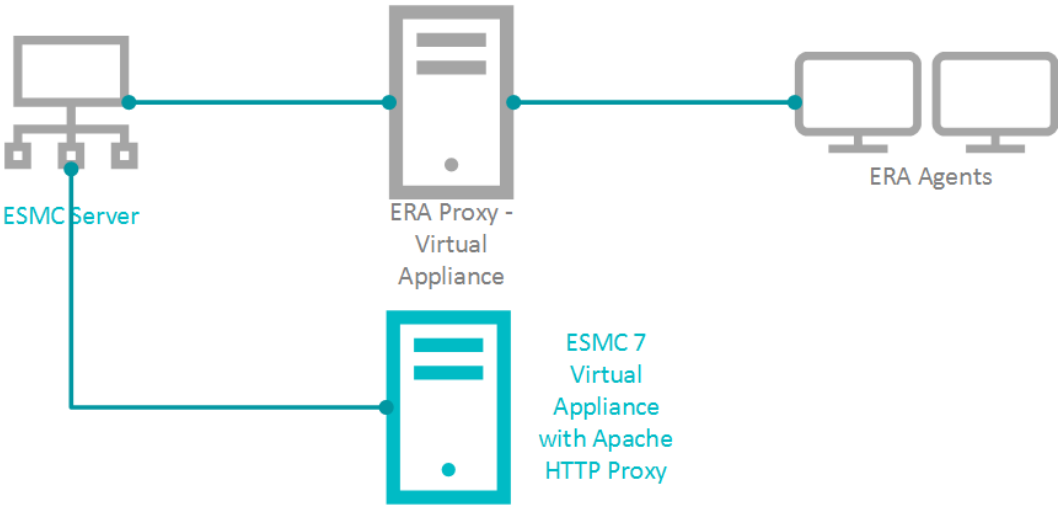

Figure 2-1

1. 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`

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

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

Systemd

```
systemctl disable eraserver

systemctl disable mysql

systemctl disable tomcat
```

2. Modify the Apache HTTP Proxy configuration file */etc/httpd/conf.d/proxy.conf.*Use thenanoeditor in the Terminal or access the file usingWebmin. 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 ESMC Server to the configuration file. The hostname you add must be exactly the same as the hostname agents use to connect to the ESMC Server. You can also add aProxyMatch expression.
   3. Close the file and save the changes.
   4. Restart the Apache HTTP Proxy service.

      ```
      systemctl restart httpd
      ```

3. Open the ESET Security Management Web Console(ESMC 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 ESMC Web Console click Policies →New Policy.

