ESET ENDPOINT ENCRYPTION SERVER

Product Manual
(intended for product version 2.9)
1. Overview

Please note that ESET Endpoint Encryption uses the DESlock Encryption engine.

ESET Endpoint Encryption Server includes several encryption solutions that you can distribute to client workstations using the DESLock+ Enterprise Server Console. This guide will help you download and install DESLock+ Enterprise Server Console, distribute encryption keys to client workstations and encrypt them. To learn more about an ESET Endpoint Encryption solution for your business, visit https://www.eset.com/us/business/endpoint-security/encryption/

Figure 1-1 ESET Encryption cloud distributes policies and instructions to client PCs
2. System requirements

Enterprise Server
- Internet Explorer 7 or later
- 32-bit OS: X(PSP3 ), Vista, 7, 8, 8.1, 10
  - 1GB RAM minimum (more is recommended for more recent operating systems)
  - 30GB available disk space (installation)
  - SQL Server 2005 Express or later
  - Port 443 must be configured to access the internet to successfully connect DESlock+ software to the cloud, proxy and licensing servers.

Client workstations
- Windows XP(SP3 ), Vista, 7, 8, 8.1, 10
- Internet Explorer 7 or later
- CPU 2GHz+
- 64 MB available disk space
- Access to the Server Proxy (HTTPS)
3. Download

1. Visit the ESET Endpoint Encryption Server page to download the installer. Click the Server tab. In the Installer Type drop-down menu, select All in one. Click Download to start the download. Save the file to the computer where you are installing ESET Endpoint Encryption Server. If you are upgrading an existing installation of ESET Endpoint Encryption Server, select Standalone installer.

2. Check that you have both of the license emails you received following your purchase of ESET Endpoint Encryption Server. You will need to have access to the DESlock+ Proxy ID and the Product key included in these emails to complete the installation of ESET Endpoint Encryption Server.
4. Enterprise Server installation

1. Double-click the DESLock enterprise server all in one installer file you downloaded in the download section. The setup Wizard will guide you through the installation process.

2. In the Enterprise Server License window, type your DESlock+ Proxy ID from the Important DESlock+ Enterprise Server license information email in the DESlock+ Proxy ID field and click Next.

![Figure 1-1](image)

Optional SQL Setup or Create your organization.

4.1 SQL Setup

Enterprise Server includes a version of Microsoft SQL Server Express. However, you may use your own version of Microsoft SQL Server. To do so, enter the details for your instance of SQL server during Enterprise Server setup.

- **SQL Server Name**—Include the full name of your instance unless it is an unnamed instance.

- **SA Username/SA Password**—This is the login for the sa database login, or any login which is a member of the sysadmin group. This login is used to create a new login for the Enterprise Server to use, creates a new Database on the specified instance and configures the login with db_owner, db_datareader and db_datawriter access to that database.

- **Database Name**—This is the name of the database that will be created on the specified instance. You may change this if you prefer to use a different name.
NOTE: SQL Server 2005 and 2008 Express Editions have a 4GB database maximum size limit. To increase this size limit you can upgrade to SQL Server 2008 R2 which has a 10GB limit or supply your own non-express version of SQL.

Create your organization.
4.2 Create your organization

1. In the Enterprise Server Details window, type a name for your organization in the Organization name field. This name will be used to navigate in the DESlock+ Enterprise Server dashboard. Type the Administrator Username and password you will use to log in to the Enterprise Server dashboard. Click Next.

![Enterprise Server Details](image)

**Figure 1-1**

Complete installation.
4.3 Complete installation

1. The server installation setup is complete. Click **Finish** to close the Setup wizard.

![Setup is Complete](image)

**Figure 1-1**

*Set up ESET Endpoint Encryption Server.*
5. Setting up ESET Endpoint Encryption Server

Setting up ESET Endpoint Encryption Server includes the following sections:

- ESET Endpoint Encryption Server [dashboard login]
- Add your license key

You will need to complete the following sections before you can begin enforcing encryption:

- Add users to your organization
- Create encryption key
- Create encryption key groups
- Generate activation codes for users

You may also need to set up the following optional settings:

- SMTP Server settings
- Sync with Active Directory
5.1 Dashboard login

1. Log in to DESlock+ Enterprise Server using the admin credentials you created during installation.

2. Select your organization and click OK.

Add your license key
5.2 Add your license key

NOTE: You will need a Pro license in order to perform Full Disk Encryption from Enterprise Server.

