ESET SHARED LOCAL CACHE

User Guide

Linux distribution: CentOS 6.x 64-bit

Click here to download the most recent version of this document

ENJOY SAFER TECHNOLOGY™

ESET SHARED LOCAL CACHE

Worldwide Customer Support: www.eset.com/support

REV. 3/13/2017

Contents

1. Introduction

In virtualized environments, multiple computers on a network often use the same base image. Such an arrangement results in a large number of identical files stored on different virtual machines. The ESET Shared Local Cache boosts performance in virtualized environments by eliminating the need to scan duplicate files. Each file is scanned once and stored in the share cache.

ESET Shared Local Cache (ESLC) records files declared clean by the Anti-virus scanner (represented by ESET Endpoint Security, ESET Endpoint Antivirus or ESET File Security). Once recorded, this information is available for all clients in the virtual environment, and is processed when these clients perform a new scan. Unaltered files that are marked as clean in the cache will not be scanned by other clients.

NOTE
Cache entries are written to RAM only. When a newer version of the virus signature database is present on the machine, cache entries are rewritten automatically.

2. System requirements

Supported Linux distributions:

- CentOS 6.x, 7.x 64-bit
- Red Hat Enterprise Linux 6.x, 7.x

ESET Shared Local Cache is also available as an OVA file appliance, which is intended for use with VMware solutions but is also compatible with most hypervisors (such as VMware, Microsoft Hyper-V, etc.).

3. Overall principles and benefits

ESET endpoint solutions on virtual client computers combat malware with the same set of tools used in physical environments. The ESET Shared Local Cache takes advantage of the fact that virtual machines often share the same base image, which results in over 80% duplication of files stored on these machines.

The ESET Shared Local Cache component is compatible with desktop and server products for Windows and Mac, and delivers a significant reduction in resources used during scanning.

4. Installation

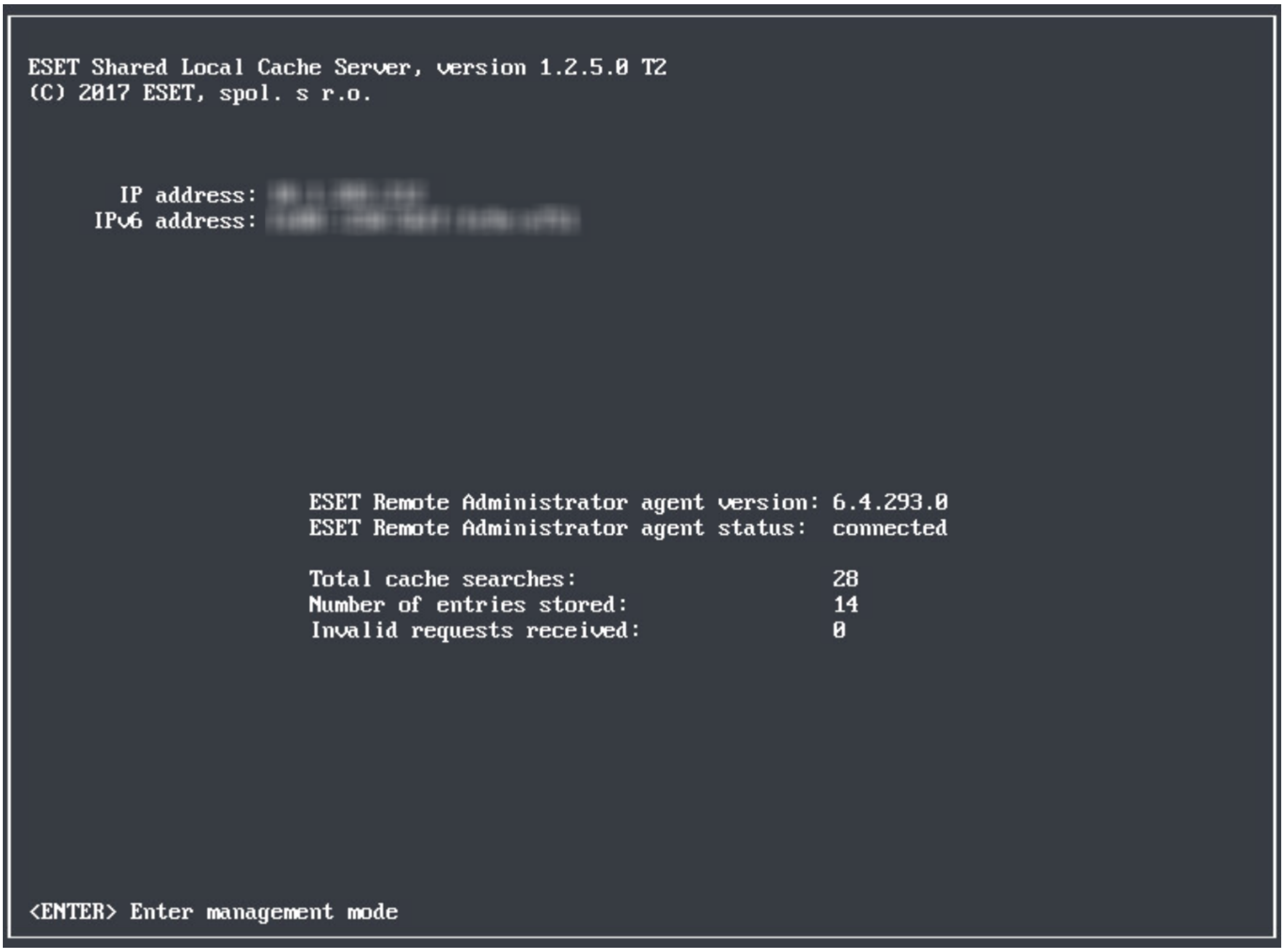
To install ESET Shared Local Cache on a 64-bit linux distribution, load the image file to the virtual machine where you want to install it (using SCP, WinSCP or Wget, depending on where the package is stored) and follow the steps below:

> **IMPORTANT**
> We recommend installing the ESET Shared Local Cache on CentOS 6.7 64-bit.

> **NOTE**
> Before installation, make sure that all dependencies (for example, *libc.so.6*) including i686 dependencies are installed. Install them by entering the command: *yum install ed make glibc.i686 openssl.i686 libgcc.i686 libstdc++.i686*

1. Change permissions to run the installation package with the following command:
   - *chmod +x eslc_appliance.x86_64.rpm.bin*
2. Run the installation package by entering the following command:
   - *rpm -i eslc_appliance.x86_64.rpm*
3. Add an exception to your system firewall to allow inbound UDP traffic to the cache (the default port is 3537), using the iptables command:
   - *iptables -I INPUT -p udp --dport 3537 -j ACCEPT*
4. Start the main service by entering the following command:
   - */etc/init.d/eslc start*

To view the status of ESET Shared Local Cache, or change settings using system console, enter the following command */opt/eset/eslc/sbin/eslc_syscon*.



```
ESET Shared Local Cache Server, version 1.2.5.0 T2
(C) 2017 ESET, spol. s r.o.


       IP address: [redacted]
     IPv6 address: [redacted]









                       ESET Remote Administrator agent version: 6.4.293.0
                       ESET Remote Administrator agent status:  connected

                       Total cache searches:                    28
                       Number of entries stored:                14
                       Invalid requests received:               0







<ENTER> Enter management mode
```

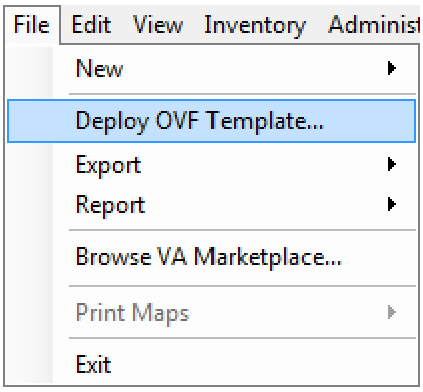
5. ESLC Appliance deployment process

5.1 VMware

The appliance is formatted as a VMware compatible image intended primarily for use in local networks with a dedicated Shared Local Cache server. The OVA file contains a functional operating system, and is ready to use as soon as it is deployed. You can deploy the OVA file using vSphere Client.

Deployment procedure:

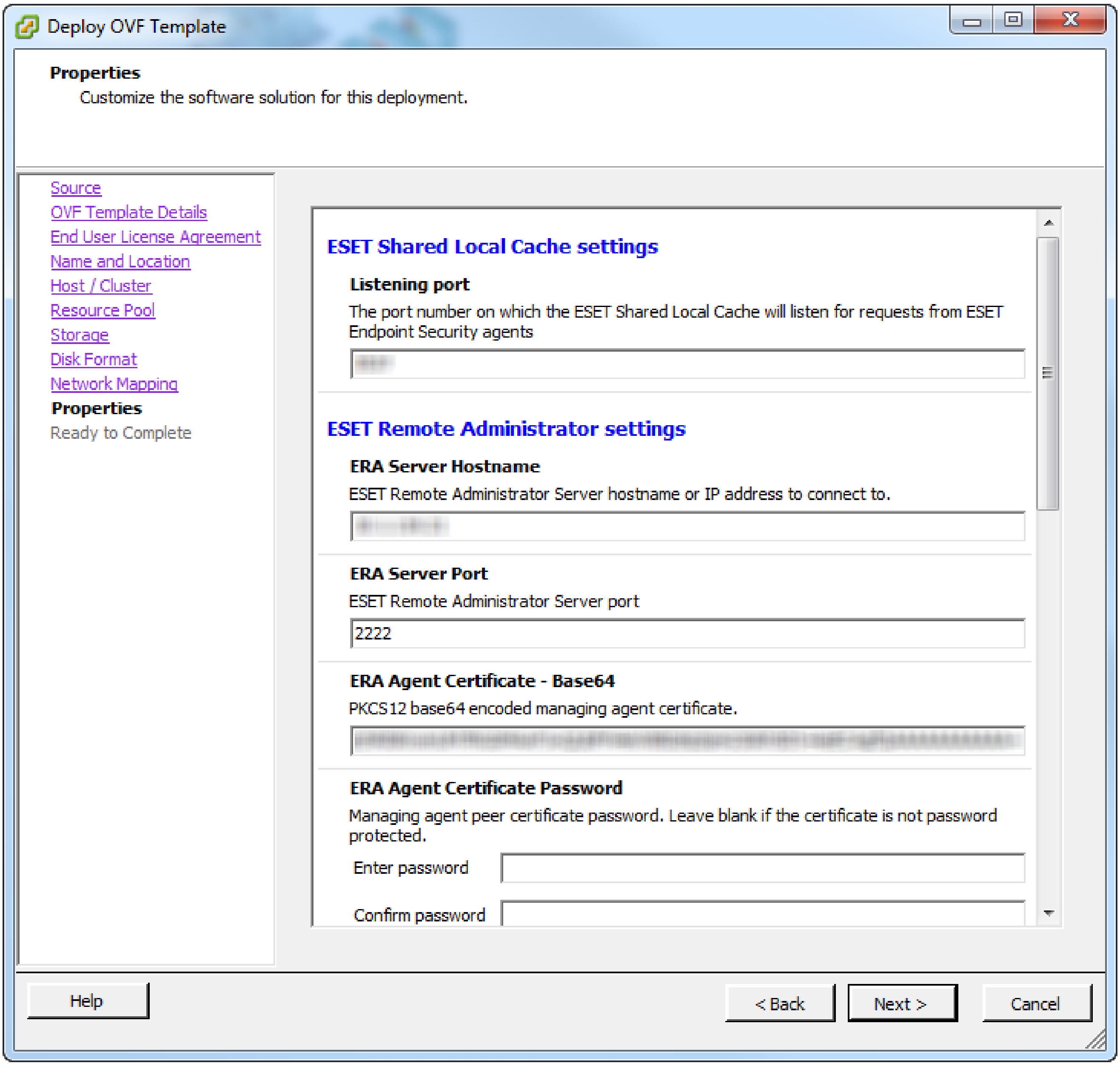
1. Log into vSphere Client, click **File** in the top menu bar and select **Deploy OVF Template**.