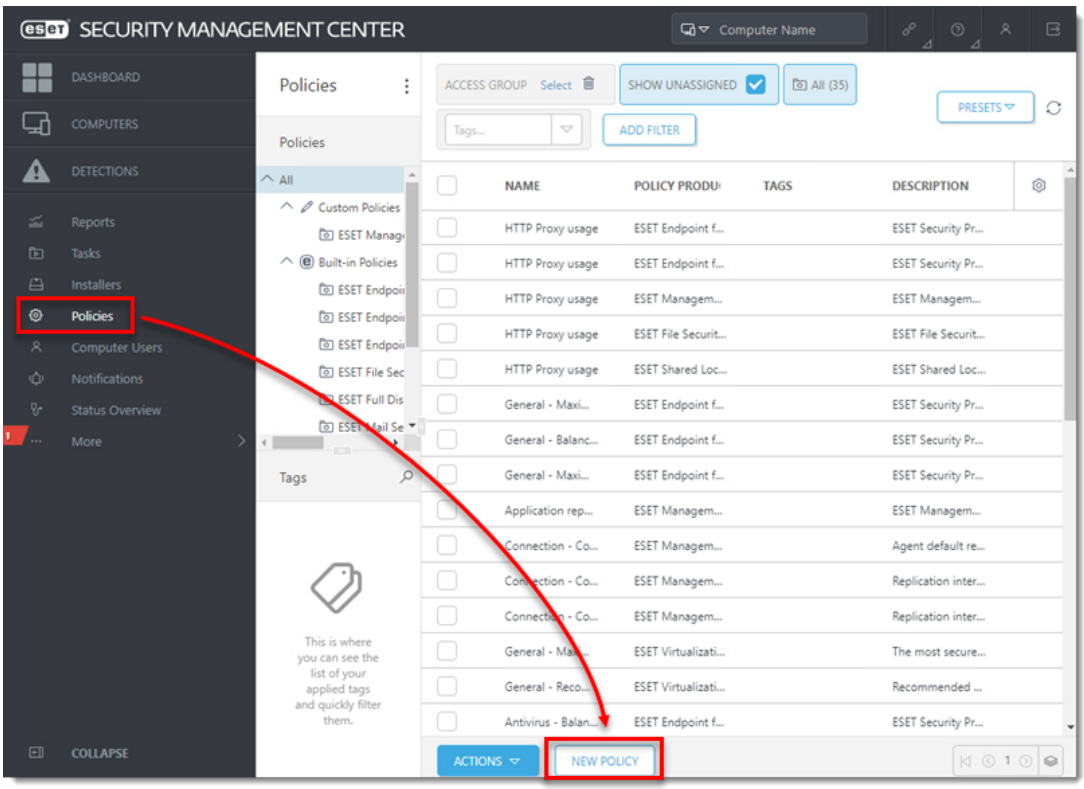

Figure 3-1

1. Type aName for the policy.

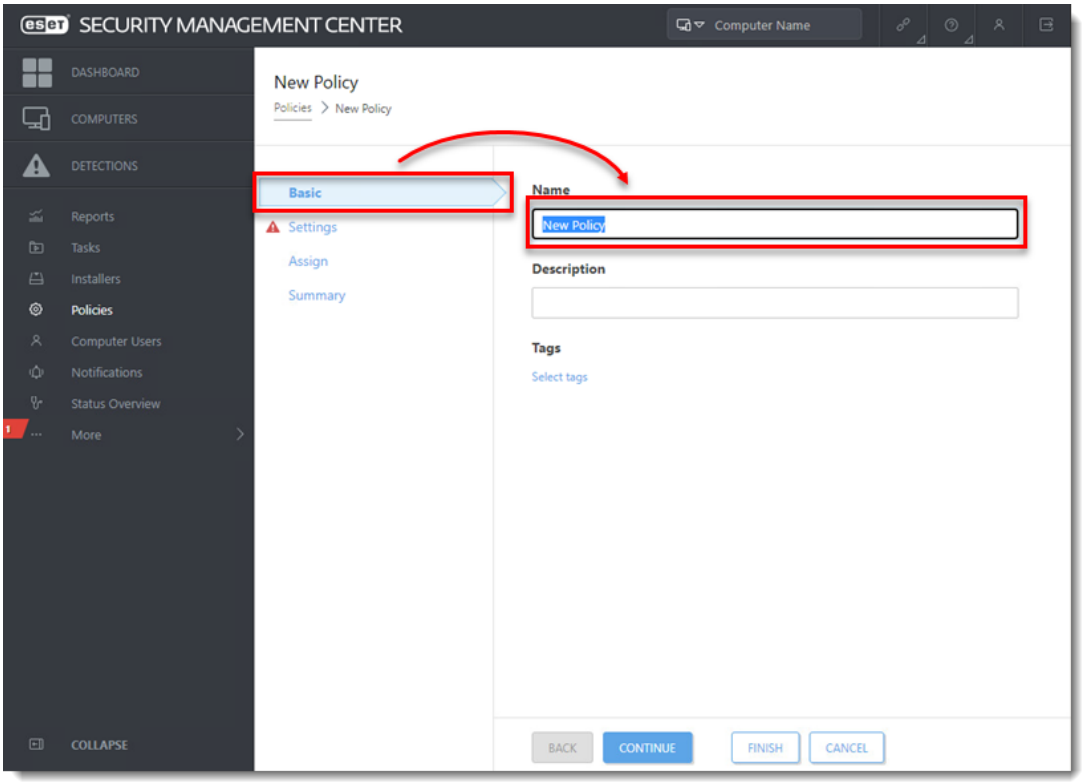

Figure 3-2

1. ClickSettings, select ESET Management Agent.
2. In theConnectionsection, next to Server connects to,clickEdit server list.