1. From the DESlock+ Enterprise Server main view, select your organization from the navigation tree and click the Licenses tab.

2. Click Add.

3. Type a description in the Description field, type the Product ID and Product Key you received in the DESlock+ Pro license information email in the appropriate fields and then click Next.

Figure 1-1
4. Review the information in the **License Validated** window and click **Next**.

5. A **License Added** message indicates the license was added successfully. Click **Close**.
6. Repeat steps 1-5 for each license you want to add.
7. Continue to SMTP Server settings, Sync with AD Directory or Add users to organization.

5.3 SMTP Server settings

If your organization uses an SMTP server, set up these settings to allow DESlock+ Server to send email via SMTP.

1. Click the menu icon > Control Panel > Settings.
2. Scroll down to the SMTP Server section and select the check box next to Configure SMTP Server.
3. Type the fully qualified domain name (FQDN) for your SMTP server and the port used for SMTP communications.
4. If you use SSL communication, select the check box next to Use a Secure connection (TLS).
5. If your mail server requires users to submit their credentials to log in, select the check box next to Authentication is required and type your mail server Username and Password in the appropriate fields.
6. Click Save at the bottom right when you are finished entering information.
7. Type an email address in the Test Email Address field and click Send a test email to verify that your settings were entered correctly.
Figure 1-1

Continue to Sync with Active Directory or Add users to organization.
5.4 Sync with Active Directory

If your organization uses Active Directory, configure these settings to allow DESlock+ Server to access user information from Active Directory.

1. Select your organization from the navigation tree.
2. Click the Active Directory tab and then click Settings.

3. Select the check box next to Enable Active Directory Synchronization.
4. Type the fully qualified domain name (FQDN) or IP address of the computer that has your Active Directory installed in the Directory Path field.
5. Type your Active Directory administrator Username and Password in the appropriate fields. Enterprise Server will search for users in the Active Directory with an email address property.
6. Select one of the options in the **Sync Mode** tab:

- **Manual import only**: The simplest method to import new users. You will need to select each user that you want to import. If the user's domain name changes, DESlock+ will not move them between teams.

- **Automatic with Team import**: This will retain Organization Unit (OU) information configured in AD and use it to create teams in DESlock+ Enterprise Server.

- **Basic Automatic import**: This will add AD users to the organization root, but will ignore any OU information configured in AD.

7. If you are using Self Enrollment, click the **Self Enrolment** tab and **Enable Self Enrolment**. Click **Choose License** to select the license to be associated with the users.
8. Click **Test** when you are finished configuring the settings.
8. If the settings are properly configured, you will see a confirmation dialog box. Once you are satisfied with the test results, **Close** the test results and then click **OK** to save the Active Directory settings. AD Sync is now operational.

9. Click **Resync** to initiate the sync. You can resync at any time to refresh Active Directory settings.

Figure 1-5

Add users to the organization
5.5 Add users to organization

Users must be added to ESET Endpoint Encryption Server before you can begin enforcing encryption.

Active Directory users:

If you selected Manual Import Only in the Sync with Active Directory section, follow the steps below:
1. From the DESlock+ Enterprise Server main view, select your organization from the navigation tree and click the Active Directory tab.
2. Select one or more users to add and click Quick Import.

Non-Active Directory users:

1. From the DESlock+ Enterprise Server main view, under your organization in the navigation tree, select Users.
2. Click Add.
3. Type the email addresses for the users you want to include and click **Add**. You can copy and paste the contents of a .csv file to add multiple users at a time.