2. Click **Browse** and navigate to the image stored on your computer (local hard drive, network share...) or enter a URL where the image is located.
3. Click **Next** to verify that you have selected the correct image to use.
4. Read and accept the end user license agreement.
5. Follow the instructions on screen to complete installation and specify the following information about your virtual appliance:

   - **Name and Location** – Specify a name for the deployed template and location where virtual machine files are stored.
   - **Host / Cluster** – Select the host or cluster on which you want to run the template.
   - **Resource Pool** – Select the resource pool within which you want to deploy the template.
   - **Storage** – Select a location to store virtual machine files.
   - **Disk Format** – Select the format that virtual disks will use.
   - **Network Mapping** – Select the network for the virtual machine to use. Ensure that you select the virtual machine network associated with the IP pool you created.

6. If you plan to manage ESET Shared Local Cache using ESET Remote Administrator, specify all required values on the **Properties** window. Failure to enter these values can keep your virtual machine from starting or deny it the necessary certificates for communication with ESET Remote Administrator.



Properties

Customize the software solution for this deployment.

ESET Shared Local Cache settings

Listening port

The port number on which the ESET Shared Local Cache will listen for requests from ESET Endpoint Security agents

ESET Remote Administrator settings

ERA Server Hostname

ESET Remote Administrator Server hostname or IP address to connect to.

ERA Server Port

ESET Remote Administrator Server port

2222

ERA Agent Certificate - Base64

PKCS12 base64 encoded managing agent certificate.

ERA Agent Certificate Password

Managing agent peer certificate password. Leave blank if the certificate is not password protected.

Enter password

Confirm password

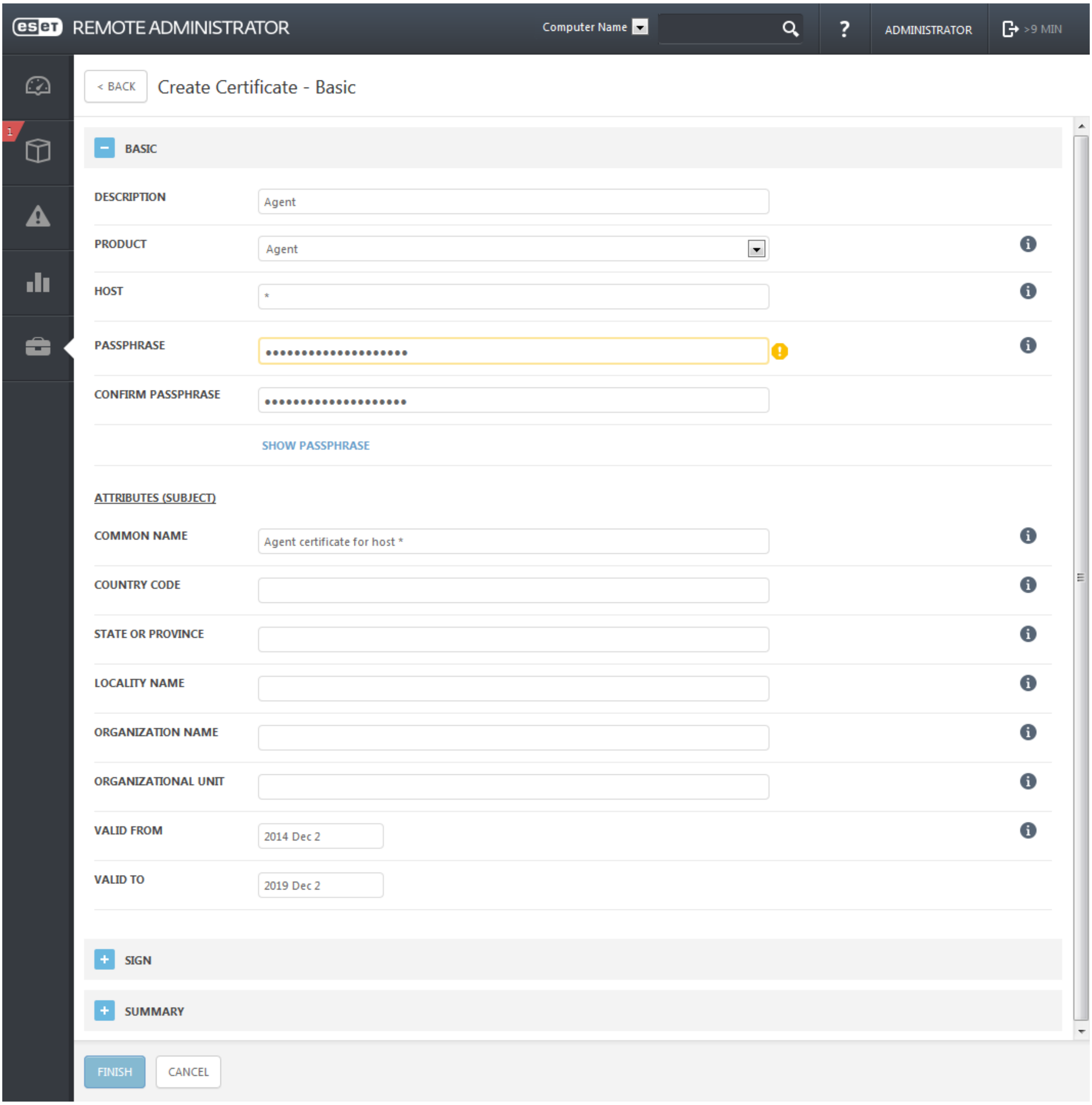
7. If you do not already have a certificate authority and agent/server certificate, you will need to create them in ERA Web Console:

To create a **certificate authority**, follow the steps below in ERA Web Console:

a) Navigate to **Admin** > **Certificates** > **Certificate Authorities** and click **New**.
b) Complete the required fields, add whatever optional information you want to and then click **Save**.

To create an **agent/server certificate** follow the steps below in ERA Web Console:

a) Navigate to **Admin** > **Certificates** > **Peer Certificates** and click **New** at the bottom of the window to add a new certificate.
b) Complete all mandatory fields, add any optional information that you want to and then click **Finish**.
c) Select your Agent certificate and select **Export as Base64** from the **Action** drop-down menu. You will be prompted to save the text file.
d) To enter this certificate into the respective field, open the file, copy all text and paste the text into the appropriate field. Repeat these steps when exporting and entering the Server certificate.



Create Certificate - Basic

BASIC

DESCRIPTION	Agent
PRODUCT	Agent
HOST	*
PASSPHRASE	••••••••••••••••••••
CONFIRM PASSPHRASE	••••••••••••••••••••

SHOW PASSPHRASE

ATTRIBUTES (SUBJECT)

COMMON NAME	Agent certificate for host *
COUNTRY CODE	
STATE OR PROVINCE	
LOCALITY NAME	
ORGANIZATION NAME	
ORGANIZATIONAL UNIT	
VALID FROM	2014 Dec 2
VALID TO	2019 Dec 2

SIGN

SUMMARY

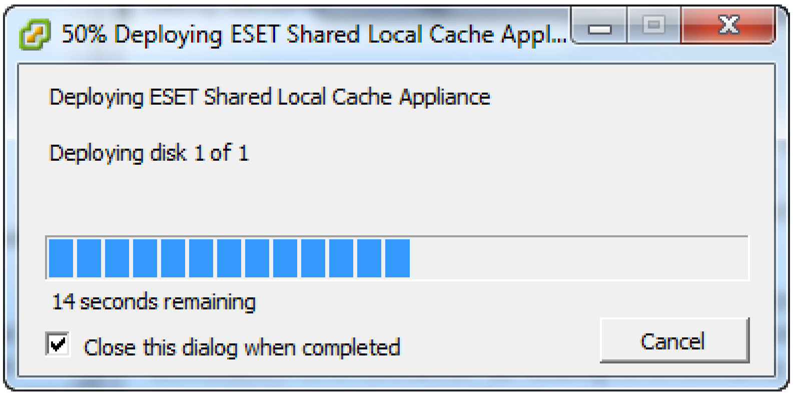
FINISH CANCEL

8. Repeat these steps to create a new Server certificate.

NOTE
For more details on creating Agent/Server certificates and certificate authority, navigate to the **Peer Certificates** and **Certificate Authorities** sections of ESET Remote Administrator User Guide.

9. Review the deployment summary and confirm by clicking **Finish** (the **Power on after deployment** check box is optional).

10. The deployment process will automatically create a virtual machine with the settings you specified. This process can take several minutes depending on network performance.



50% Deploying ESET Shared Local Cache Appl...