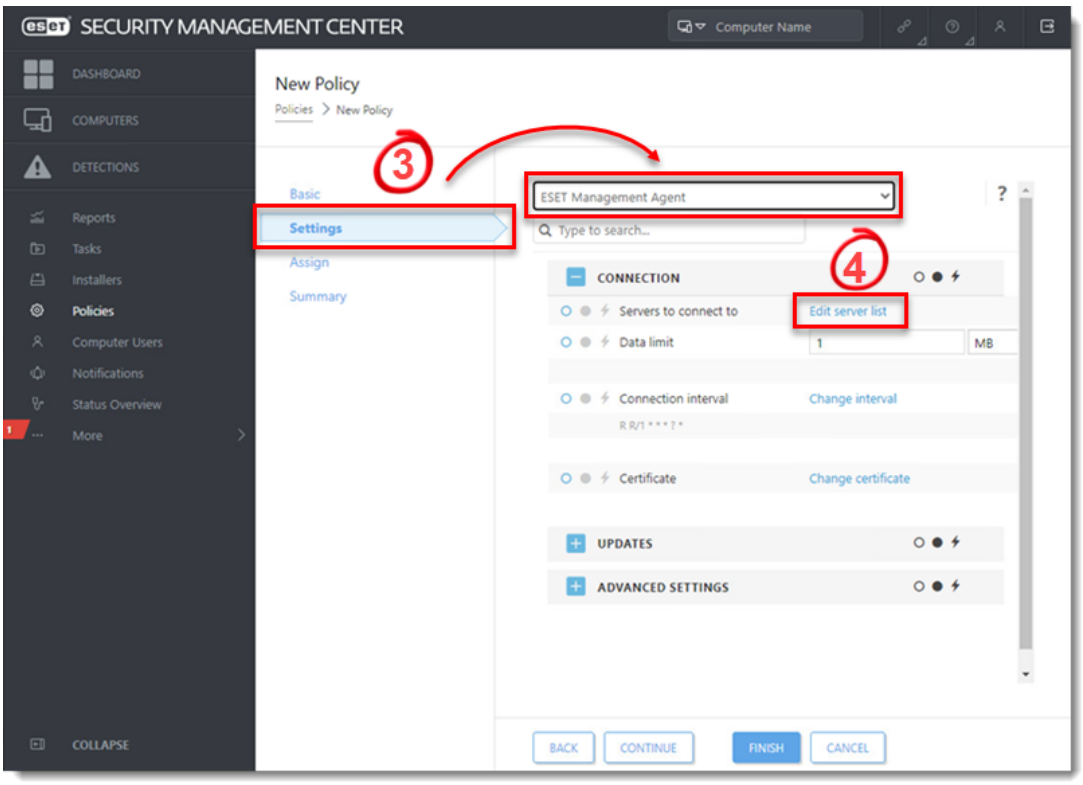

Figure 3-3

1. ClickAdd.

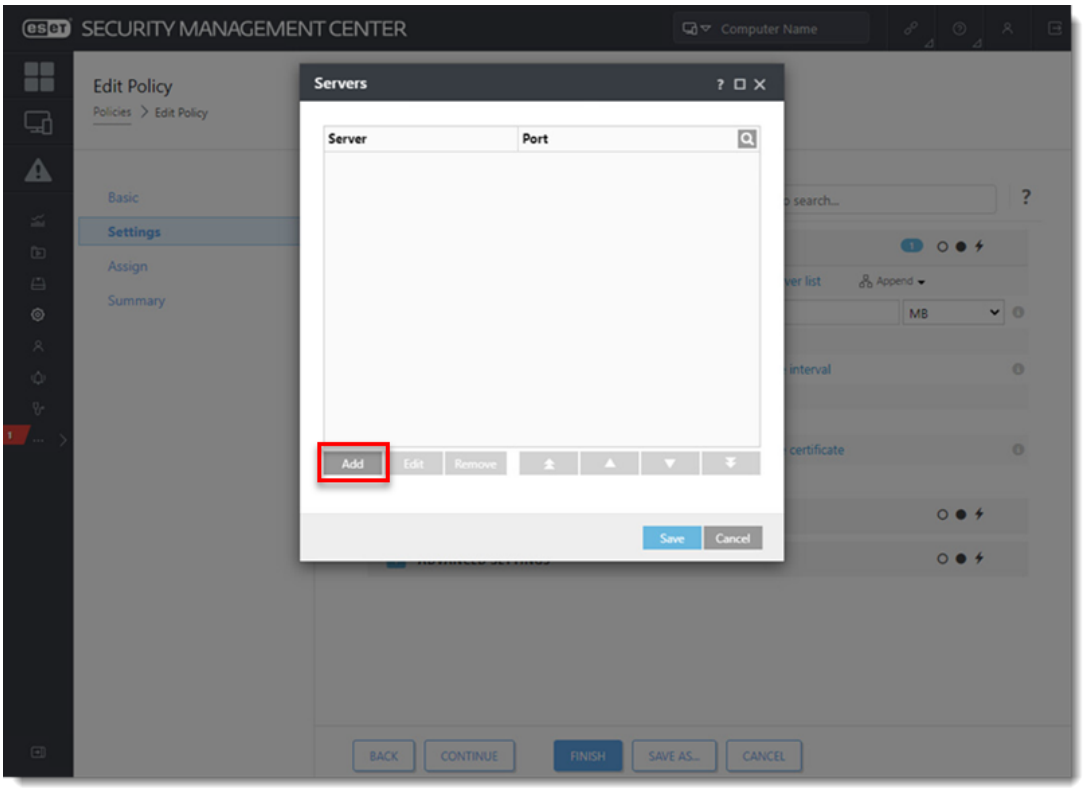

Figure 3-4

1. In theHostfield, type the applicable address (the address must match what the agent uses in the configuration) of your ESMC Server and clickOK.

