kaspersky

Kaspersky Security Center FAQ

Contents

Kaspersky Security Center Frequently Asked Questions

We've got answers

How do I activate Kaspersky Security Center and Kaspersky applications?

The answer depends on what exactly you want to activate. To activate licensed features of Kaspersky Security Center, add an activation code or a key file in the Administration Server Quick Start Wizard or in the **License keys** section of the Administration Server properties.

If you activate Kaspersky Endpoint Security, you can do it through the *Add key* task to activate the application on specific devices, or you can enable the **Automatically distributed license key** option in the license key properties.

To activate any Kaspersky managed application, add the activation code or key file in the **Kaspersky Licenses** section through the Add License Key Wizard, and then enable the **Automatically distribute license key to managed devices** option.

Can I include a license key into an installation package to distribute the license key together with the Kaspersky managed application?

Yes, you can. However, we do not recommend including license keys in installation packages because this increases the risk of the license key being compromised. Instead, add the license key in the **Kaspersky Licenses** section, and then enable the **Automatically distribute license key to managed devices** option. View details in the step-by-step instructions.

How do I fix problems with connecting Network Agent to Administration Server?

You can detect connection issues by using the klnagchk utility. Run klnagchk with the needed flags to obtain diagnostic information, and then learn about the reasons of the detected connection issues.

How do I upgrade Kaspersky Endpoint Security for Business?

Purchase a license key for the next tier of Kaspersky Endpoint Security for Business. Add this license key in the Administration Server repository, and then add this license key in the **License keys** section of the Administration Server properties. After that, distribute the license key to the managed devices. View details in the step-by-step instructions.

How do I prevent the leakage of sensitive data when a corporate device is lost or stolen?

You can do it by using the File Level Encryption or Full Disk Encryption features. Because these features are available only in Kaspersky Endpoint Security for Windows, you can enable data encryption only for Windows-based managed devices. You can enable these features through the *Change application components* task for Kaspersky Endpoint Security for Windows. View details in the step-by-step instructions.

For additional details, refer to Online Help of Kaspersky Security Center.

How to activate Kaspersky Security Center and Kaspersky applications

This section describes how to activate the additional features of the Kaspersky Security Center and Kaspersky applications that are managed by Kaspersky Security Center, including Kaspersky Endpoint Security.

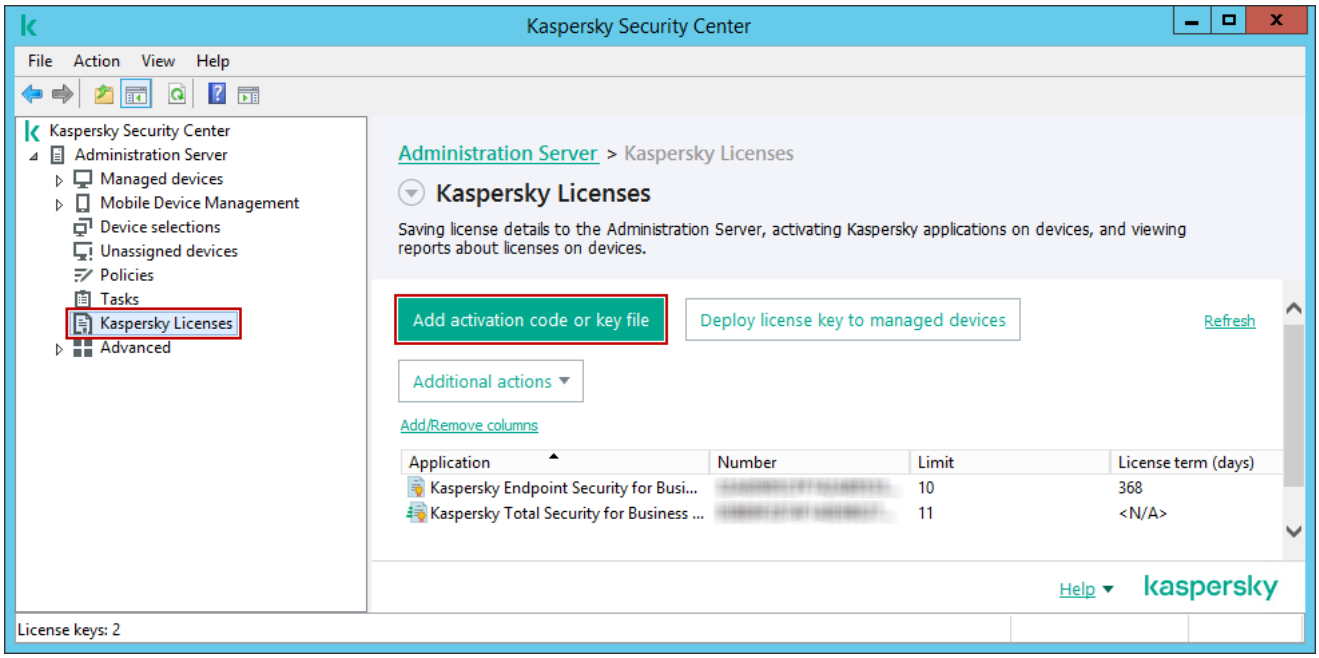
Activation of managed Kaspersky applications

License keys allow you to activate and use managed Kaspersky applications. When you use Kaspersky Security Center to add a license key, the license key settings are saved on the Administration Server. To add a license key to the Administration Server repository, you can apply a key file or enter an activation code. The key file (optional) and activation code are attached to the email message that you receive after you purchase Kaspersky Security Center. The received email message also contains the Kaspersky License Certificate and compatibility list (optional).

Activation of a managed application by using a key file

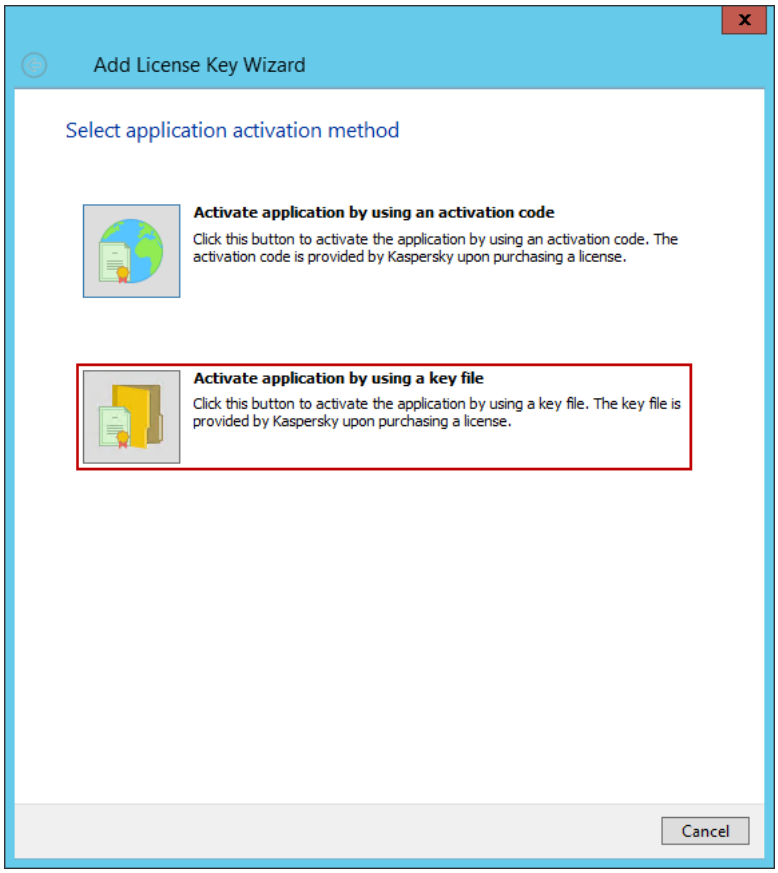
To activate a managed application by using a key file:

1. In the console tree, go to the **Kaspersky Licenses** node, and then click the **Add activation code or key file** button.