Deploying ESET Shared Local Cache Appliance

Deploying disk 1 of 1

14 seconds remaining

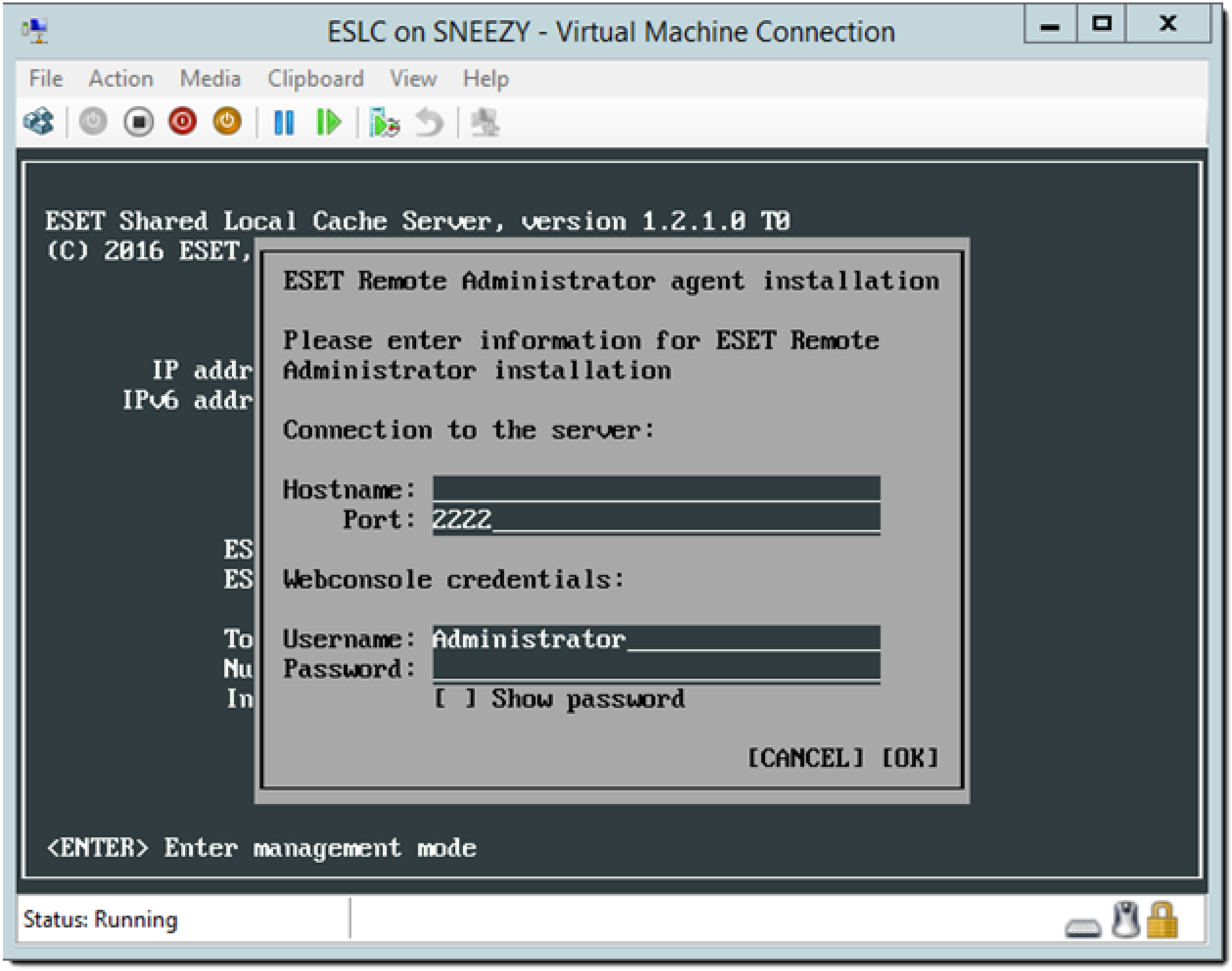
☑ Close this dialog when completed

5.2 Microsoft Hyper-V

Deploying ESLC virtual appliance in Microsoft Hyper-V

1. Download the file from ESET.com.
2. Launch the Hyper-V manager and connect to the appropriate Hyper-V.
3. Create a new virtual machine, with at least 1 CPU and 1 GB of RAM.
   3.1. When you are specifying which generation of Virtual Machine you would like to use, select **Generation 1**.
   3.2. In Configuring Network menu select available network or create a new with help of Virtual Switch Manager.
   3.3. Select a location where the virtual hard drive (ESET_Shared_Local_Cache_Appliance.vhd) is stored.
4. Review the virtual machine details and click **Finish** to complete the virtual machine creation.
5. Once the VM is successfully created, power it on.

6. Enter valid ERA Server Hostname or IP Address and Username and Password for Webconsole. This information you can get from ERA Server Administrator.



ESLC on SNEEZY - Virtual Machine Connection
File Action Media Clipboard View Help

```
ESET Shared Local Cache Server, version 1.2.1.0 T0
(C) 2016 ESET,

      IP addr
    IPv6 addr

           ES
           ES

           To
           Nu
           In

ESET Remote Administrator agent installation

Please enter information for ESET Remote
Administrator installation

Connection to the server:

Hostname:
    Port: 2222

Webconsole credentials:

Username: Administrator
Password:
          [ ] Show password

                         [CANCEL] [OK]

<ENTER> Enter management mode
```

6. Activation

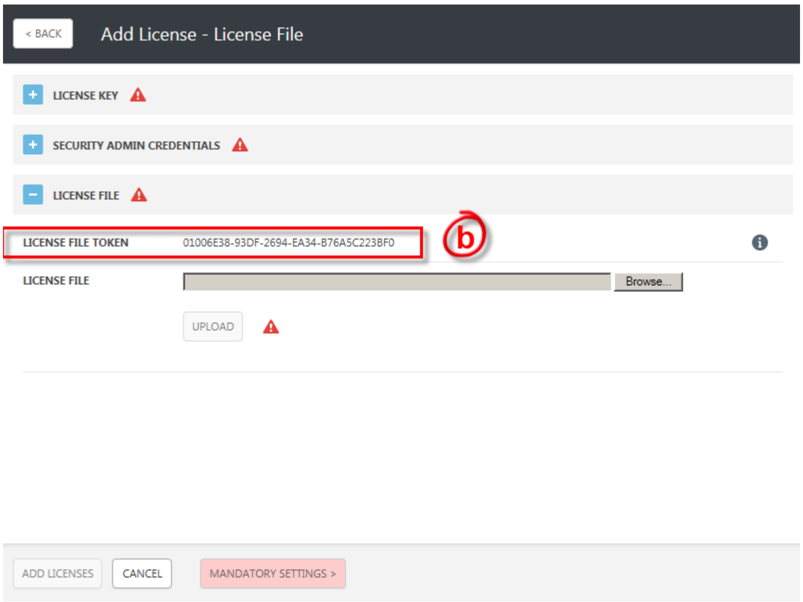
You must activate ESET Shared Local Cache in order to manage it using ESET Remote Administrator. ESET Shared Local Cache requires an offline license file, which must be generated in ESET License Administrator in ELA and transferred to the machine on which ESET Shared Local Cache is installed before you can use it to activate ESET Shared Local Cache. Follow the instructions below to generate a new offline license file and activate ESET Shared Local Cache:

i **NOTE**

You will need your **License File Token** to create the License file in ELA. Follow the steps below to find your License File Token:

a. Open ESET Remote Administrator Web Console (ERA Web Console), log in, and navigate to **Admin** > **License Management.**

b. Click **Add Licenses** and expand **License File**. Your **License File Token** will be displayed, make note of it for use later.



Add License - License File

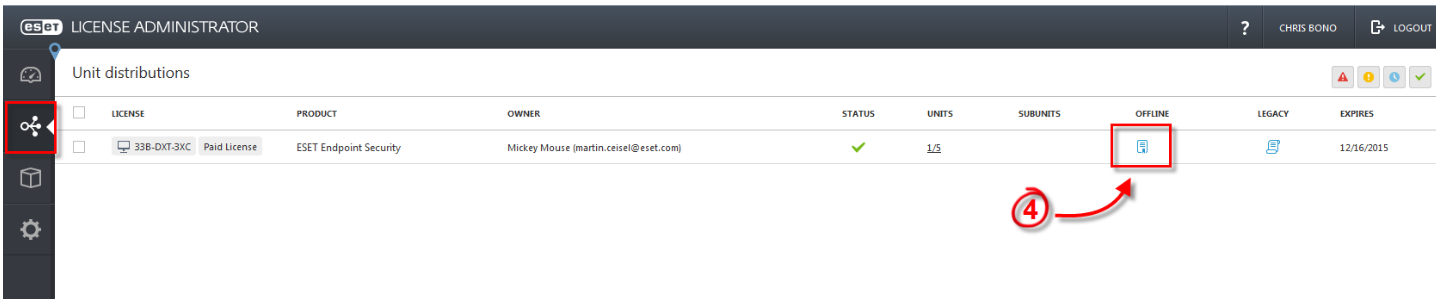
LICENSE FILE TOKEN 01006E38-93DF-2694-EA34-B76A5C223BF0

1. In your web browser, open ESET License Administrator (ELA). You will need to register for an account if you do not already have one.

2. Log into ELA and expand **Settings.**

3. Select the check box next to **Offline license files** if it is not already selected and then click **Save Settings.**

4. Expand **Unit distribution**. Locate the **Offline** column for the license you want to use and click the number or icon (if you already have offline licenses in use, a number will be displayed) to open the **Offline License File** dialog.

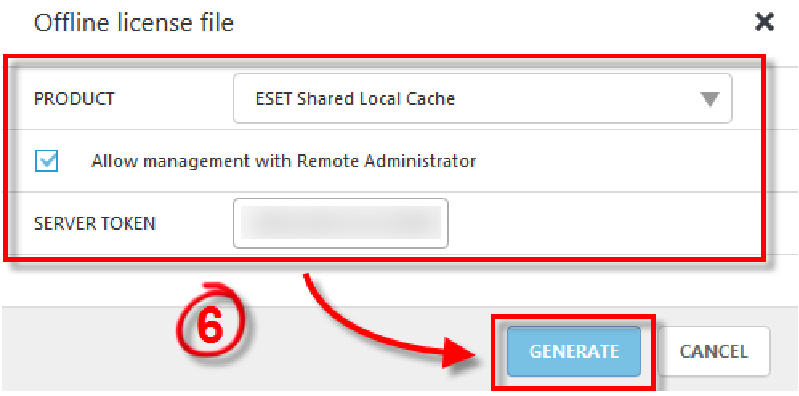


Unit distributions

	LICENSE	PRODUCT	OWNER	STATUS	UNITS	SUBUNITS	OFFLINE	LEGACY	EXPIRES
□	33B-DXT-3XC Paid License	ESET Endpoint Security	Mickey Mouse (martin.ceisel@eset.com)	✓	1/5				12/16/2015

5. Click **Add License File.**

6. Select **ESET Shared Local Cache** from the drop-down menu, select the check box next to **Allow management with Remote Administrator**, type your License File Token into the appropriate field and then click **Generate**. A new license file will be generated.