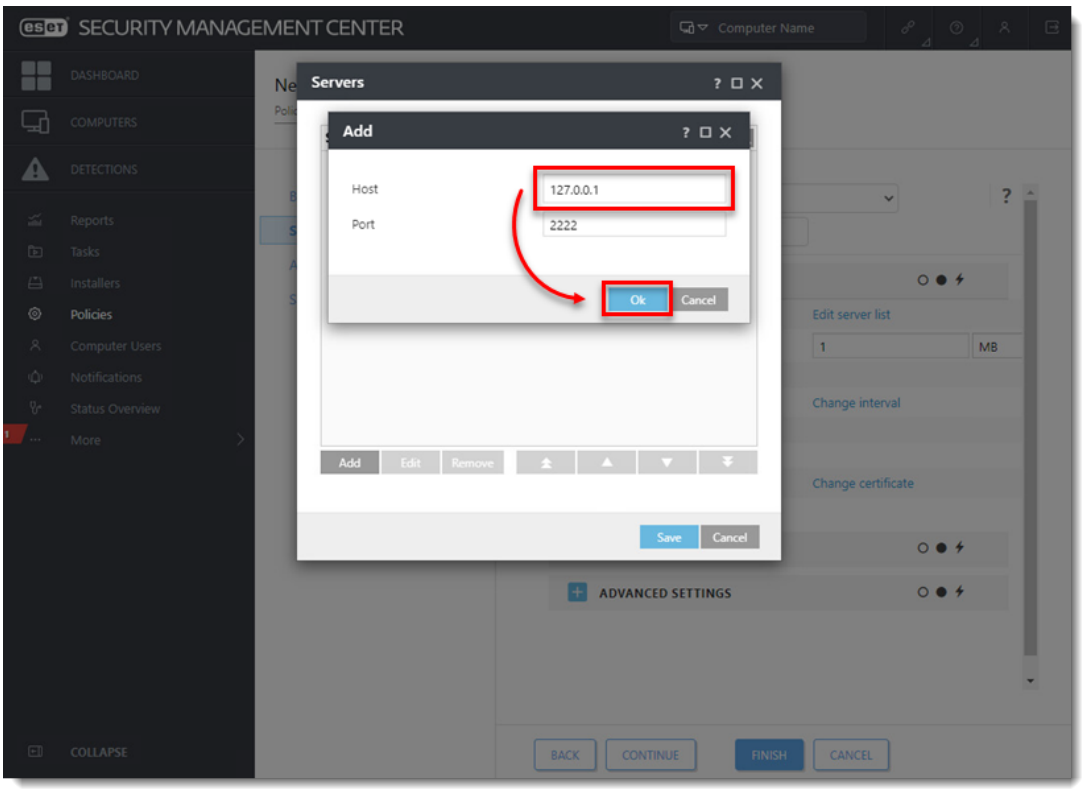

Figure 3-5

1. ClickSave.

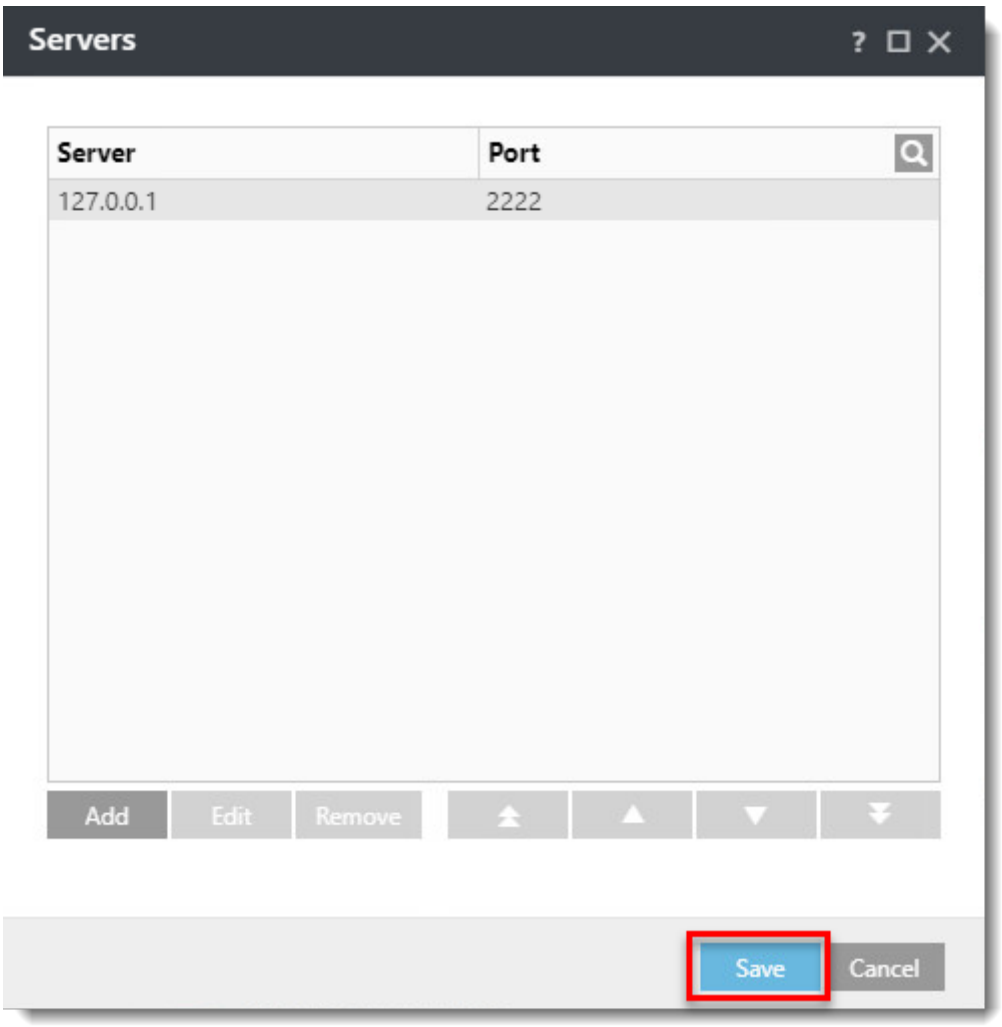

Figure 3-6

1. In thePolicy settingsdrop-down menu, select Append.

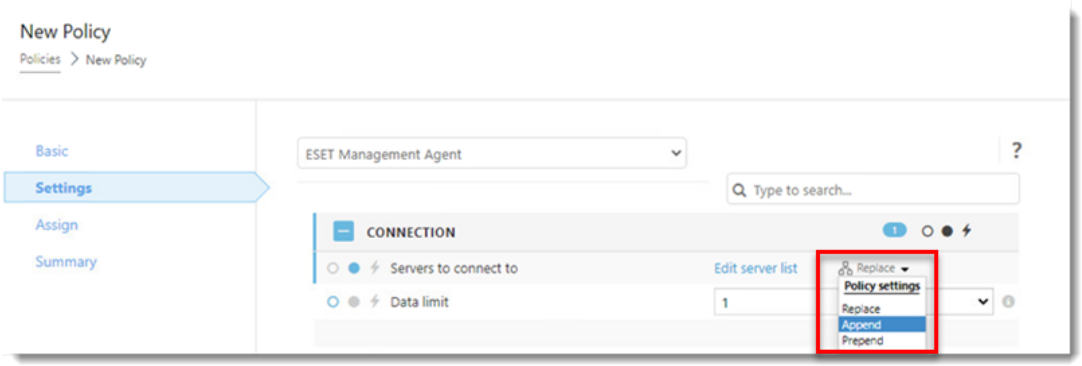

Figure 3-7

1. ClickAdvanced Settings. In the HTTP Proxysection, selectDifferent Proxy Per Service from theProxy Configurationdrop-down menu.