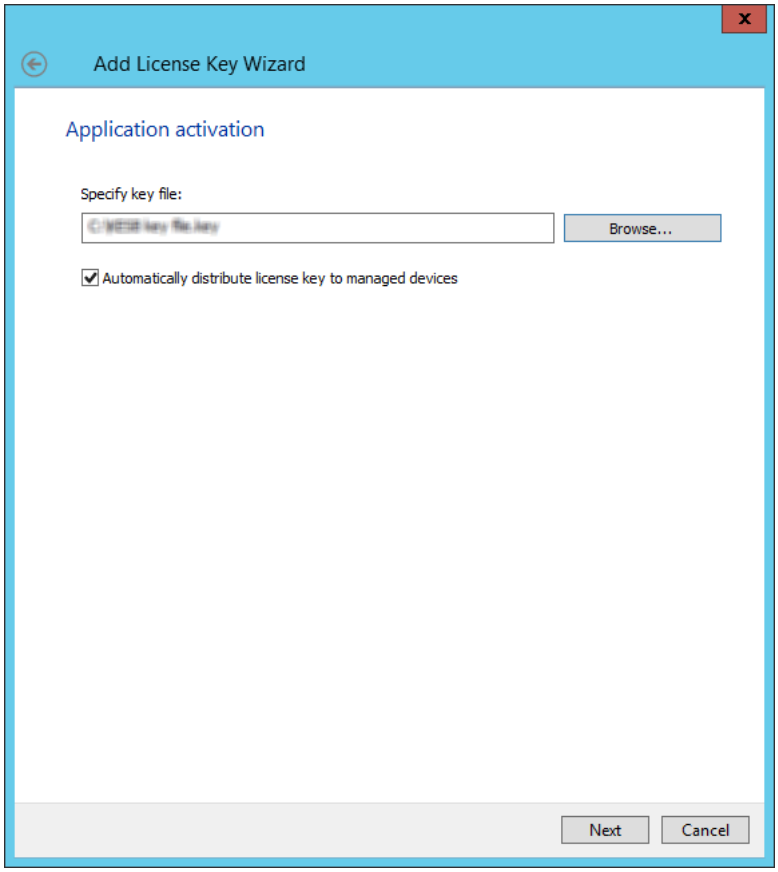
The **Kaspersky Licenses** workspace

2. In the Add License Key Wizard, click the **Activate application by using a key file** button.



The Add License Key Wizard. Select application activation method

3. Click the **Browse** button, and then select the key file that activates the managed application. You can select the **Automatically distribute license key to managed devices** check box to deploy the license key to devices automatically. Click the **Next** button to proceed.



The Add License Key Wizard. Application activation

4. Wait for the activation to finish, and then close the Wizard.

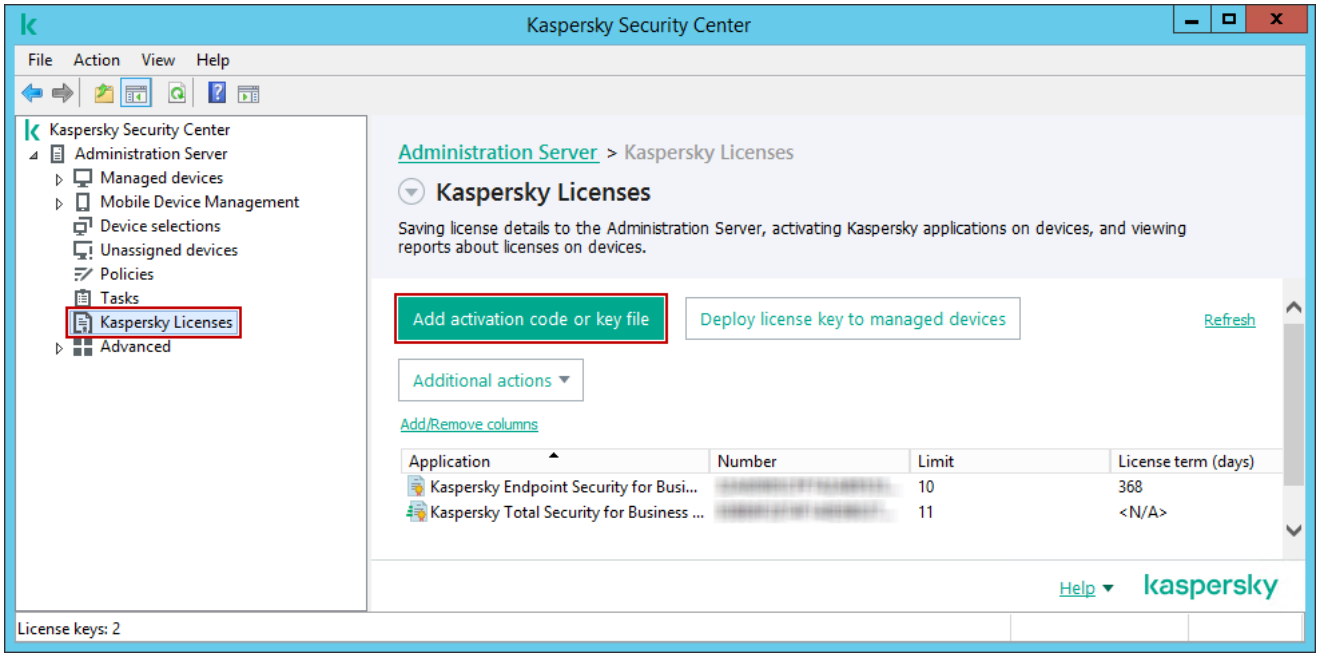
As a result, the managed application is activated and the license key is added to the Administration Server repository. The license key is now displayed in the **Kaspersky Licenses** workspace.

Activation of a managed application by using an activation code

To activate a managed application by using an activation code:

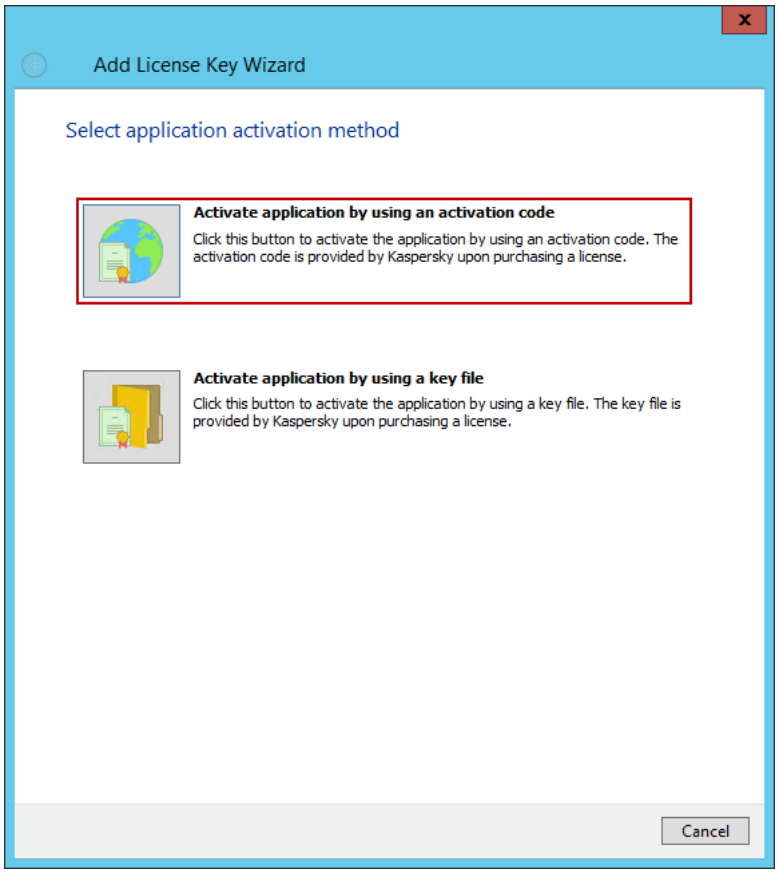
1. Ensure that Kaspersky Security Center is connected to the internet. Internet access is required to establish a connection with Kaspersky activation servers.

2. In the console tree, go to the **Kaspersky Licenses** node, and then click the **Add activation code or key file** button.