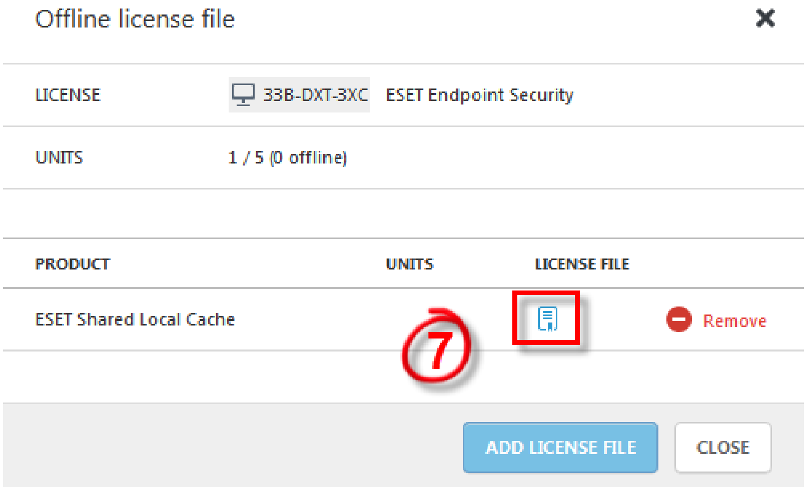
Offline license file

PRODUCT ESET Shared Local Cache

☑ Allow management with Remote Administrator

SERVER TOKEN [redacted]

7. Click the **License File** icon to download the license file that you just created.



Offline license file

LICENSE 33B-DXT-3XC ESET Endpoint Security

UNITS 1 / 5 (0 offline)

PRODUCT	UNITS	LICENSE FILE	
ESET Shared Local Cache			Remove

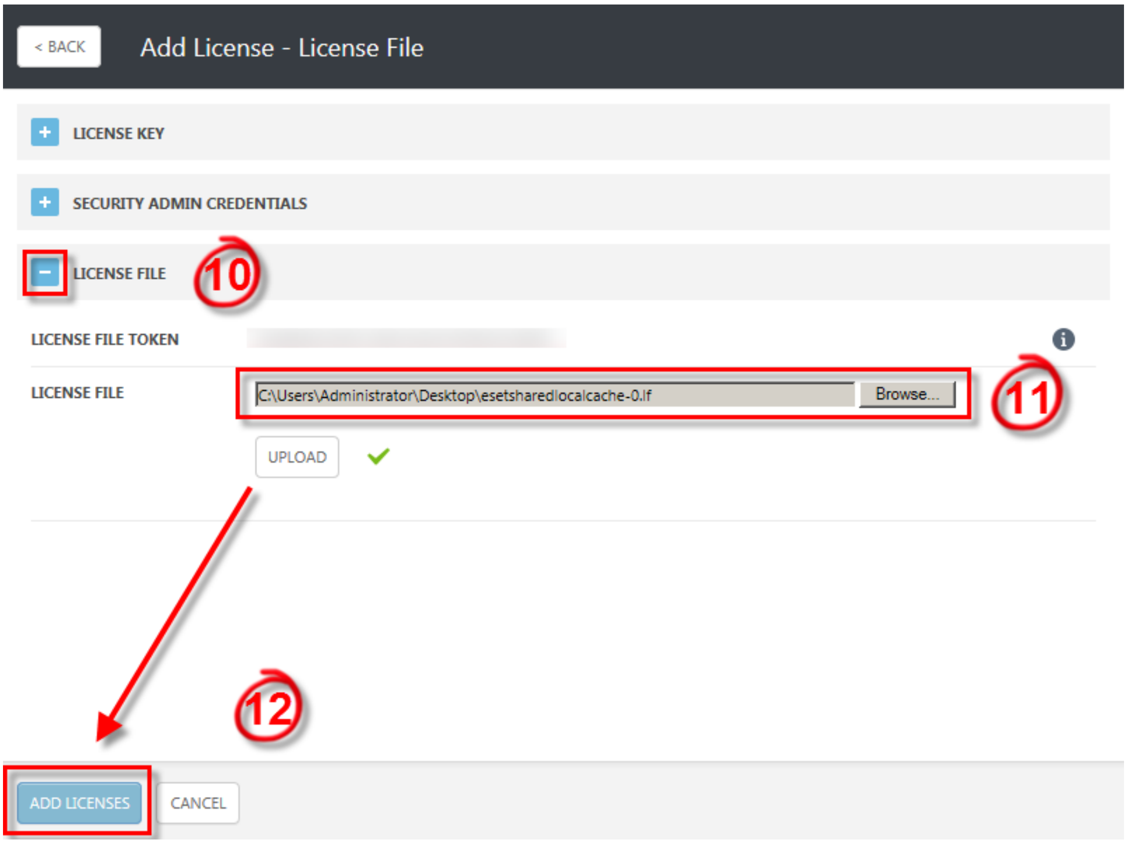
8. Transfer the file to your server where ESET Remote Administrator installed using removable media, email or whatever method you prefer.

9. Open ESET Remote Administrator, log in, and navigate to **Admin** > **License Management**.

10. Click **Add Licenses** and expand **License File.**

11. Click **Browse**, navigate to the License file that you exported in step 7 and click **Open.**

12. Click **Upload** and then click **Add Licenses**. ESET Remote Administrator will add the License file and ESET Shared Local Cache will now be activated.



< BACK

Add License - License File

LICENSE FILE TOKEN

LICENSE FILE C:\Users\Administrator\Desktop\esetsharedlocalcache-0.lf

NOTE

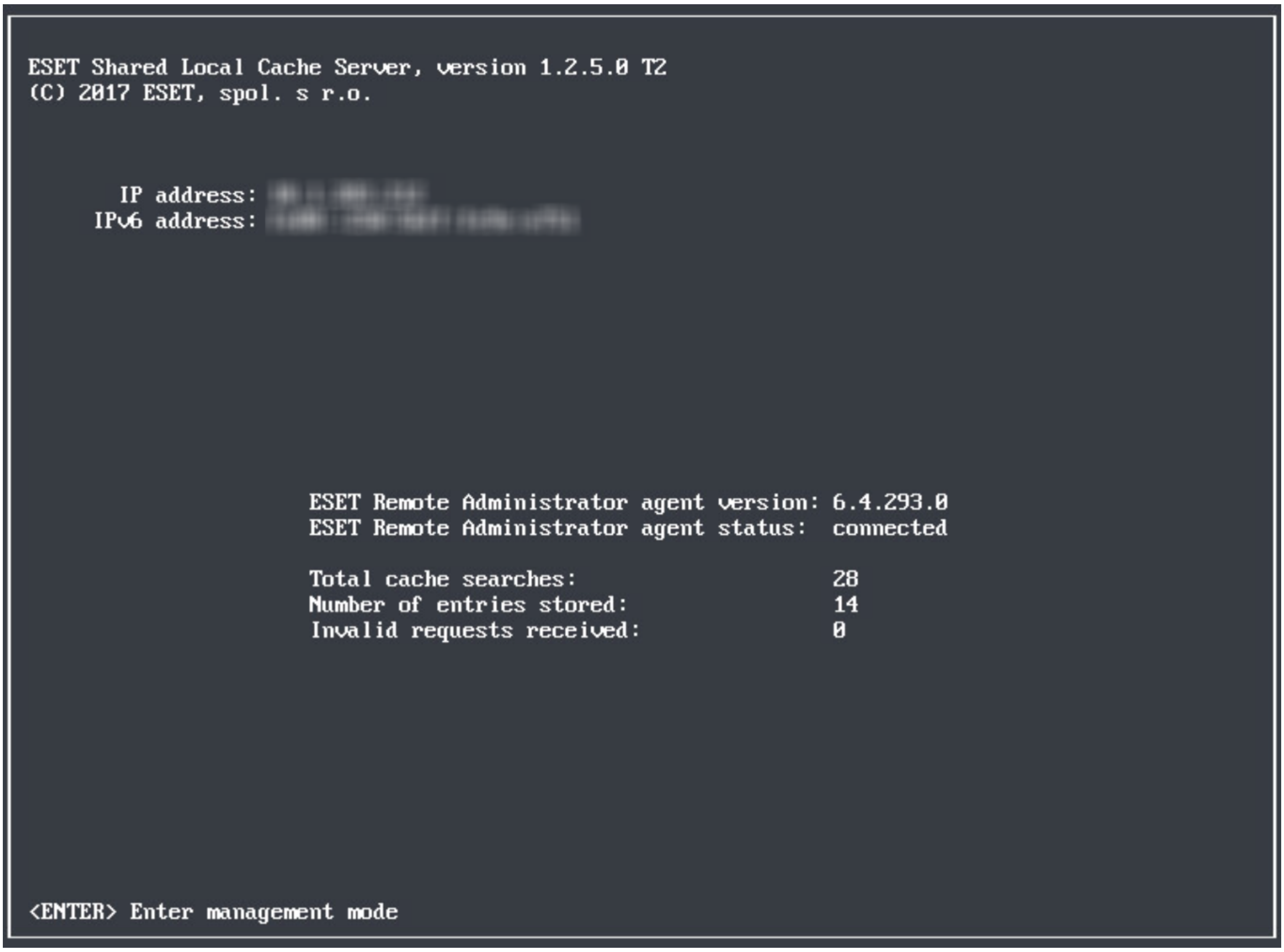
Please allow a short delay until the activation task reaches your server with ESET Shared Local Cache installed.

7. Configuration of the appliance

ESET Shared Local Cache requires the following information for proper configuration:

- IP address or hostname of the ERA server
- Shared cache server listening port (3537 by default)
- Cache password
- Cache size (maximum number of items that can be stored in the cache)

The basic information screen, shown below, gives an overview of your cache usage and allows you to configure settings by pressing **Enter**.