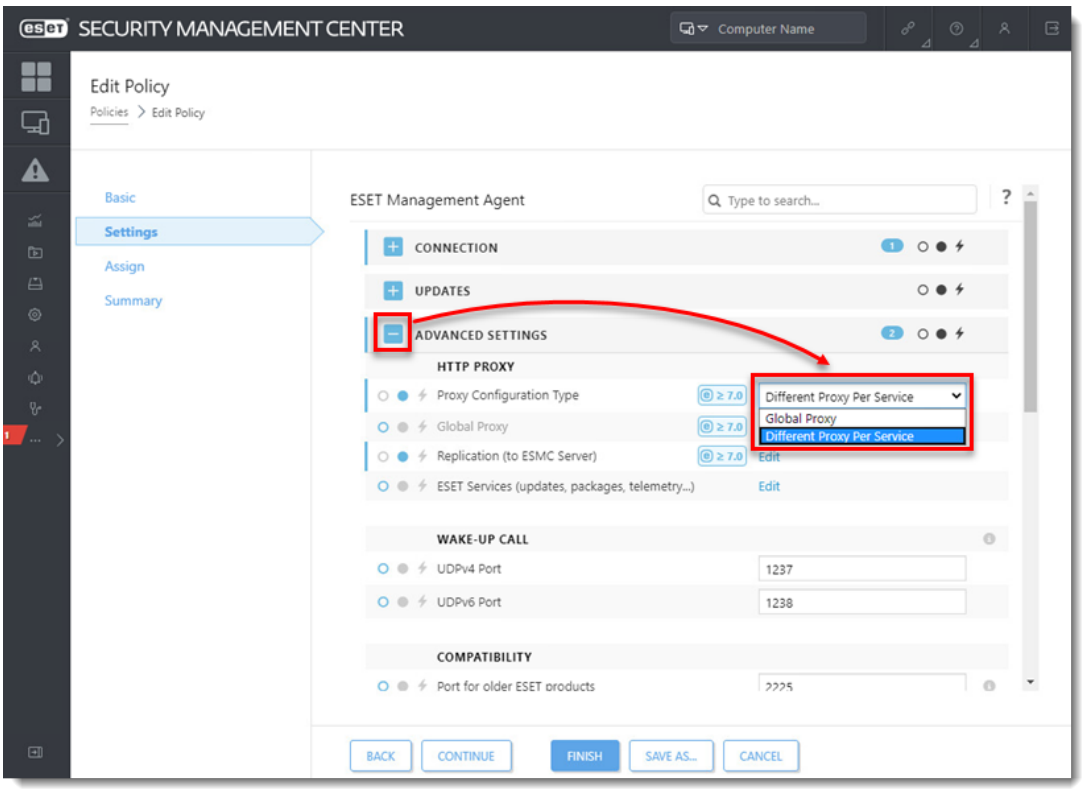

Figure 3-8

1. Next toReplication (to ESMC Server), clickEdit.

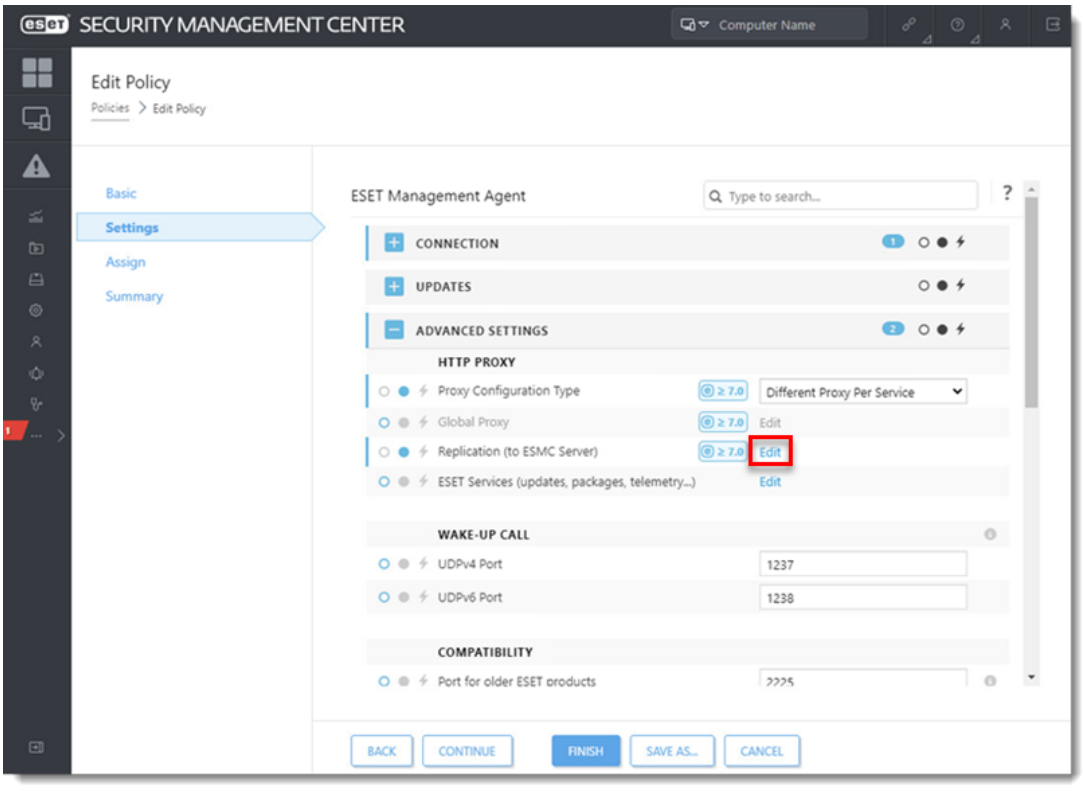

Figure 3-9

1. Enable theUse proxy server.In the Host field, type the IP address of the proxy machine. In thePortfield, leave the default value (3128), and clickSave.