The users you add are visible in the **Users** tab.
Figure 1-3

Create Encryption Key.
5.6 Create Encryption Key

1. From the DESlock+ Enterprise Server main view, select your organization from the navigation tree, click the Encryption Keys tab and then click Create.

![Figure 1-1](image1)

2. Type a name for the key in the Key Name field and select the type of encryption to use from the Algorithm drop-down menu (we recommend AES). Click Create when you are finished.

![Figure 1-2](image2)

3. The encryption keys you add are visible in the Encryption Keys tab.
5.7 Create Encryption Key Groups

Once a user is active (they have activated a client computer with the activation code sent from ESET Endpoint Encryption Server), you can add that user to an Encryption Key Group in ESET Endpoint Encryption Server.

Create a key group and assign encryption keys

1. From the DESlock+ Enterprise Server main view, select your organization from the navigation tree, click the Encryption Key Groups tab and then click Create.
2. Type a name in the Key group name field and click Add. We recommend that you name your Encryption Key Groups to mirror your team names to make it easier to know which users have access to which encryption keys.
3. Click the **Users** tab and double-click the active user that you want to add to your new Encryption Key group.

4. Click the **Encryption Key Groups** tab for that user and then click **Join Group**.
5. In the Select 1 or more Encryption Key Groups to join window, select the Encryption key group this user will be added to and click OK.
6. Click the **Encryption Key Groups** tab, double-click the Encryption key group and click **Add**.
7. In the **Add Encryption Keys to Key Group** dialog box, select the key that you created in the [Create encryption key](#) section and click **Add**. Click **Close**.

![Add Encryption Keys to Key Group dialog box](image)

**Figure 1-6**

*Generate activation codes for users.*
5.7.1 Add active users to Encryption Key Groups

If the encryption key groups are allocated to teams before any users are activated, you do not need to complete the steps below.

Send key files to users

1. From the DESlock+ Enterprise Server main view, select your organization from the navigation tree and click the Users tab.

2. Double-click your active user(s) and click Post Key-File > Post.

![Image of DESlock+ interface showing user details and Post Key-File option]

Figure 1-7

The user status will change and display the "The user has an update pending." message. Click Close.
5.8 Generate activation codes

If you will be using the self-enrolment feature, you do not need to generate activation codes. See the Self-enrolment section.

1. From the DESlock+ Enterprise Server main view, under your organization in the navigation tree, select Users.
2. Select one or more users and click Generate Activation Codes.

```
Figure 1-1
```

3. Select the DESlock+ platform to activate and click Next.
4. Select an available Pro license and click **Generate**.

Emails with the activation code will be sent to the email addresses associated with the users you selected in step 2. Proceed to **Client computer installation**.
6. Client workstation installation

Once a user receives their activation code, they have the necessary information to complete the installation on client workstations. You can use ESET Endpoint Encryption Server to distribute the client installation package to users.

- **Download the most recent installer version**
- **Network installation**
- **Internet installation**
- **Complete installation on client workstations**

6.1 Download client installer

To make sure you are distributing installation packages with the most recent version of the client installer, download it directly from www.eset.com.

1. Visit the [ESET Endpoint Encryption Server page](#) to download the most recent client installer. Click the **Client** tab. In the **Installer Type** drop-down menu, select the appropriate installer for your system and language. Click **Download** to start the download.

2. In ESET Endpoint Encryption Server, click **Client Software Deployment** in the navigation tree. Click the **Install Package Management** tab and then click **Upload**.

3. Select the file you downloaded in step 1 and click **Upload**.

![Figure 1-1](image)
4. Click **OK** in the Success dialog box. The client installer will be visible in the **Install Package Management** tab.
Complete a network installation or Complete an internet installation.
6.2 Network installation

1. From the DESlock+ Enterprise Server main view, select your organization > Workstations > Client Software Deployment. Click the Network Workstations tab.

2. Click Rescan Network to add any new users. Click OK when prompted.
3. Select the client workstations on which you want to install the endpoint encryption installation package and click Remote Install.