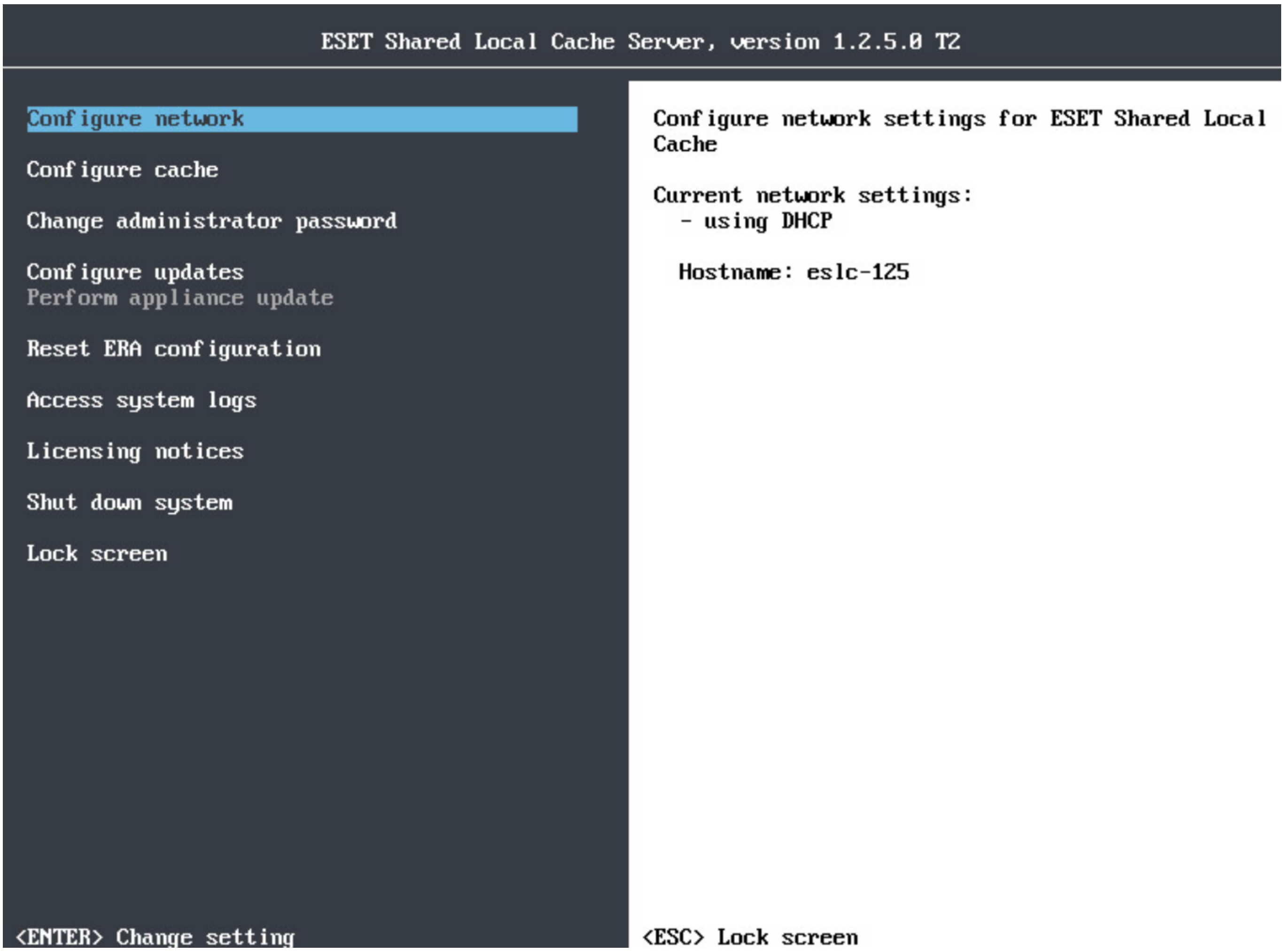


```
ESET Shared Local Cache Server, version 1.2.5.0 T2
(C) 2017 ESET, spol. s r.o.


       IP address: [redacted]
     IPv6 address: [redacted]








                      ESET Remote Administrator agent version: 6.4.293.0
                      ESET Remote Administrator agent status:  connected

                      Total cache searches:                    28
                      Number of entries stored:                14
                      Invalid requests received:               0








<ENTER> Enter management mode
```

The following options can be edited in management mode:

- **Configure network** – network settings for ESET Shared Local Cache such as IP address, mask, gateway and DNS server
- **Set cache size** – configure the maximum number of items stored in ESET Shared Local Cache
- **Set cache password** – required for clients to add items to the cache
- **Set cache listening port** – communication port on which ESET Shared Local Cache will listen for requests
- **Change administrator password** – the system console can be configured so that only administrators can change settings (set an administrator password to use this configuration)
- **Configure updates** – configure updates of ESET Shared Local Cache within the appliance
- **Perform appliance update** – will trigger an update of the appliance when available
- **Reset ERA configuration** – will revert settings to the defaults specified in virtual machine parameters
- **Restart system** – will restart your server
- **Shut down system** – will shut down your system
- **Lock screen** – will lock the console and return to the basic information screen

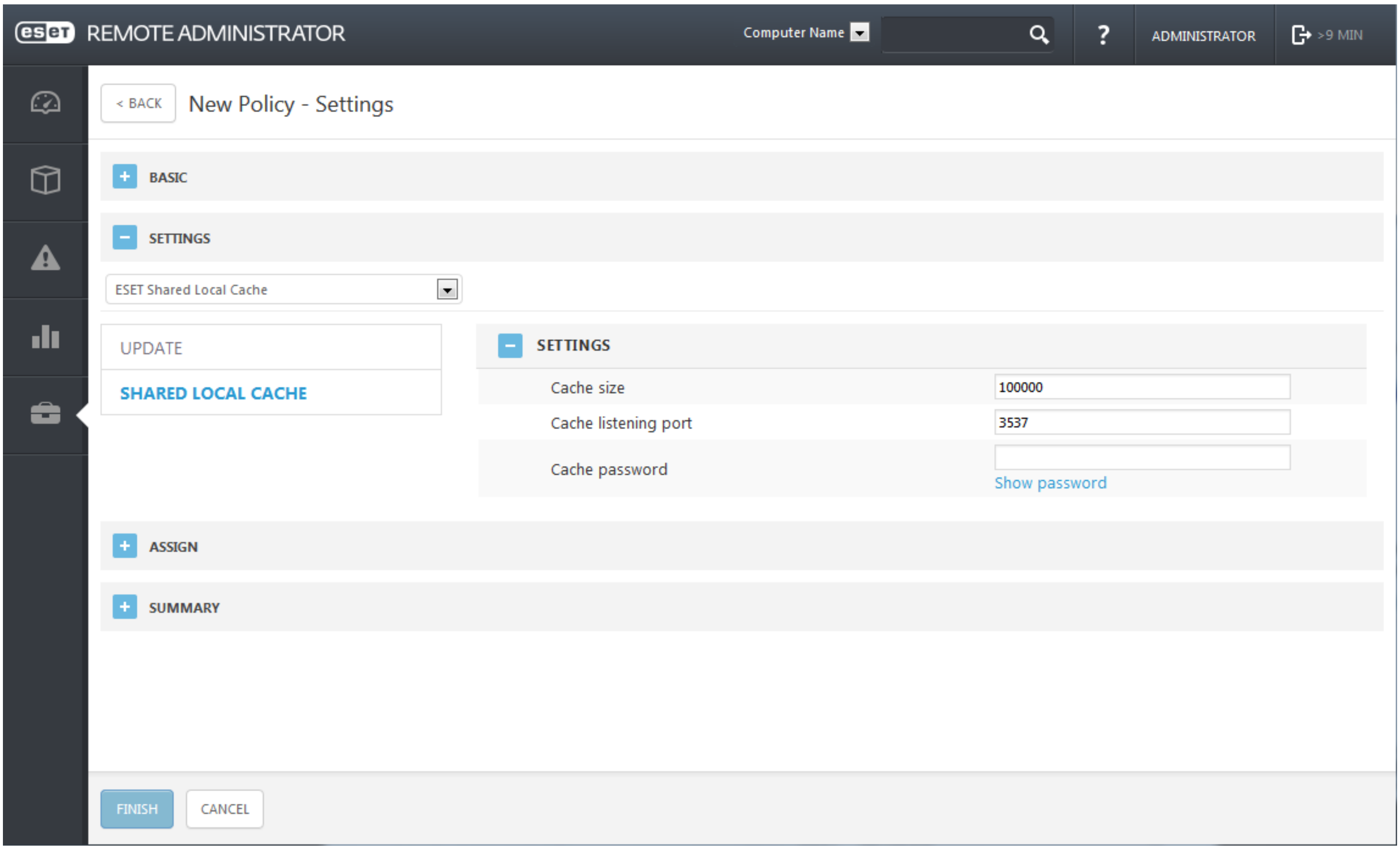
Use the arrow keys to select a setting and press **Enter** to configure it.



```
ESET Shared Local Cache Server, version 1.2.5.0 T2

Configure network                    Configure network settings for ESET Shared Local
                                     Cache
Configure cache
                                     Current network settings:
Change administrator password          - using DHCP

Configure updates                      Hostname: eslc-125
Perform appliance update

Reset ERA configuration

Access system logs

Licensing notices

Shut down system

Lock screen

<ENTER> Change setting               <ESC> Lock screen
```

To create a policy for ESET Shared Local Cache, follow the steps below in ERA Web Console:

1. Navigate to **Admin** > **Policies** and select **New** from the **Policies** drop-down menu.
2. Expand the **Basic** tab and enter a **Name** and **Description** for your new policy.
3. Expand the **Settings** tab, select **ESET Shared Local Cache** from the drop-down menu, click **Shared Local Cache** and set the parameters as shown in the figure below:



Cache size: 100000

Cache listening port: 3537

Cache password:

After a Policy is created, you can assign it to a **Static** or **Dynamic Group**. There are a two ways to assign a policy in the ERA Web Console:

- Under **Admin** > **Policies** select a policy and click **Assign Group(s)**. Select a static or Dynamic Group and click **OK**.
- Click **Admin** > **Groups** > **Group** or click the cogwheel ⚙ icon next to the group name and select **Manage Policies**.

8. Client side configuration

ESET Shared Local Cache supports the following client solutions:

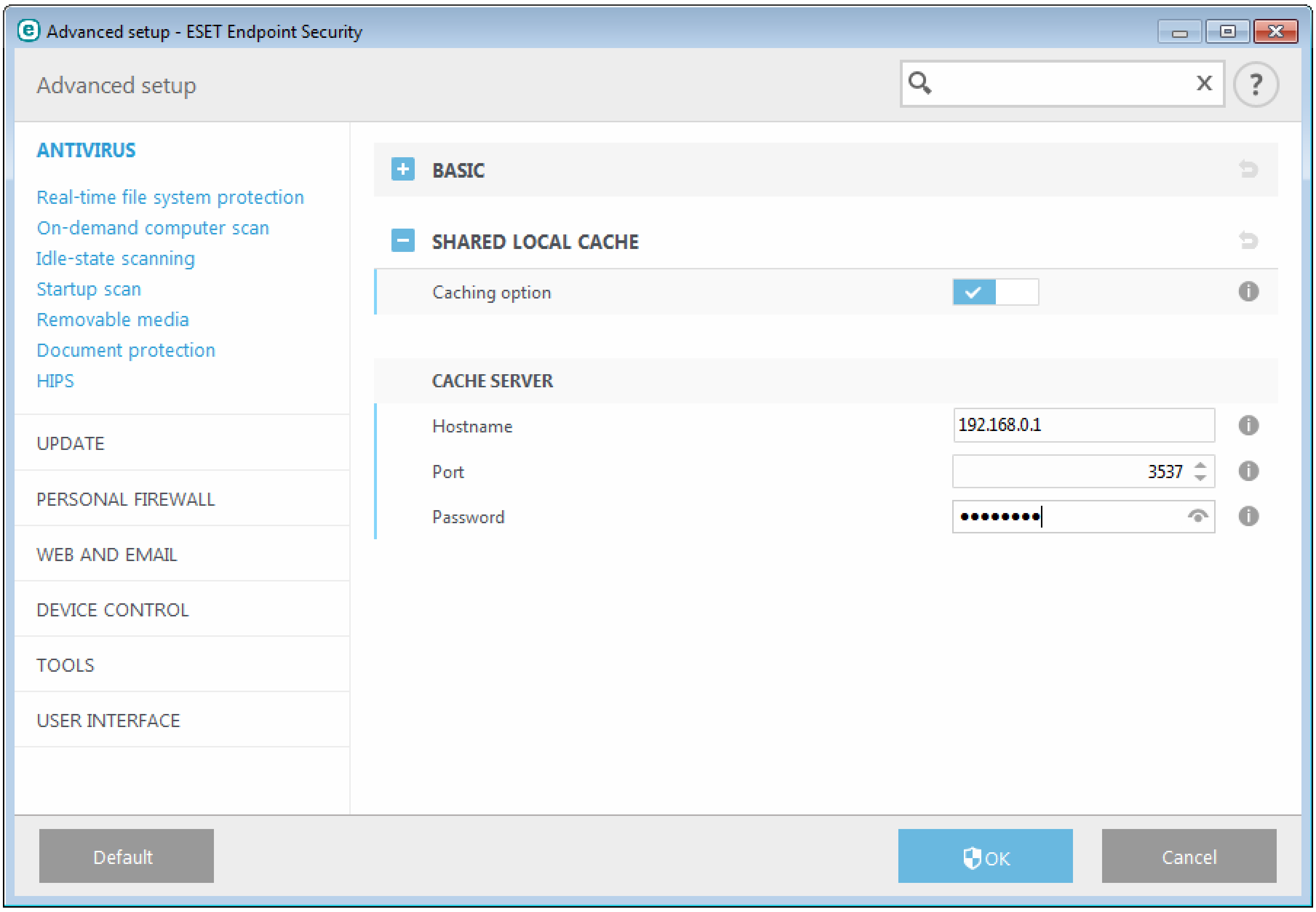
- ESET File Security
- ESET Endpoint Security for Windows and OS X
- ESET Endpoint Antivirus for Windows and OS X