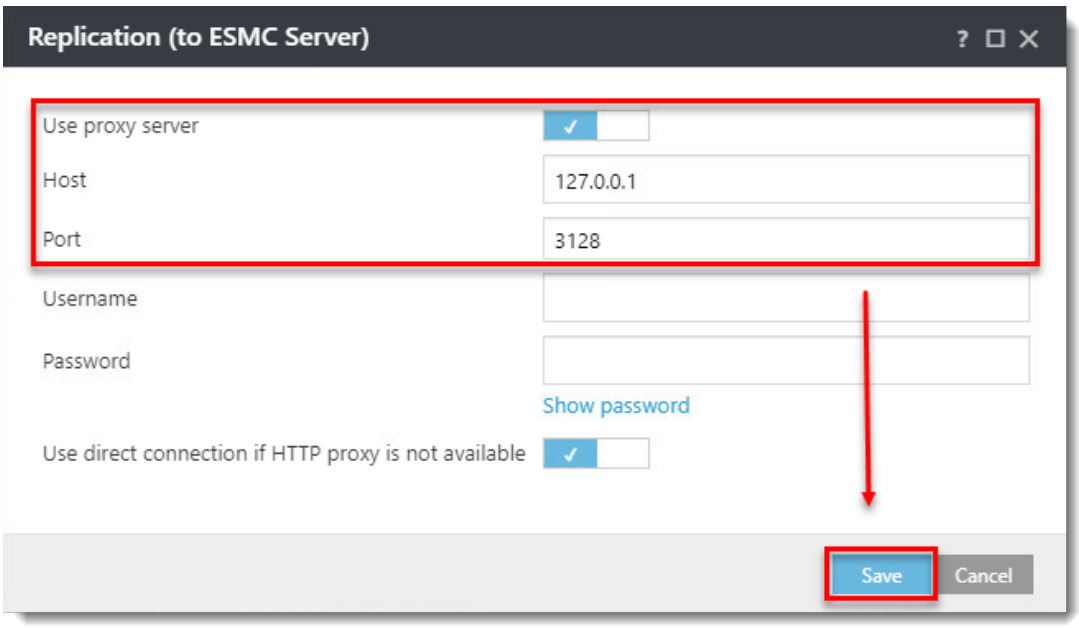

Figure 3-10

1. ClickFinish 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 ESMC Server after the upgrade. Such an agent must be fixed manually by running a repair installation and using the correct ESMC Server address. If the HTTP Proxy setting is not applied in the policy, the agent is able to connect the ESMC Server.

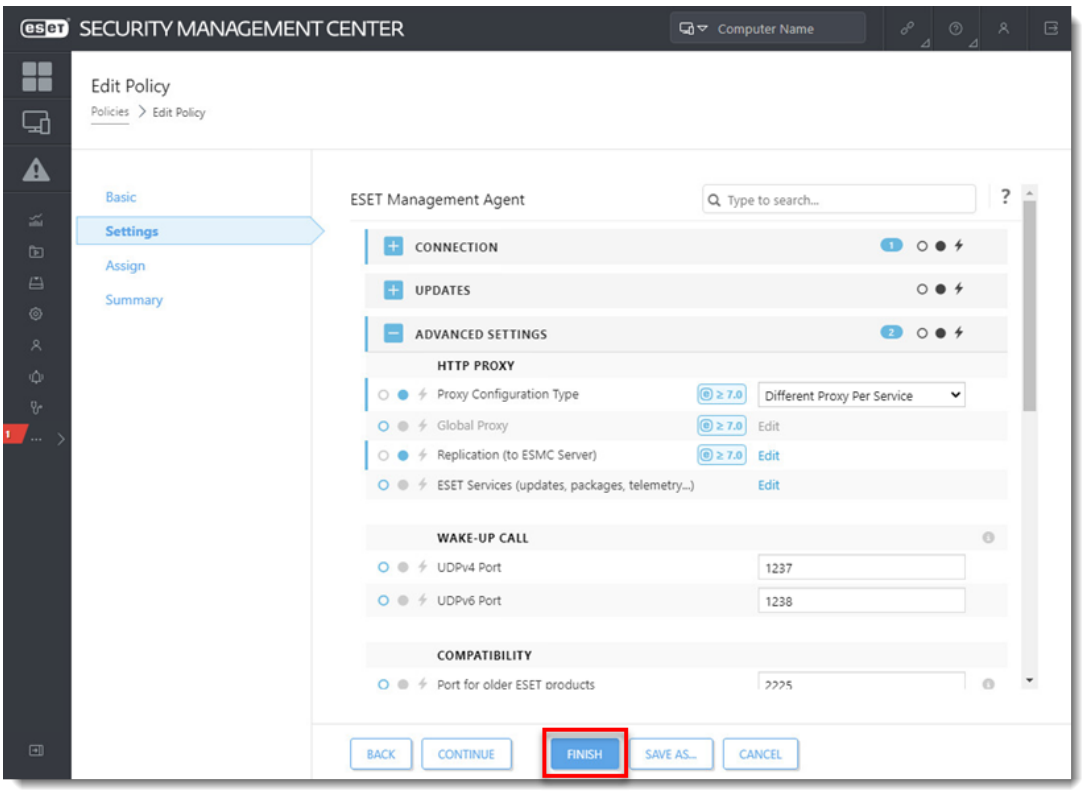

Figure 3-11

1. Choose one computer that is connected via ERA Proxy andassign the new policy to that test client.
2. After a few minutes, verify the computer is still connecting to the ESMC Server.