4. Review the settings and enter the necessary Administrator credentials in the Workstation Details tab of the Remote Install dialog box. Select a Workstation Policy, Version and Language for your installation package.
5. We recommend that you click the Managed Uninstall tab and select the check box next to **Enable Managed Uninstall Mode** so that the administrator will have the ability to force an uninstallation on client workstations.

6. When you are done with configuration, click **Post** to send the installation package to clients.
Complete installation on client workstations.

6.3 Internet installation

1. From the DESlock+ Enterprise Server main view, select your organization > Workstations > Client Software Deployment. Click the Install Package Management tab.

2. Select the appropriate installer version, architecture and language for the target computer.

3. Click Download Merged Install.

4. Select the Workstation Policy to apply to the install. We recommend that you select the check box next to Enable Managed Uninstall Mode so that the administrator will have the ability to force an uninstallation on client workstations.

5. Click Download to generate and download the installation package.
7. Send the file to the target computer, download and run it locally.

*Complete client installation.*
6.4 Complete client installation

Complete these steps on the client computer on which you are installing endpoint encryption.

1. Run the installation package after it has finished downloading.
2. Click Next to start the Setup wizard.
3. Accept the terms of the End-user license agreement. Follow the prompts in the wizard.
4. In the Customer Information window, type the User Name and Company name in the appropriate fields and click Next.

![Figure 1-1](image1.png)

5. In the Ready to Install window, click Install. In the Completing the DESlock+ Setup Wizard window, click Finish to complete setup and restart the computer.

6. In the DESlock+ (Activation required) window, type the activation code from the email that was sent in the Generate activation codes section and then click OK.

![Figure 1-2](image2.png)

7. The "DESlock+ is now activated" message will be displayed. Right-click the DESlock+ icon in your system tray.
DESIlock+
DESIlock+ is now activated.
Right-click the DESIlock+ icon to begin protecting your data.
DESIlock+ Frontend
7. Self-enrolment

The Self Enrolment feature provides automatic activation for client workstations that are on the same local network as the Enterprise Server. In order to use this feature, users must be in an Active Directory which is queried by the Enterprise Server to identify and enroll the user. You will need to complete the following steps in order to enable self-enrolment:

1. Enable Enterprise Server Direct Communications (ESDirect)
2. Configure firewall
3. Add Client license keys
4. Configure Active Directory settings
5. Configure Workstation policy settings
6. Install software on target client computers

With these settings configured, when the user logs into their domain network profile on a client workstation, they will activate automatically and appear licensed and linked to the workstation in Enterprise Server.
7.1 Enable ESDirect

Enable Enterprise Server Direct Communications (ESDirect)

1. Click the menu icon and select Control Panel.
2. Click Settings and scroll down to the Enterprise Server LAN Settings section.
3. Select Enable Enterprise Server Direct Communications if it is not already selected and optionally make changes to the Communications Port.

Note: If the communications port is changed, any existing DESlock+ clients will need to be reconfigured.

Configure firewall settings.

7.2 Configure firewall settings

For the client workstations to self-enrol, the network must allow access on the communications port specified in step 1, Enable ESDirect, into the machine hosting the Enterprise Server.

You should ensure that both hardware and software firewalls that protect the Enterprise Server are open on port 8266 (default setting) for both UDP and TCP traffic from domain network traffic. Alternatively, with software firewalls you can specify the executable of the Enterprise Server itself, dpecsrv.exe as an exclusion. This file can be located in the Enterprise Server folder C:\Program Files\DESlock+ Enterprise Server\ (or Program Files (x86) on 32 bit hosts).

Configure Active Directory settings.
7.3 Configure Active Directory Settings

Self Enrolment requires that the users have their details imported from an Active Directory server and have a license assigned to them. When configuring the **Active Directory settings**, you can select the license that the users are associated with when they enroll. If no license is selected, then only users that already have a license can use Self Enrolment.

![Active Directory Settings](image)

*FIGURE 1-1*

If you did not select to automatically import users in the **Active Directory settings** section, follow the steps in the **add users** section before continuing.