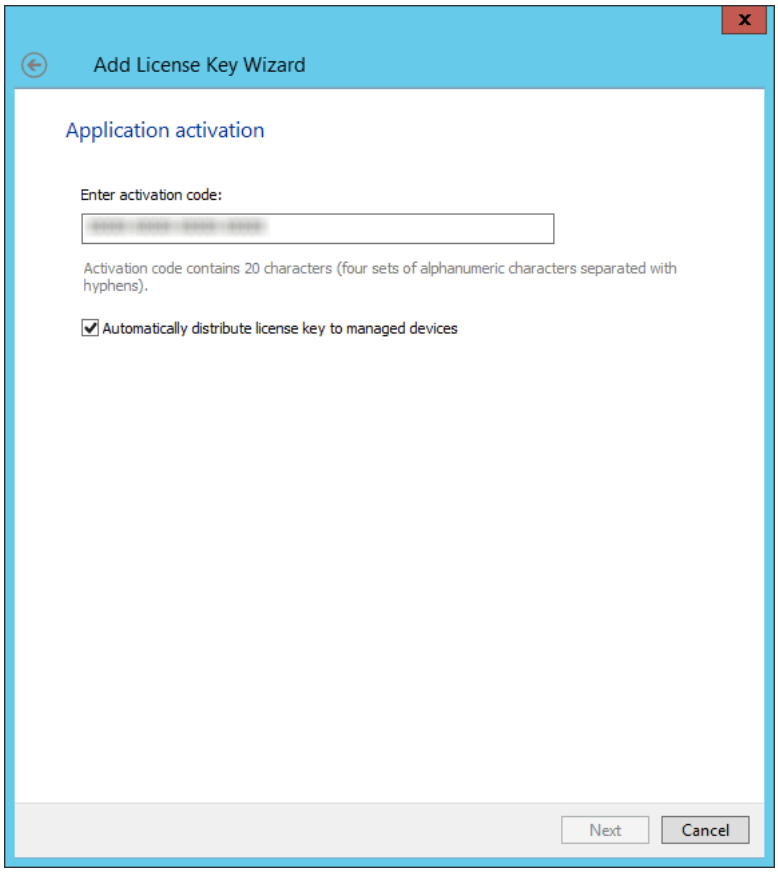
The **Kaspersky Licenses** workspace

3. In the Add License Key Wizard, click the **Activate application by using an activation code** button.



The Add License Key Wizard. Select application activation method

4. Enter an activation code. You can select the **Automatically distribute license key to managed devices** check box to deploy the license key to devices automatically. Click the **Next** button to proceed.



The Add License Key Wizard. Application activation

5. Wait for the activation to finish, and then close the Wizard.

As a result, the managed application is activated and the license key is added to the Administration Server repository. The license key is now displayed in the **Kaspersky Licenses** workspace.

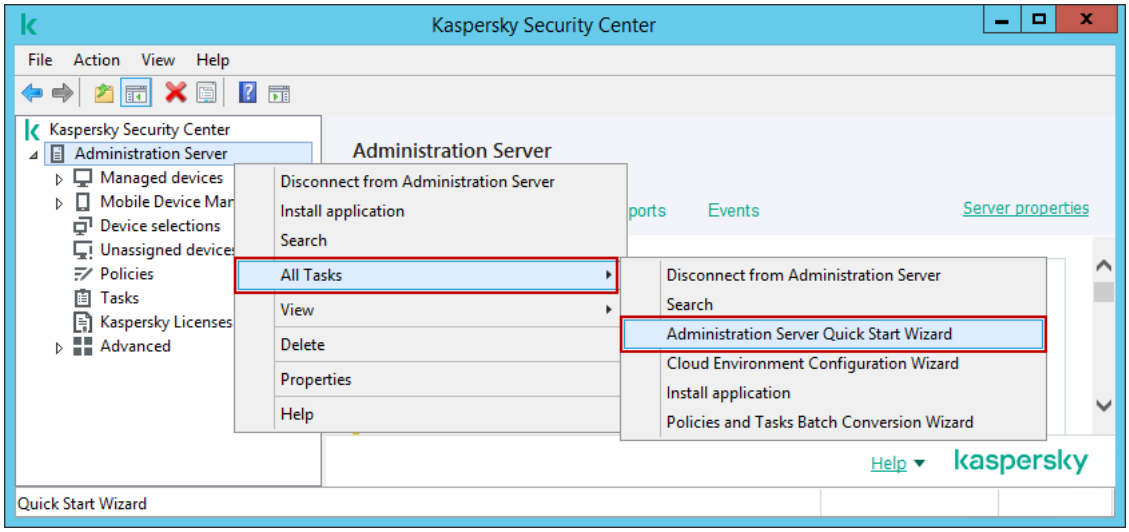
Activation of Kaspersky Security Center licensed features

You can activate licensed features to use additional functionality of Kaspersky Security Center (for example, Vulnerability and Patch Management). There are two ways to accomplish this task: use the Administration Server Quick Start Wizard or the Administration Server properties.

Activation by using the Administration Server Quick Start Wizard

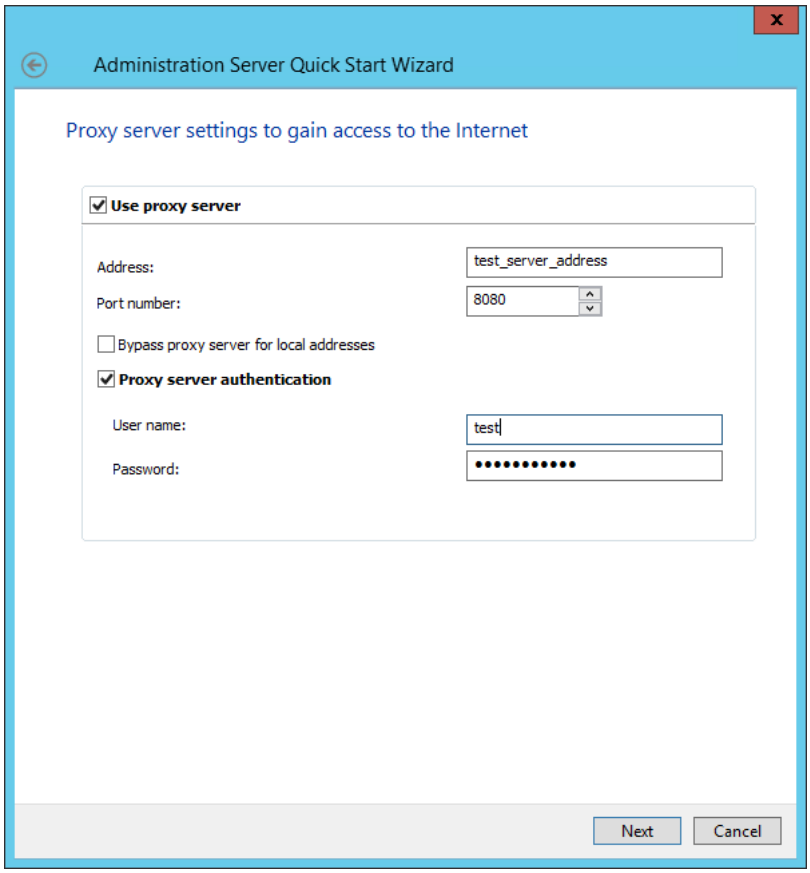
To activate licensed features of Kaspersky Security Center by using the Administration Server Quick Start Wizard:

1. In the console tree, right-click the Administration Server node, and then select **All tasks** → **Administration Server quick start wizard**.



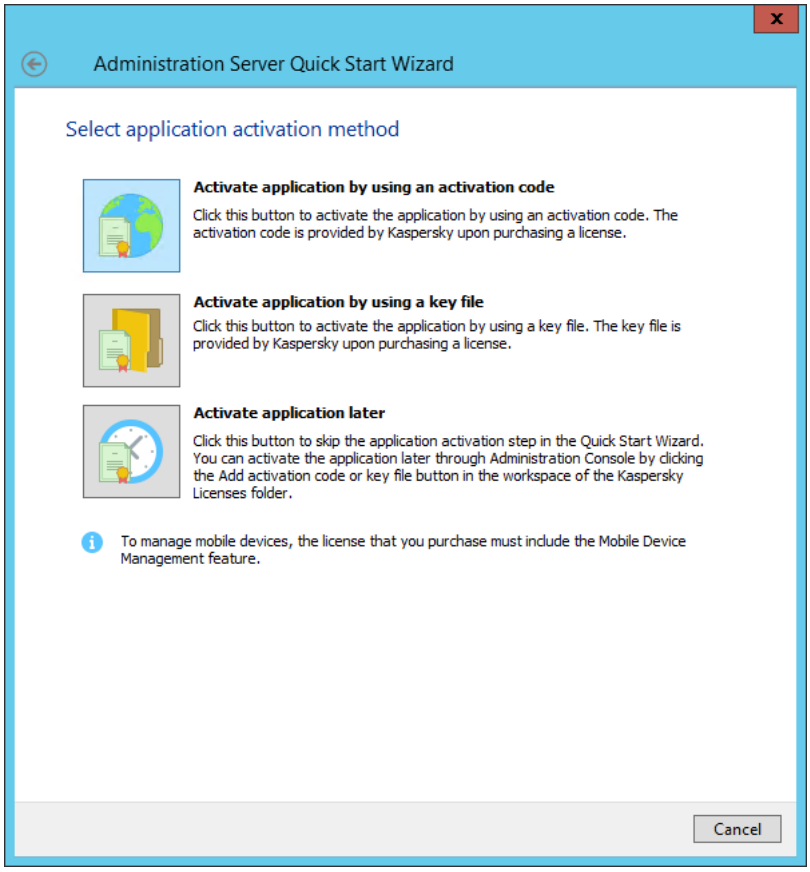
The context menu of the Administration Server node