Configuration on ESET Endpoint Security or ESET Endpoint Antivirus for Microsoft Windows

Open the main menu program window, press **F5** to open **Advanced setup**, and navigate to **Antivirus** > **Shared local cache**. Enable **Caching option** to save information about scans of files and folders on your network to the local cache. If you perform a new scan, ESET Endpoint Security or ESET Endpoint Antivirus will search for scanned files in the cache. If files match, they will be excluded from scanning.

The **Cache server** section contains the following options**:**

- **Hostname** – Name or IP address of the computer where the cache is located.
- **Port** – Number of the port used for communication (the same port specified during deployment of ESET Shared Local Cache.
- **Password** – We highly recommend that you specify a password for the Shared Local Cache.



Caching option ✓

Hostname 192.168.0.1

Port 3537

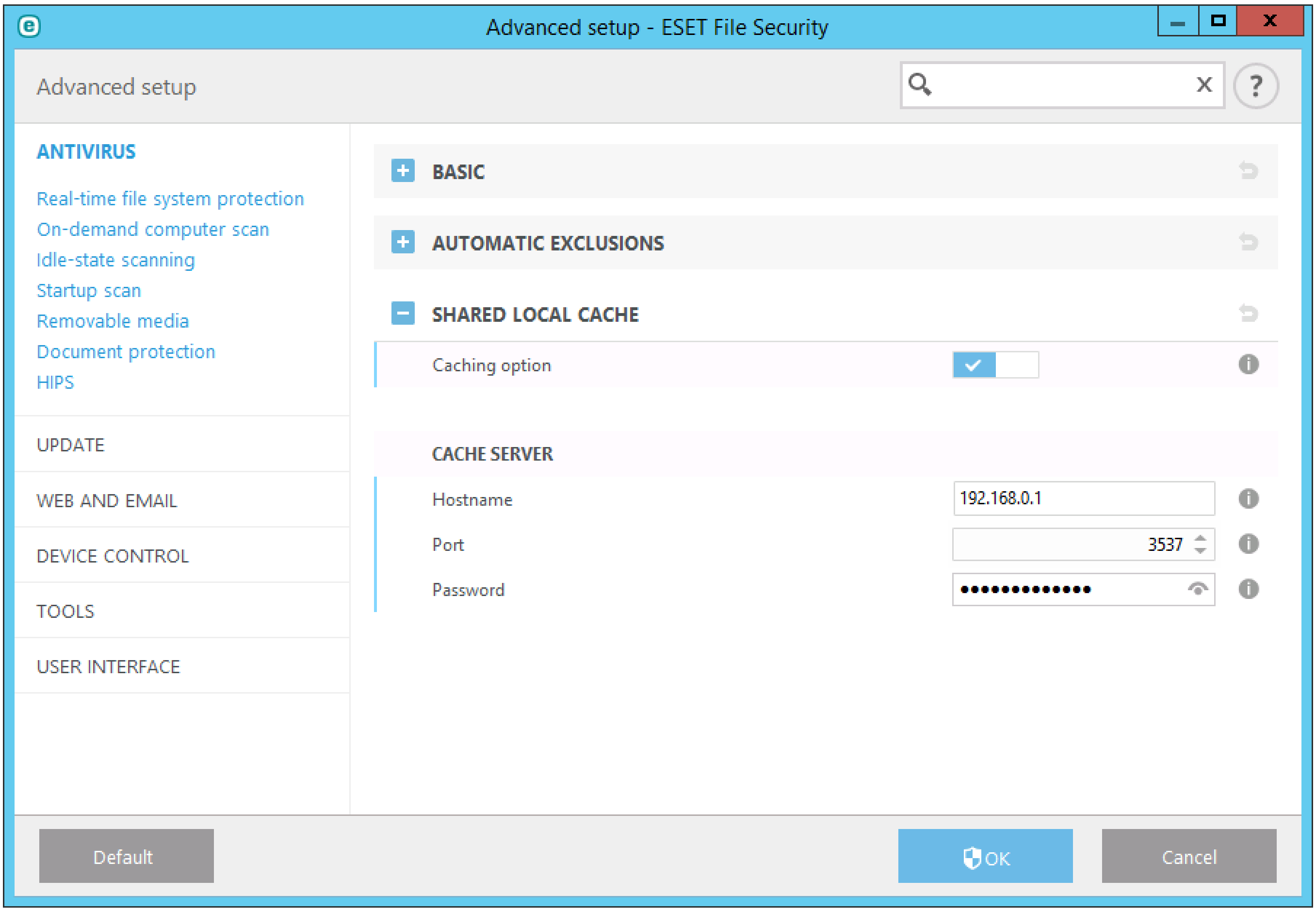
Password ••••••••

Configuration on ESET File Security

Open the main menu program window, press **F5** to open **Advanced setup**, and navigate to the **Antivirus** > **Shared local cache** tab. Enable **Caching option** to save information about scans of files and folders on your network to the local cache. If you perform a new scan, ESET File Security will search for scanned files in the cache. If files match, they will be excluded from scanning.

The **Cache server** section of Advanced setup contains the following options:

- **Hostname** – Name or IP address of the computer where the cache is located.
- **Port** – Number of the port used for communication (the same port specified during deployment of the ESET Shared Local Cache.
- **Password** – We highly recommend that you specify a password for the Shared Local Cache.



Caching option ✓

CACHE SERVER

Hostname 192.168.0.1

Port 3537

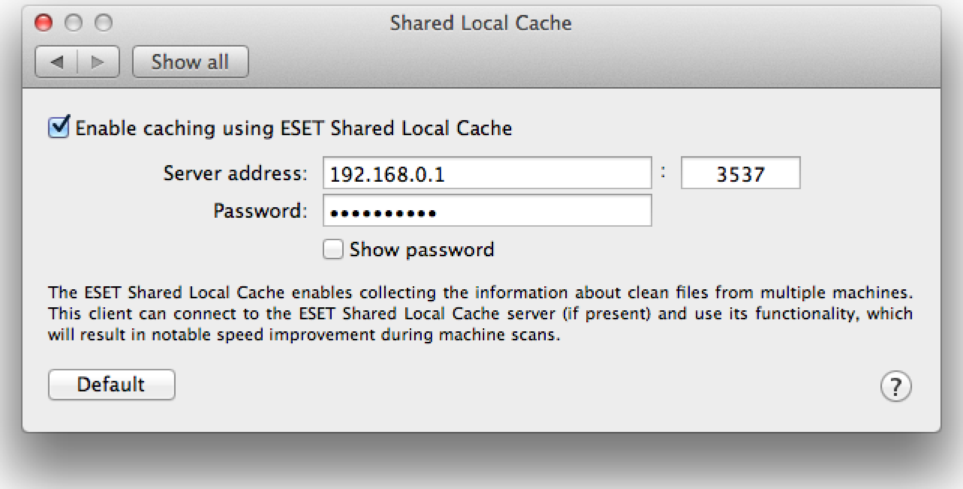
Password ••••••••••••••

Configuration on ESET Endpoint Security or ESET Endpoint Antivirus for OS X

To enable the use of the Shared local cache, click **Setup** > **Enter application preferences** > **Shared local cache** and select the check box next to **Enable caching using ESET Shared Local Cache**.

Shared Local Cache settings contains the following:

- **Server address** – Name or IP address of the computer where the cache is located. Number of the port used for communication (3537 by default).
- **Password** – We highly recommend that you specify a password for the Shared Local Cache.



☑ Enable caching using ESET Shared Local Cache

Server address: 192.168.0.1 : 3537

Password: ••••••••••

□ Show password

The ESET Shared Local Cache enables collecting the information about clean files from multiple machines. This client can connect to the ESET Shared Local Cache server (if present) and use its functionality, which will result in notable speed improvement during machine scans.

9. Updating ESET Shared Local Cache

For optimal functionality, it is important that ESET Shared Local Cache is regularly updated.