IV. Upgrade ERA Agents on client computers

1. Run aSecurity management Center Components Upgrade Task.
2. Verify the client is connected to the ESMC 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.

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

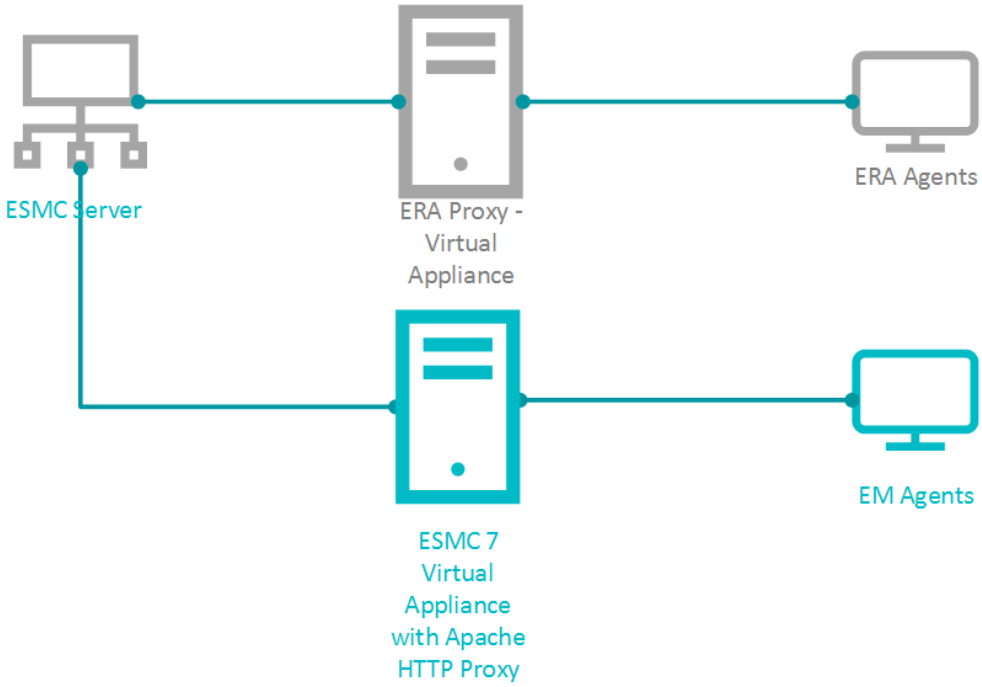

Figure 4-1

1. After the policy is applied, verify all clients are connecting to the ESMC Server.
2. Run aSecurity management Center Components Upgrade Task.
3. If all clients are connecting to the ESMC Server after the upgrade is finished, proceed to section V below.

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

1. Open the ESET Security Management Web Console(ESMC Web Console) in your web browser and log in.
2. Click Policies, select the applicable policy and clickEdit.