2. Specify the internet access settings for Administration Server.



The Administration Server Quick Start Wizard. Proxy server settings to gain access to the internet

3. Select one of the Kaspersky Security Center activation methods.



The Administration Server Quick Start Wizard. Select application activation method

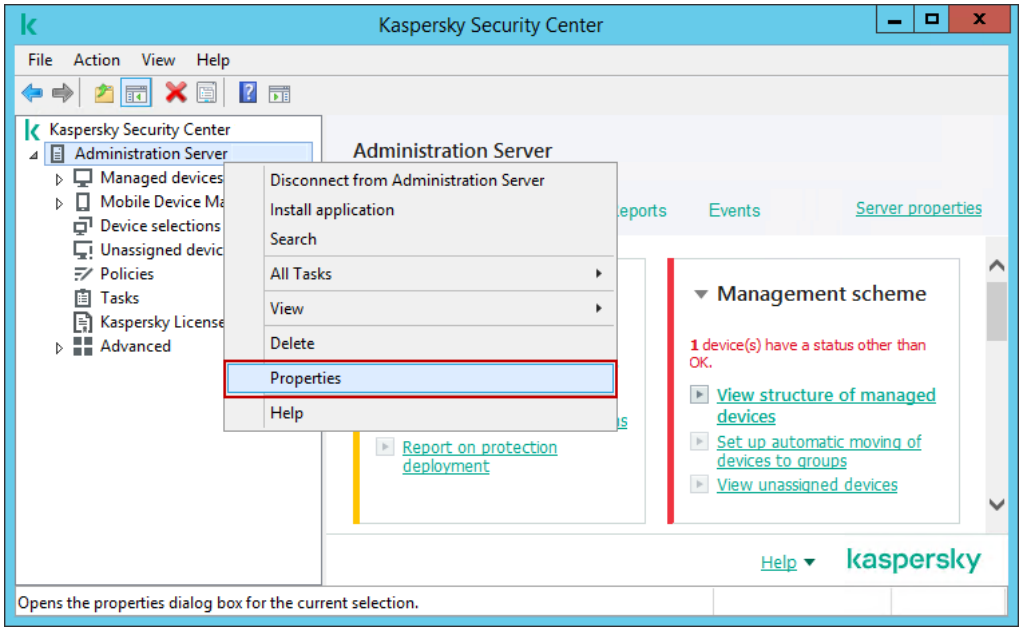
4. Activate a Kaspersky Security Center feature with a key file or an activation code.

Activation by using the Administration Server properties

To activate the Vulnerability and Patch Management feature, use only the Administration Server properties.

To activate licensed features of Kaspersky Security Center by using the Administration Server properties:

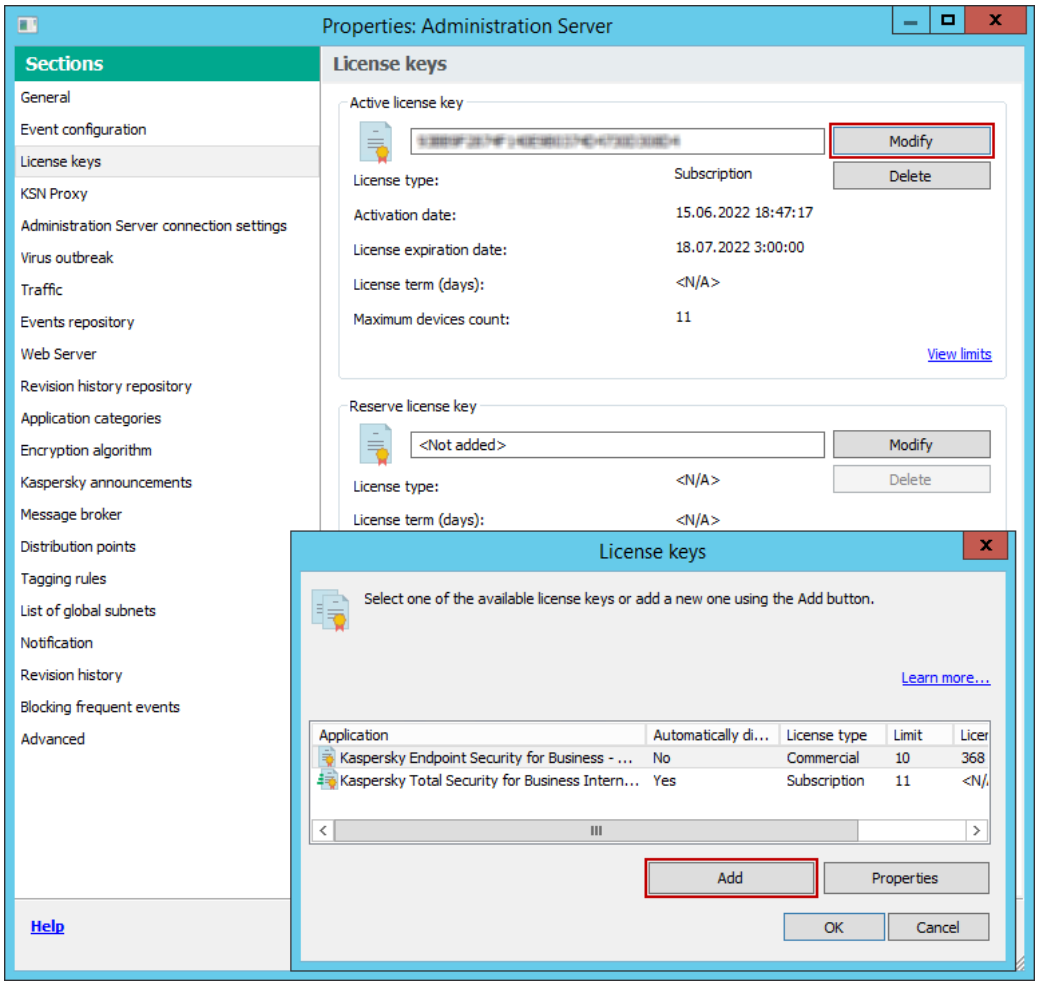
1. In the console tree, right-click the Administration Server node, and then select **Properties**.



The context menu of the Administration Server node

2. In the **Properties** window, go to the **License keys** section. The **Active license key** section displays the license key in use. To change the active license key, click the **Modify** button, and then choose an available license key from the Administration Server repository. If you want to add a new active license key, click the **Add** button, and then follow the Add License Key Wizard steps.

   You can also add a reserve license key. Click the **Modify** button in the **Reserve license key** section, and then choose an existing license key or add a new one. Note that you cannot add a reserve license key if there is no active license key.



The Administration server properties window

Kaspersky Endpoint Security Activation

You can activate Kaspersky Endpoint Security remotely through Kaspersky Security Center or locally through the Kaspersky Endpoint Security interface.

If you perform a remote Kaspersky Endpoint Security activation through Kaspersky Security Center, use one of the following methods:

- Use the *Add key* task.

  This method allows you to add a license key to a specific computer or to computers that are part of an administration group.

- Distribute a license key stored on the Kaspersky Security Center Administration Server to the computers.

  This method allows you to add a license key automatically to computers that are already connected to Kaspersky Security Center, and to new computers. To use this method, you first need to add the key to the Kaspersky Security Center Administration Server.

- Add a license key to a Kaspersky Endpoint Security installation package.