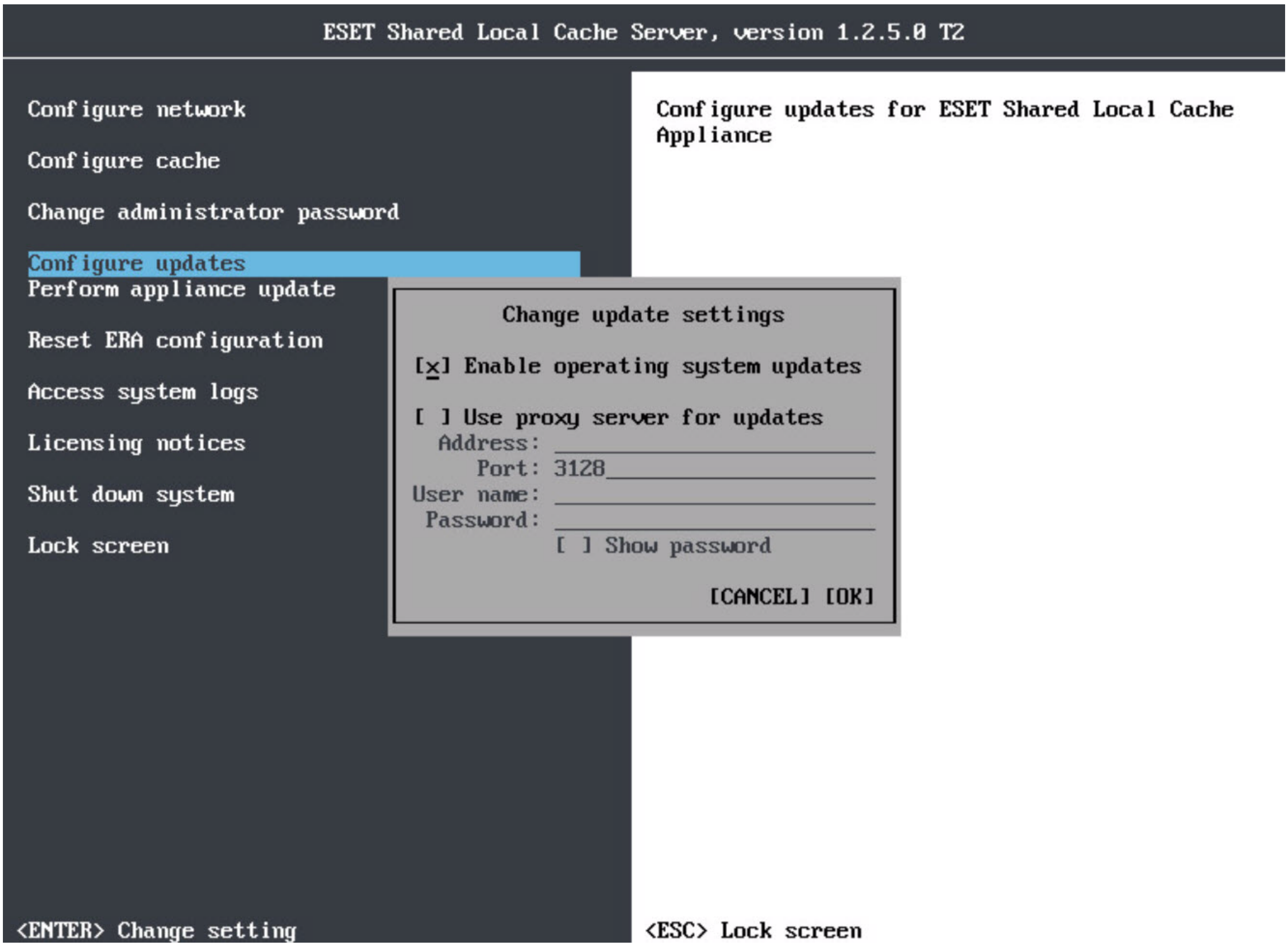
IMPORTANT
To update ESET Shared Local Cache, please download the newest installation file from download servers and re-deploy appliance or re-install .rpm.bin package.

To update operating system, select **Configure updates** from the management mode screen to edit the following settings:

- **Enable operating system updates** – Leave this option selected to check for all updates for the appliance operating system.
- **Use proxy server for updates** – Enter the IP address of your proxy server in the **Address** field. If your proxy server requires a Username and Password, enter these credentials in the appropriate fields.

NOTE
These fields are not for your Username/Password for ESET Shared Local Cache, and should only be completed if you know you need a password to access the internet via a proxy server.

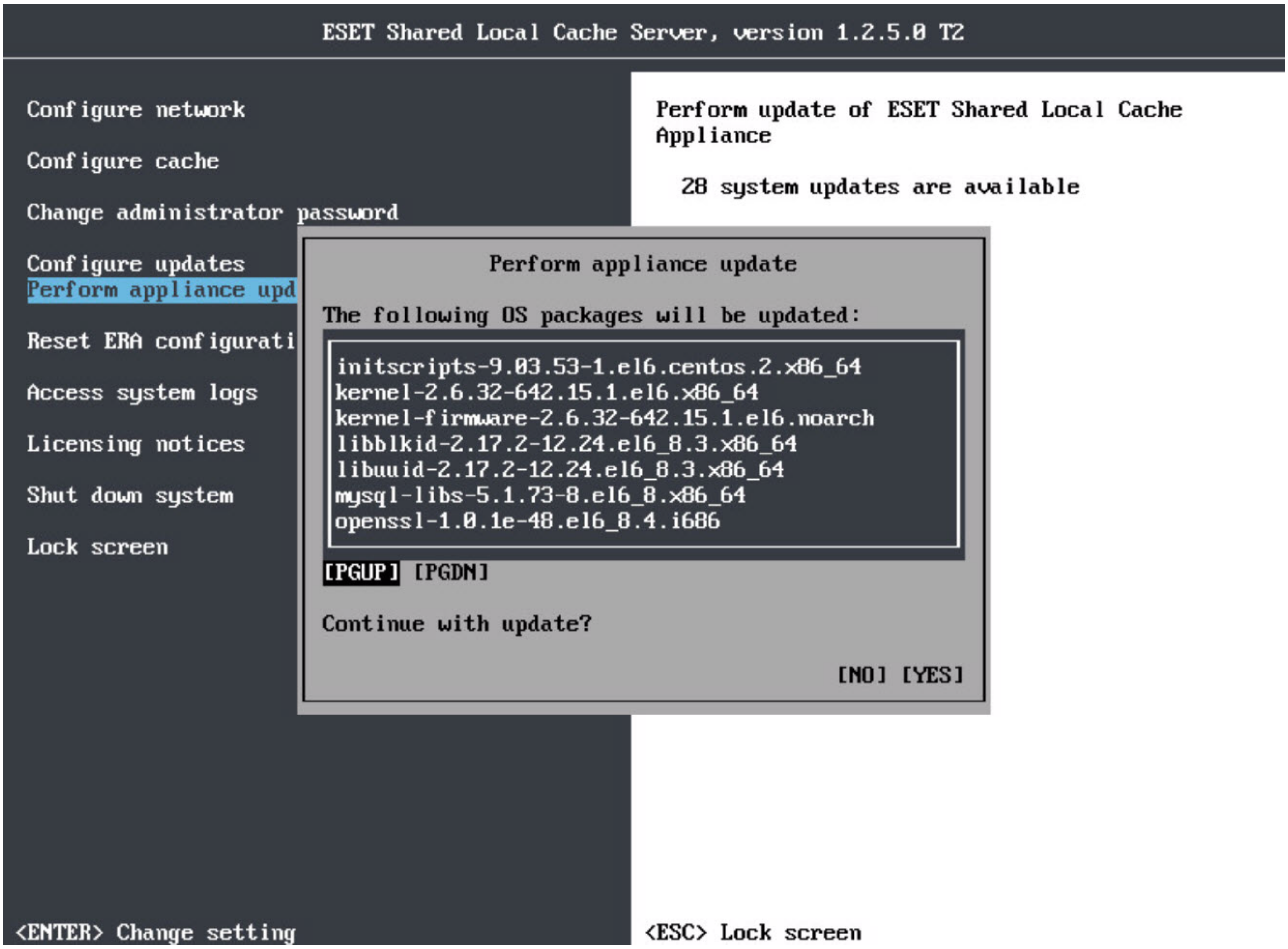
- A trusted SSL certificate is required for access to the proxy server, updates will fail is this certificate is not present.



```
ESET Shared Local Cache Server, version 1.2.5.0 T2

Configure updates for ESET Shared Local Cache
Appliance

Change update settings

[x] Enable operating system updates

[ ] Use proxy server for updates
  Address: ____________________
     Port: 3128________________
User name: ____________________
 Password: ____________________
           [ ] Show password

                  [CANCEL] [OK]
```

Once updates are available, select **Perform appliance update** from the basic information screen to open the update dialog. The update process can take several minutes depending on your network speed.

NOTE
When updates for your operating system are disabled, the operating system of the ESET Shared Local Cache appliance will not receive any updates. We recommend that you manually update ESET Shared Local Cache in situations where the automatic update feature has been disabled for operating system updates.



```
ESET Shared Local Cache Server, version 1.2.5.0 T2

Configure network                     Perform update of ESET Shared Local Cache
                                      Appliance
Configure cache
                                        28 system updates are available
Change administrator password

Configure updates
Perform appliance upd

Reset ERA configurati

Access system logs

Licensing notices

Shut down system

Lock screen

<ENTER> Change setting                <ESC> Lock screen
```

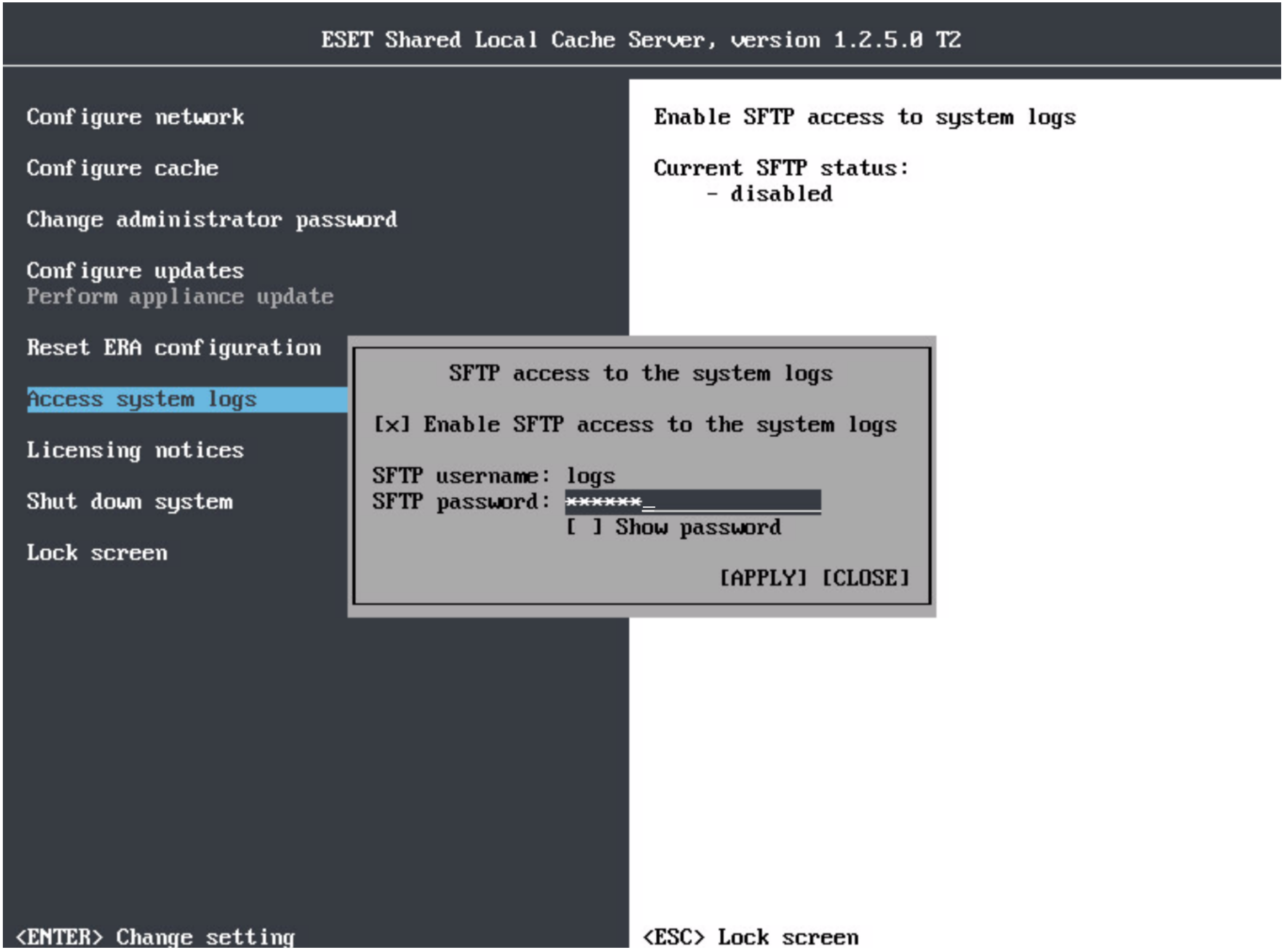
```
Perform appliance update

The following OS packages will be updated:

initscripts-9.03.53-1.el6.centos.2.x86_64
kernel-2.6.32-642.15.1.el6.x86_64
kernel-firmware-2.6.32-642.15.1.el6.noarch
libblkid-2.17.2-12.24.el6_8.3.x86_64
libuuid-2.17.2-12.24.el6_8.3.x86_64
mysql-libs-5.1.73-8.el6_8.x86_64
openssl-1.0.1e-48.el6_8.4.i686

[PGUP] [PGDN]

Continue with update?

                                [NO] [YES]
```

10. Communication

ESET Shared Local Cache cache uses the UDP communication protocol in order to provide the fastest request and response transaction. Hash-based Message Authentication Code (HMAC) is computed for each message, and a cache password which is required to ensure the authenticity of each cache request and response.