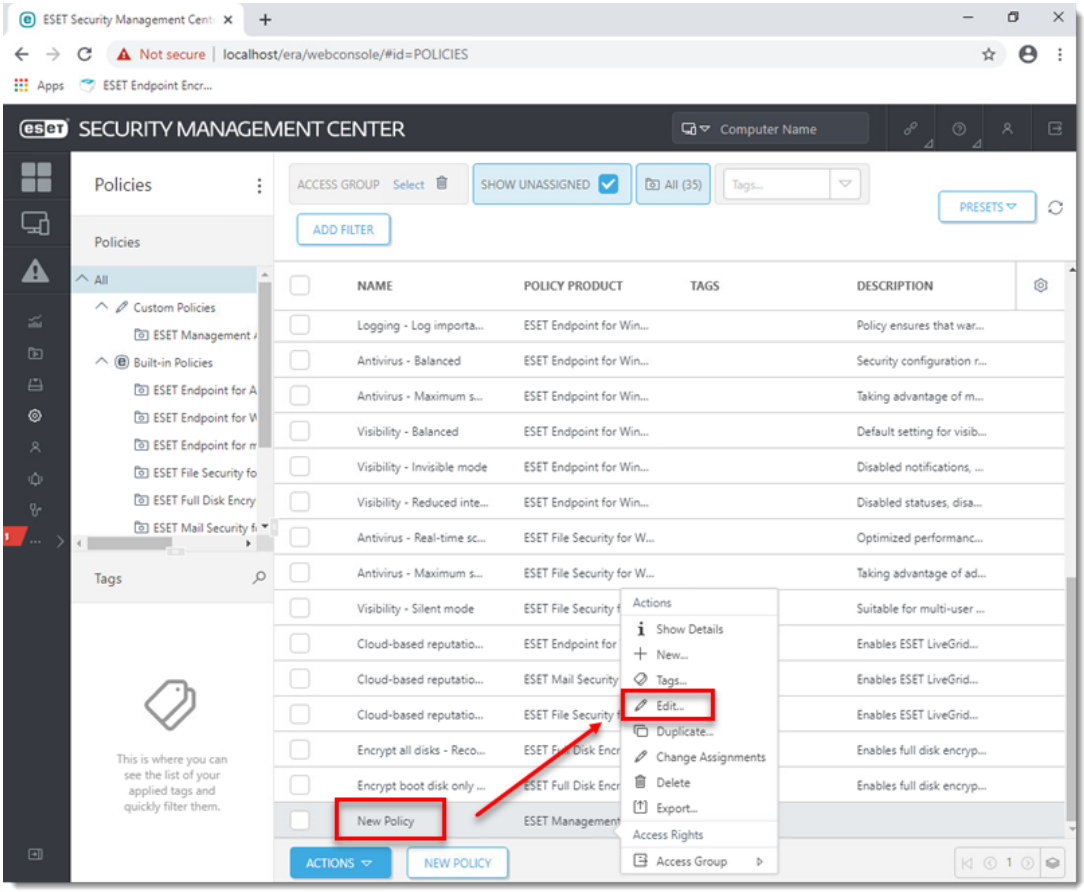

Figure 5-1

1. ClickSettings.
2. In thePolicy settingsdrop-down menu, selectReplace.
3. ClickFinishto save and apply the policy.

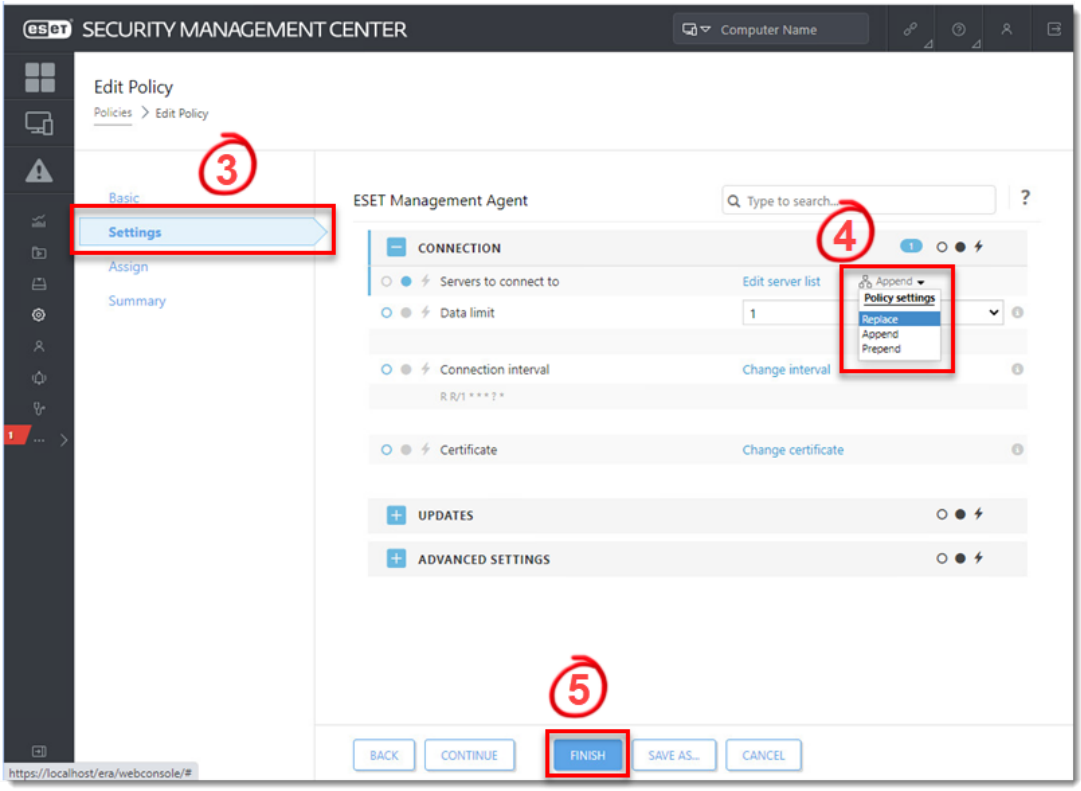

Figure 5-2

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

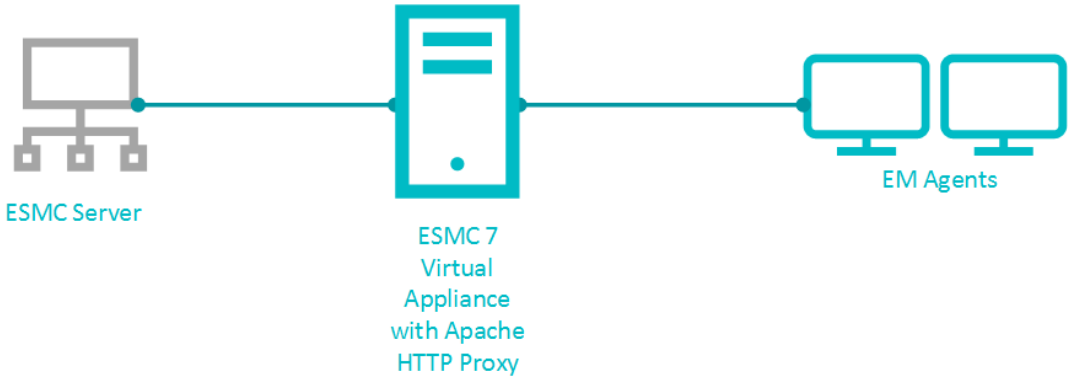

Figure 5-3