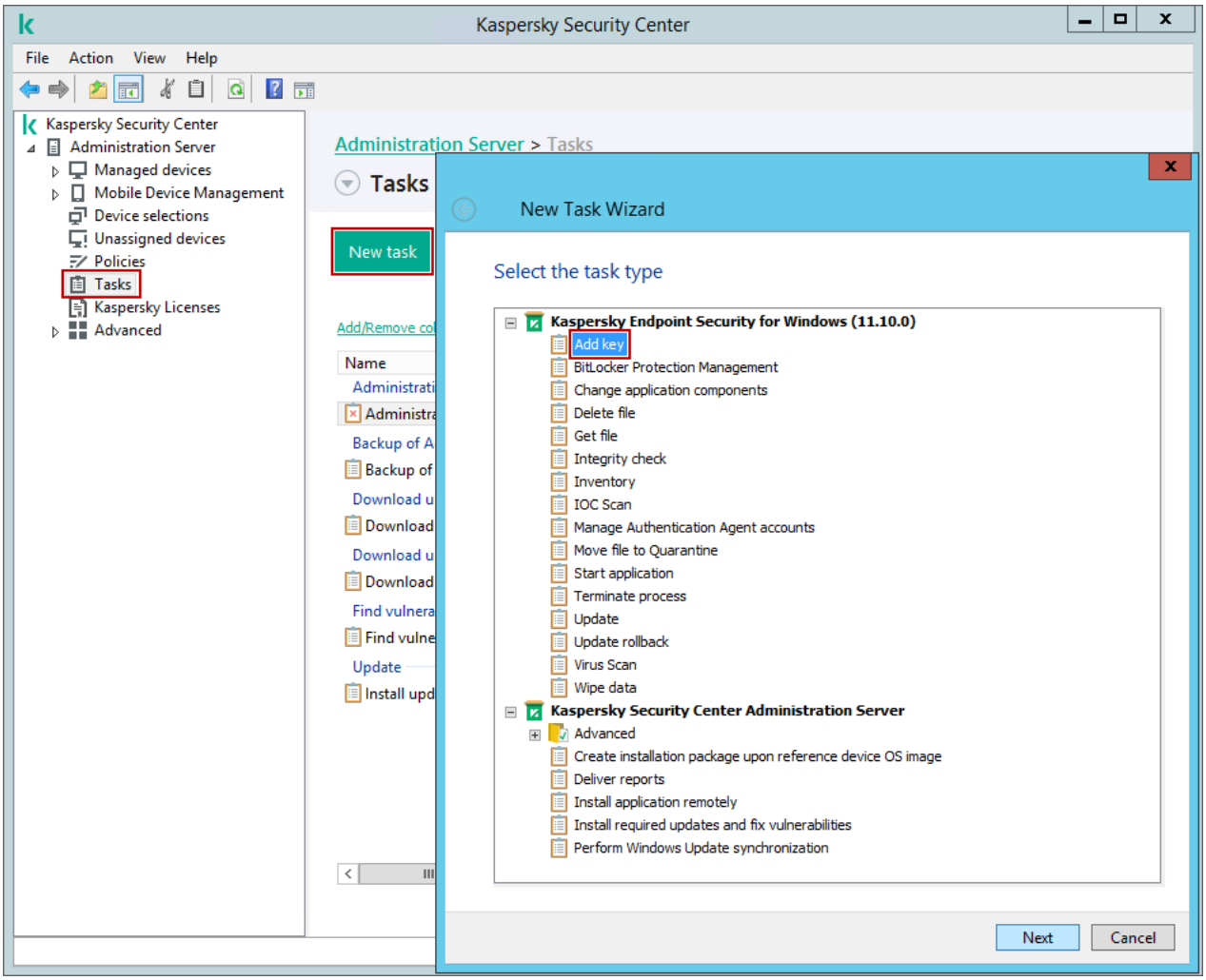
  This method allows you to add a license key to an installation package during Kaspersky Endpoint Security deployment. The application is automatically activated after the installation.

For security reasons, this method is not recommended. A key file or activation code added to an installation package may be compromised.

Remote activation by using the Add key task

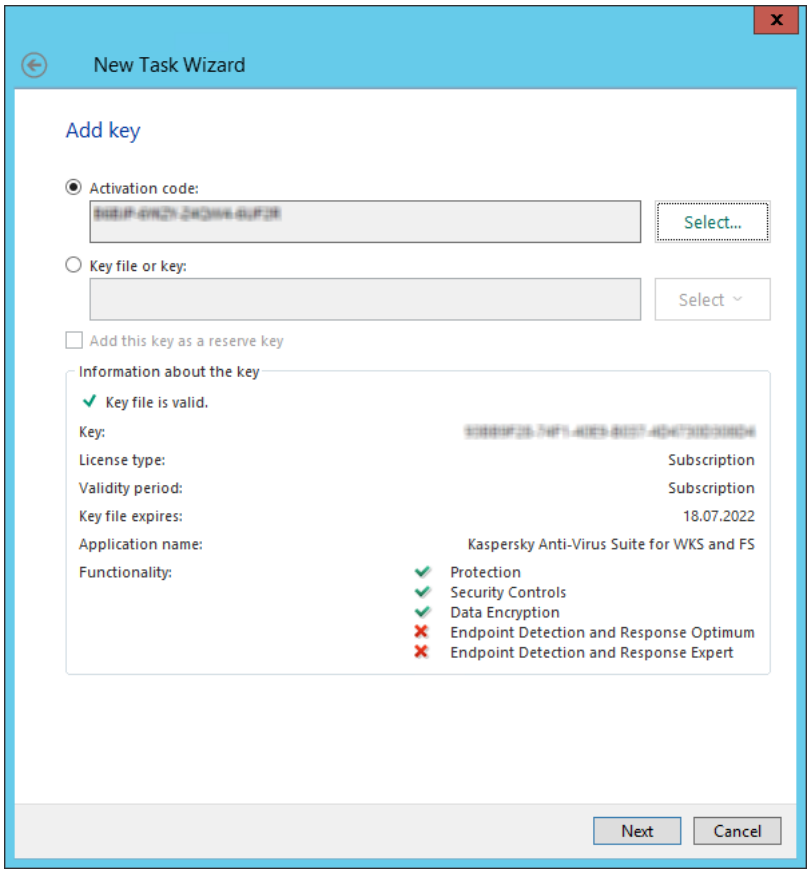
To activate Kaspersky Endpoint Security by using the Add key task:

1. In the console tree, select the **Tasks** node, and then click the **New task** button.
2. In the New Task Wizard, expand the **Kaspersky Endpoint Security** node, and then select the **Add key** item.



The New Task Wizard. Select the task type.

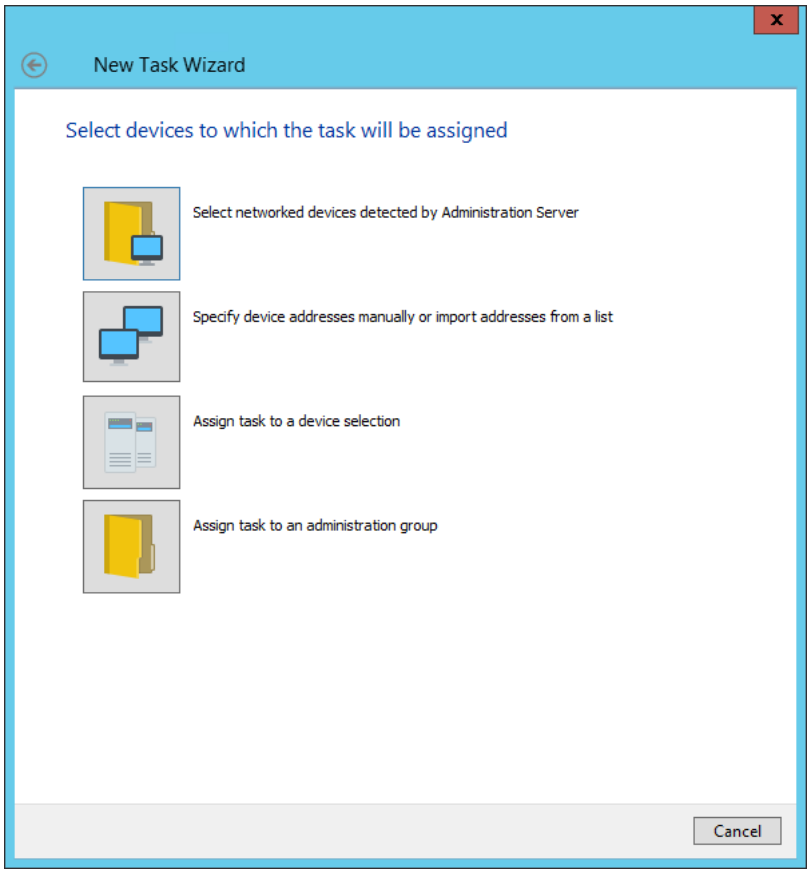
3. Enter an activation code or select a key file.