11. How to access system logs

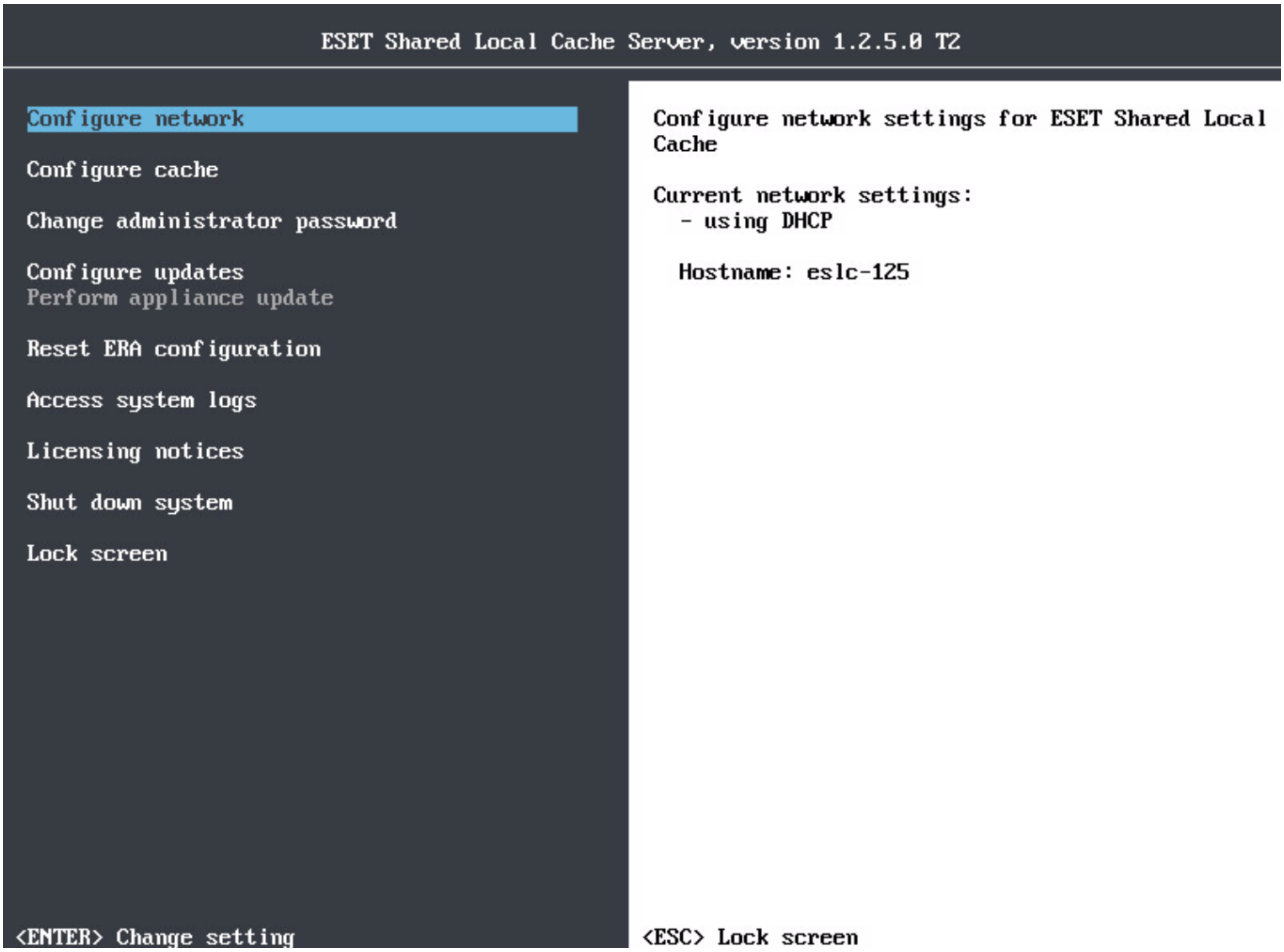
Enter Management mode and select menu **Access system logs** and then select **Enable SFTP access to the system logs**. Enter your password for SFTP access and select **Apply**.



```
ESET Shared Local Cache Server, version 1.2.5.0 T2

Configure network                 Enable SFTP access to system logs

Configure cache                   Current SFTP status:
                                      - disabled
Change administrator password

Configure updates
Perform appliance update

Reset ERA configuration
            SFTP access to the system logs
Access system logs
            [x] Enable SFTP access to the system logs
Licensing notices
            SFTP username: logs
Shut down system
            SFTP password: *******_
                           [ ] Show password
Lock screen
                                   [APPLY] [CLOSE]

<ENTER> Change setting            <ESC> Lock screen
```

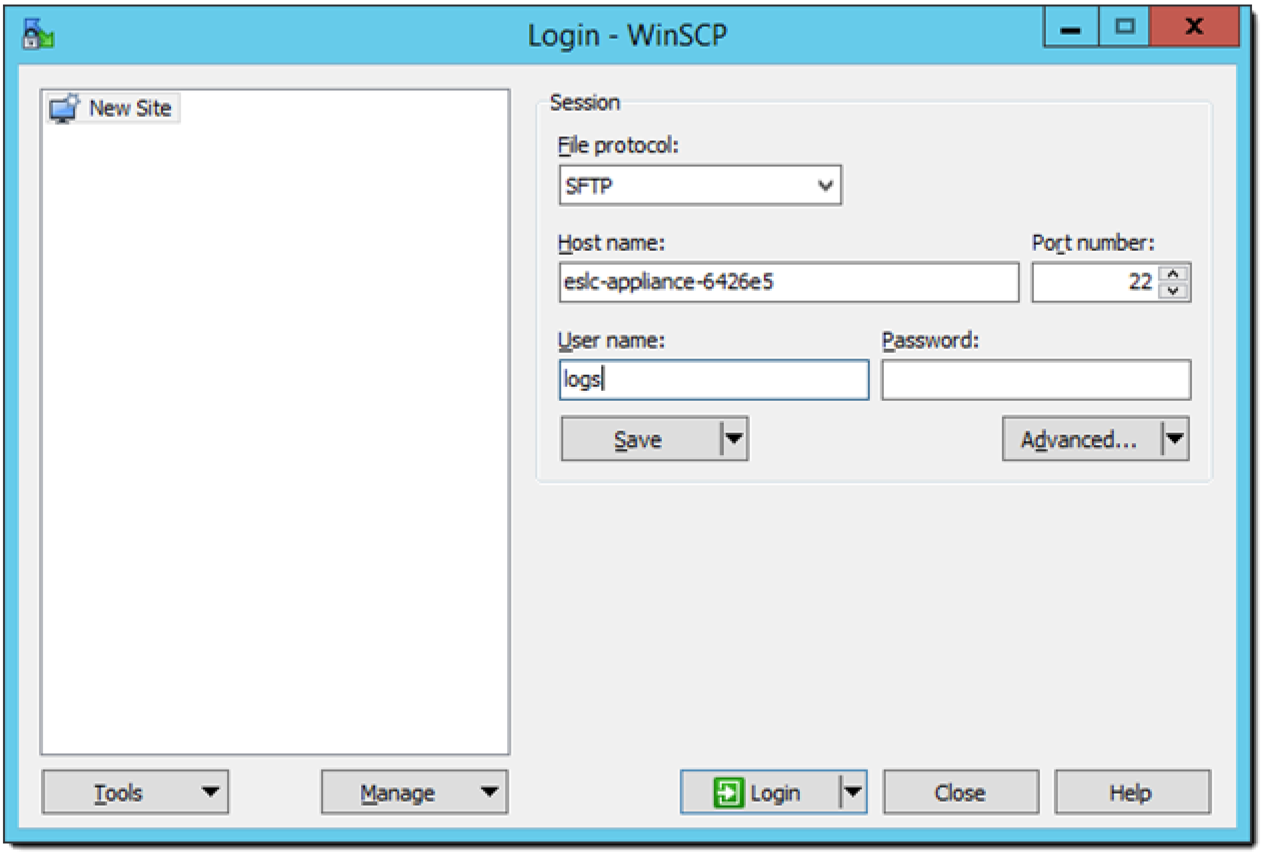
Run your SFTP client (we recommend to use free WinSCP SFTP client).

Enter the Hostname (you can find it in ESET Shared Local Cache in management mode > **Configure network**).



```
ESET Shared Local Cache Server, version 1.2.5.0 T2

Configure network                     Configure network settings for ESET Shared Local
                                      Cache
Configure cache
                                      Current network settings:
Change administrator password           - using DHCP

Configure updates                       Hostname: eslc-125
Perform appliance update

Reset ERA configuration

Access system logs

Licensing notices

Shut down system

Lock screen

<ENTER> Change setting                <ESC> Lock screen
```

Default SFTP port is 22. As User name, enter **logs**. Now you can **save** the configuration or just click **Login**.



Login - WinSCP

Session

File protocol: SFTP

Host name: eslc-appliance-6426e5

Port number: 22

User name: logs

Password:

When you are prompted for password, enter the password that you used in ESET Shared Local Cache.

Now you have access to ESET Shared Local Cache logs.

In communication with ESET Customer Care, you are normally prompted for these files:

- messages, dmesg, boot.log, yum.log (and all rotated copies (for example messages-20160411, maillog-20160411 and so on).
- all files from audit folder
- eset/RemoteAdministrator/EraAgentInstaller.log
- all files from eset/RemoteAdministrator/Agent/