**Configure the Workstation Policy.**
7.4 Configure Workstation Policy

1. From the DESlock+ Enterprise Server main view, under your organization in the navigation tree, select Workstations.

2. Click the Workstation Policy tab and scroll down to the Key-File Settings section.


4. Change the setting to Yes and click OK to save your changes.
For additional help, see the Troubleshooting and Client settings sections.

7.5 Troubleshooting

Logging

The ESDirect and Self Enrolment log can be found in the following directories. If you are experiencing difficulties and require assistance then you should provide this with your support enquiry if possible:

Windows XP: \Documents and Settings\< username>\Local Settings\DESkey\DESlock+\ESDirect.log
Windows Vista and later: \Users\<username>\AppData\Local\DESkey\DESlock+\ESDirect.log

Communications Timeout

If the logfile details 'Server Not Found C03B0003' then the client computer is unable to communicate with the Enterprise Server. You should ensure that exceptions have been included for firewalls as detailed in the firewall section to allow the client computer to communicate with the Enterprise Server for both UDP and TCP protocols. Additionally if your network is configured to block multicast UDP packets, then you will need to specify the exact Server Address as detailed in the client settings section.
User not found

If the logfile details 'Command Failed C03B000E' then the user was not found in the Enterprise Server itself. You should ensure this user has been imported from the domain and has been added to the Enterprise Server. They should also be licensed already, unless you have selected a licence to use for auto licensing within the ES Direct settings.

### 7.6 Client settings

#### Client Settings

The following settings are used to control Self Enrolment in the DESlock+ client. This information is provided for reference, take care when editing the registry.

#### Server Address

Use this to manually set the address of the server if multicast UDP packets are blocked by the network. In this example, the server address is dlpes.mydomain.local. You may also set a static IP address instead of a name if DNS is not implemented correctly.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\DESlock\Client\CentralCtrl]
"DLPESDirectAddress"="dlpes.mydomain.local"
```

#### Enable Self Enrolment

Set through ES Workstation Policy

```
[HKEY_LOCAL_MACHINE\SOFTWARE\DESlock\Client]
"EnableSelfEnrolment"=dword:00000001
```

#### Server Port

Set through Enterprise Server Workstation Policy. The example below is of the default 8266 port.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\DESlock\Client\CentralCtrl]
"DLPESDirectPort"=dword:0000204A
```

#### Balloon Popup After Activation

This prevents the notification displayed to the user when the system activates.

No value = enabled

```
[HKEY_LOCAL_MACHINE\SOFTWARE\DESlock\Client\CentralCtrl]
"SelfEnrolmentPopup"=dword:00000000
```
8. Encrypting Client computers

Once the key file has been distributed to your client computers, you can initiate Full-Disk-Encryption (FDE) on client computers. NOTE: You will need a Pro license in order to perform a Full Disk Encryption from Enterprise Server.

Send the FDE command from ESET Endpoint Encryption Server.

1. From the DESLock+ Enterprise Server main view, select your organization from the navigation tree and click Workstations.

2. Double-click the client computer on which you want to initiate encryption.

3. Click Full Disk Encryption > Next.
4. In the Compatibility Checks window, click **Next**.

5. Select a security mode and click **Next**.
6. Select the FDE user and click Next.

7. Type a Username and Password to log in to the client computer. In the Single sign-on section, deselect the check box next to Prompt user to confirm the password above, before encryption starts. Click Next.

8. Type an Administrator Username and Password and click Next.

9. The system disk to be encrypted is displayed. Click Change Disk to select a different disk to encrypt. When you are finished making changes, click Next.
10. Click **Select Start Mode** and make a selection. We recommend that you select **Safe Start**.

11. Click **Start** to begin encryption.
The Full Disk Encryption (FDE) command will be sent to the workstation. The FDE command will be processed by:

- Waiting for the background check period to elapses (60 minutes by default)
- Double-clicking the DESlock+ icon in the notification area to log out and then logging back in
- Right-clicking the DESlock+ icon in the notification area and selecting Enterprise Sync from the context menu

Once the FDE command has been processed, the computer will either restart or start the FDE depending on the start mode selected.