The New Task Wizard. Add key

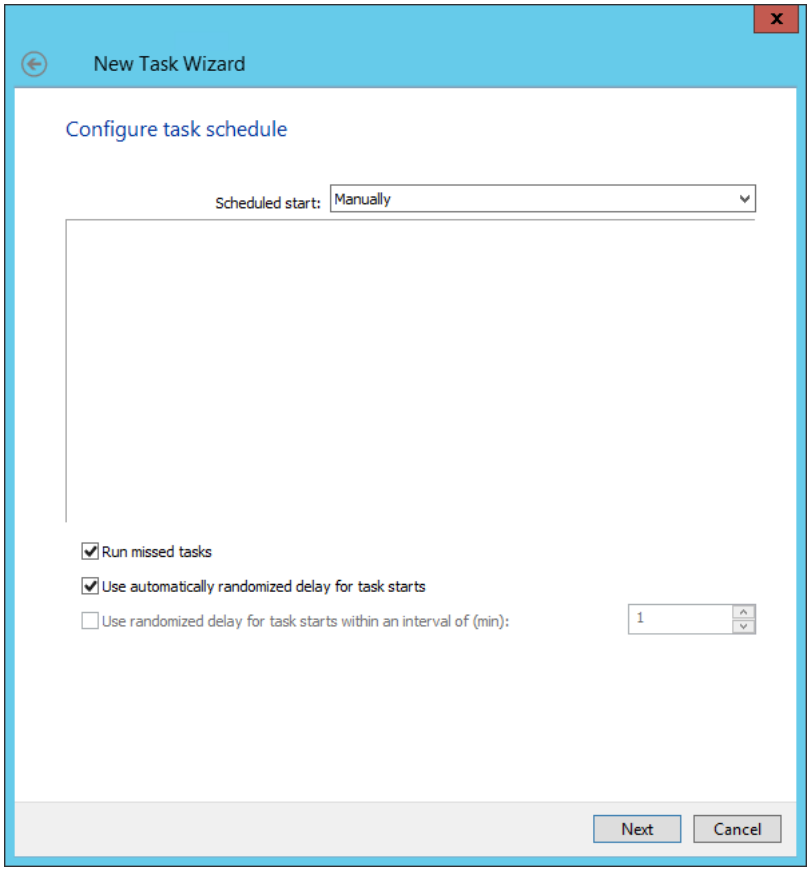
4. Select the computers on which the task will be performed. The following options are available:

- Select computers that the Administration Server detects in the network (unassigned devices). The specific devices can include devices in administration groups, as well as unassigned devices.
- Specify device addresses manually or import addresses from a list. You can specify NetBIOS names, IP addresses, and IP subnets of devices to which you want to assign the task.
- Assign the task to a device selection. In this case, the task is assigned to devices that meet specific criteria.
- Assign the task to an administration group. In this case, the task is assigned to computers included in an administration group.



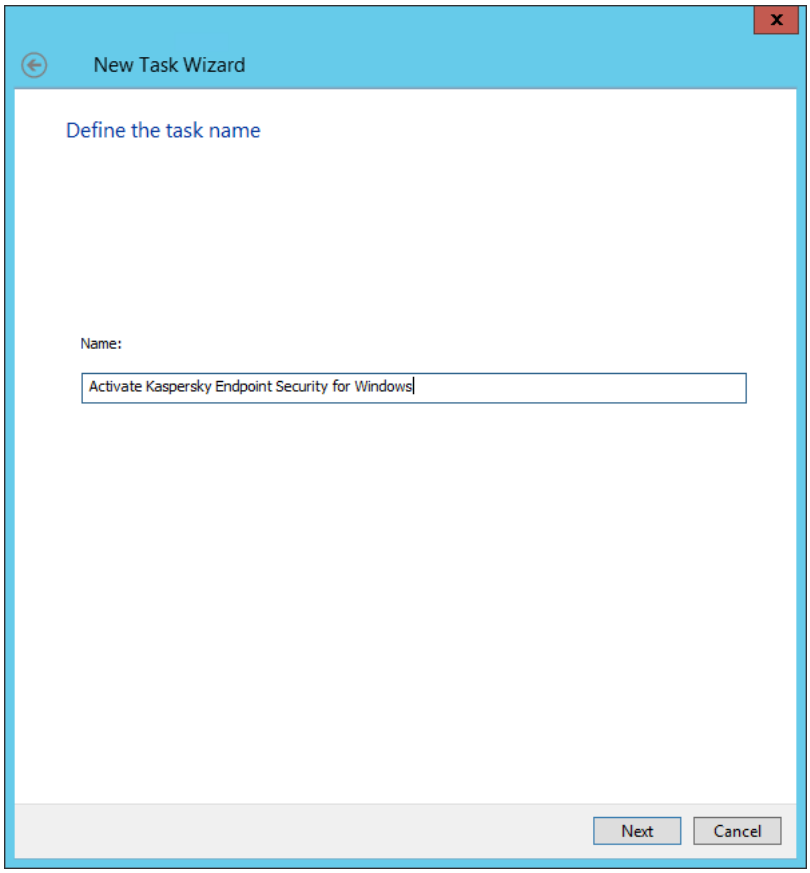
The New Task Wizard. Select devices to which the task will be assigned

5. Configure a schedule for starting the task, for example, manually or when the computer is idle.



The New Task Wizard. Configure task schedule

6. Specify the task name.

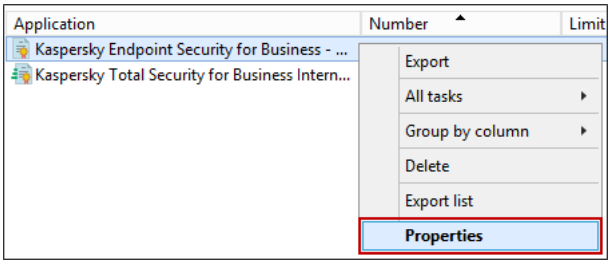


The New Task Wizard. Define the task name

Automatically distributing a license key to the computers

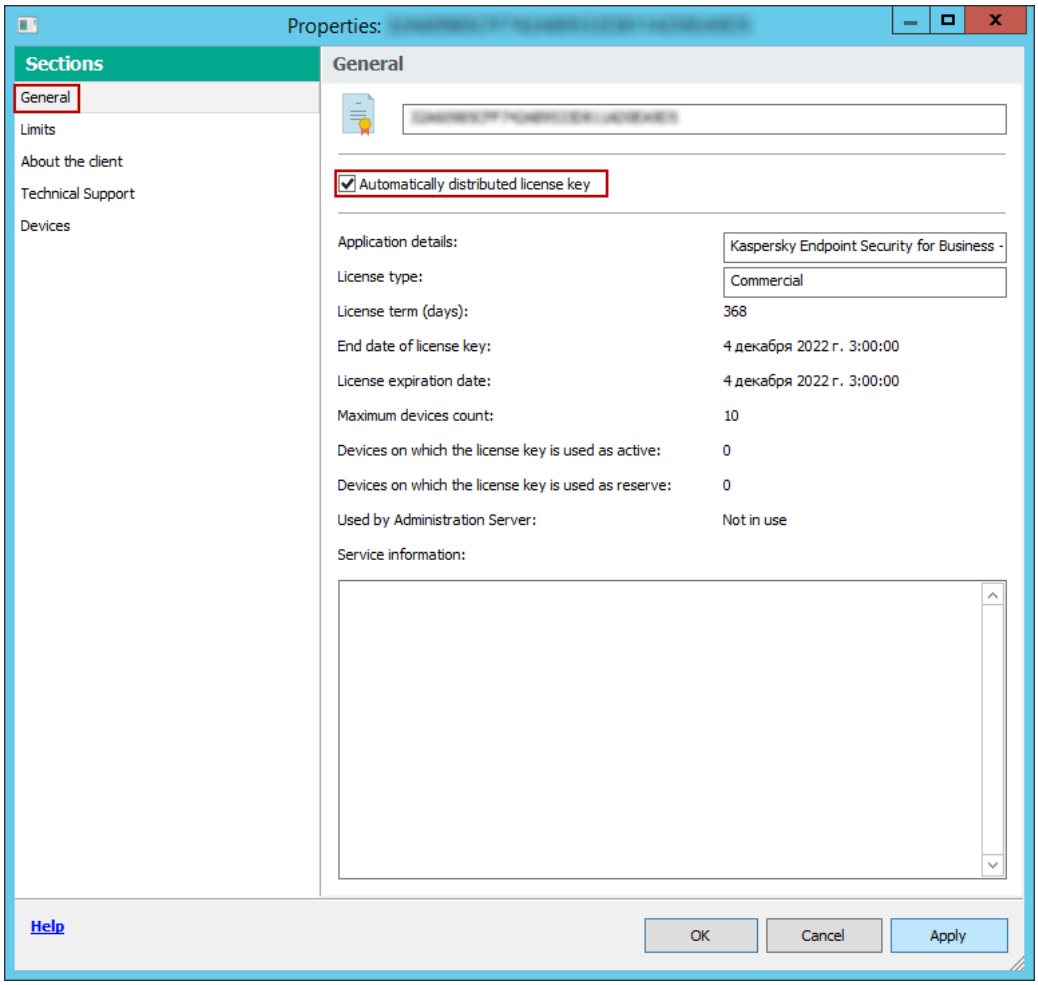
To distribute a key stored on the Kaspersky Security Center Administration Server to the computers:

1. In the console tree, go to the **Kaspersky Licenses** node.
2. In the **Kaspersky Licenses** workspace, right-click a license key to be distributed, and then select **Properties**.



The context menu of the license key

3. In the **General** section, select the **Automatically distributed license key** check box. Save your changes.



The window of the license key properties

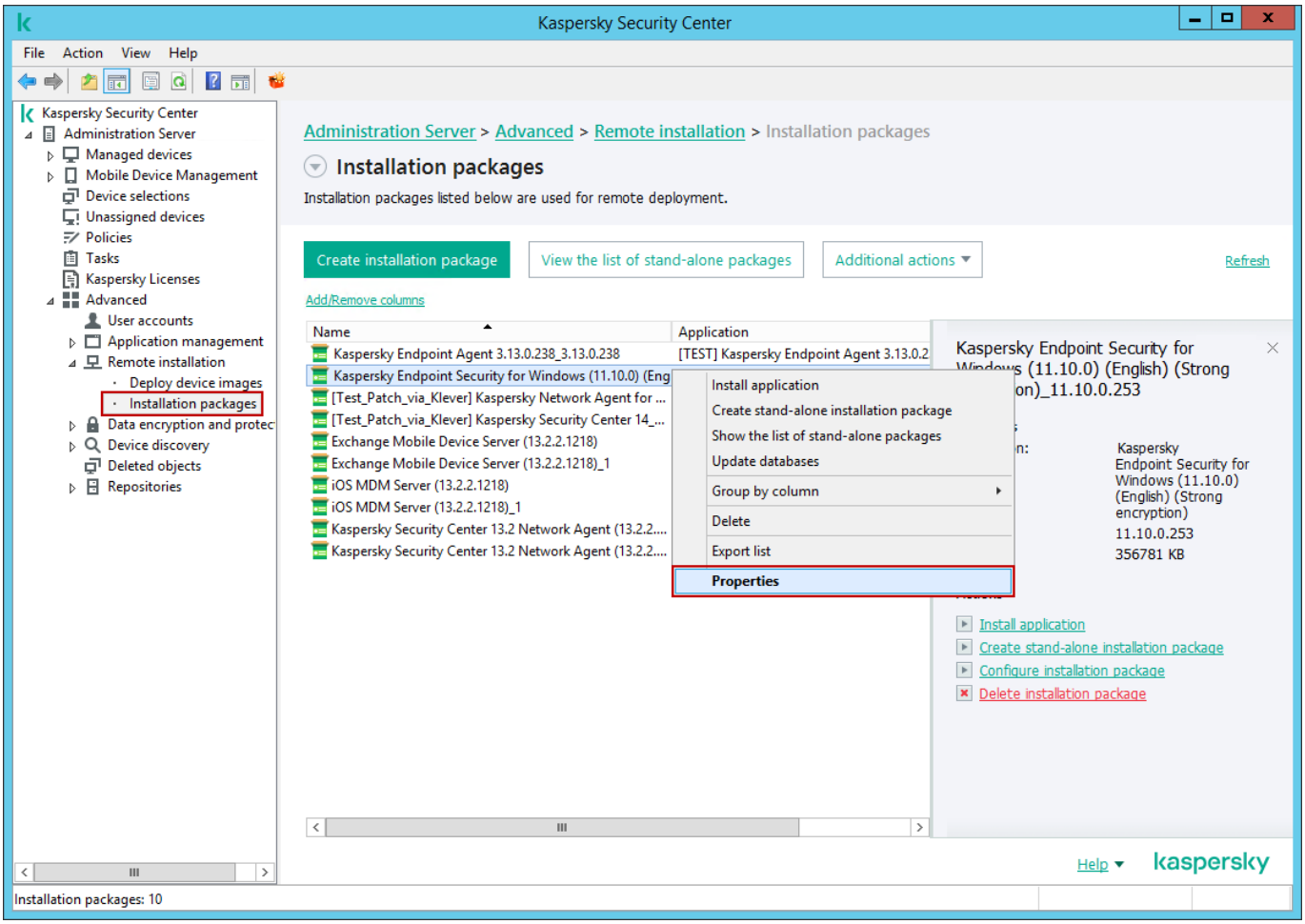
As a result, the license key is automatically distributed to the computers. During automatic distribution of a license key as an active or a reserve key, the licensing limit on the number of computers (set in the key properties) is taken into account. If the licensing limit is reached, distribution of this key to computers ceases automatically. You can view the number of computers to which the key has been added and other data in the key properties in the **Devices** section.

Adding a key file to the Kaspersky Endpoint Security installation package

To add a key file to the Kaspersky Endpoint Security installation package:

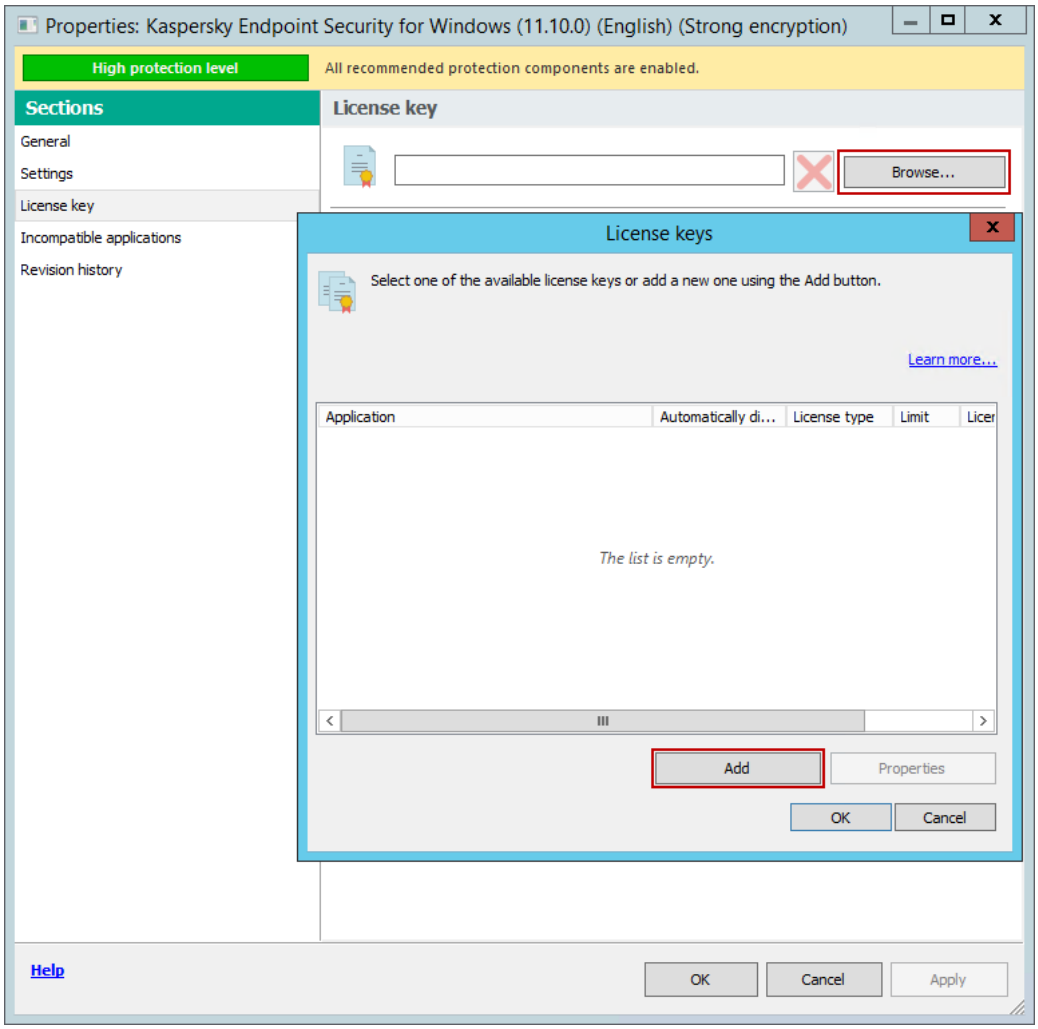
1. In the console tree, go to **Advanced** → **Remote installation** → **Installation packages**.

2. In the **Installation packages** workspace, you can view installation packages that are downloaded to Kaspersky Security Center. Right-click an installation package from the list, and then select **Properties**.



The **Installation packages** workspace

3. Go to the **License key** section, and then click the **Browse** button. Select an available license key or click the **Add** button to add a new license key.

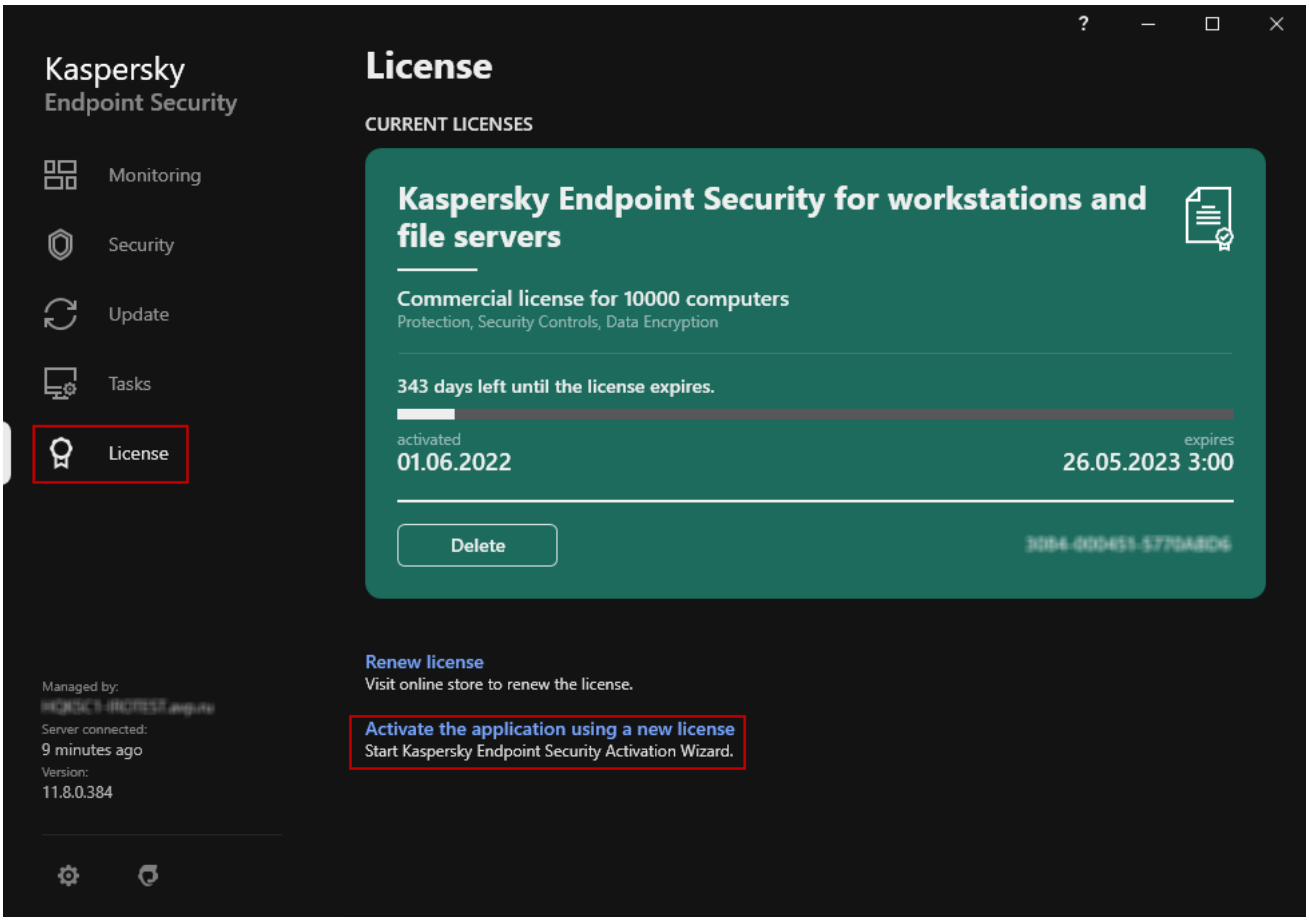


The window of the installation package properties

Local activation by using the Activation Wizard

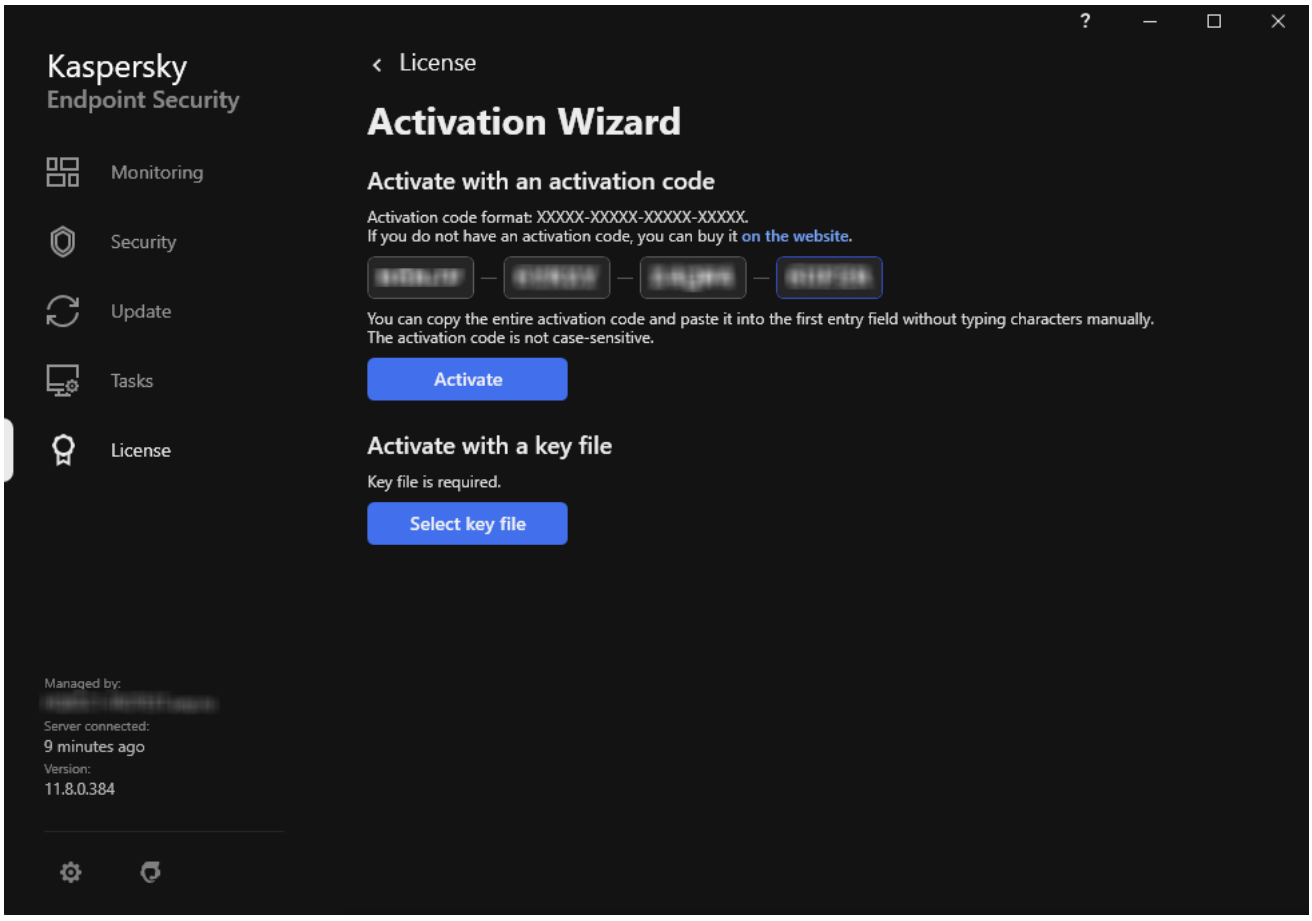
To activate Kaspersky Endpoint Security by using the Activation Wizard:

1. In the main Kaspersky Endpoint Security application window, go to the **License** section, and then click **Activate the application using a new license**.



The **License** section of the Kaspersky Endpoint Security application's main window

2. The Activation Wizard starts. Apply a key file or an activation code to activate the Kaspersky Endpoint Security.



The Activation Wizard window

Viewing license information in Kaspersky Security Center

The list of license keys in use is displayed in the **Kaspersky Licenses** workspace. You can select a license key in the workspace to view the license key properties in the **Properties** window on the right. The **Properties** window also contains the following links:

- **Export key file**

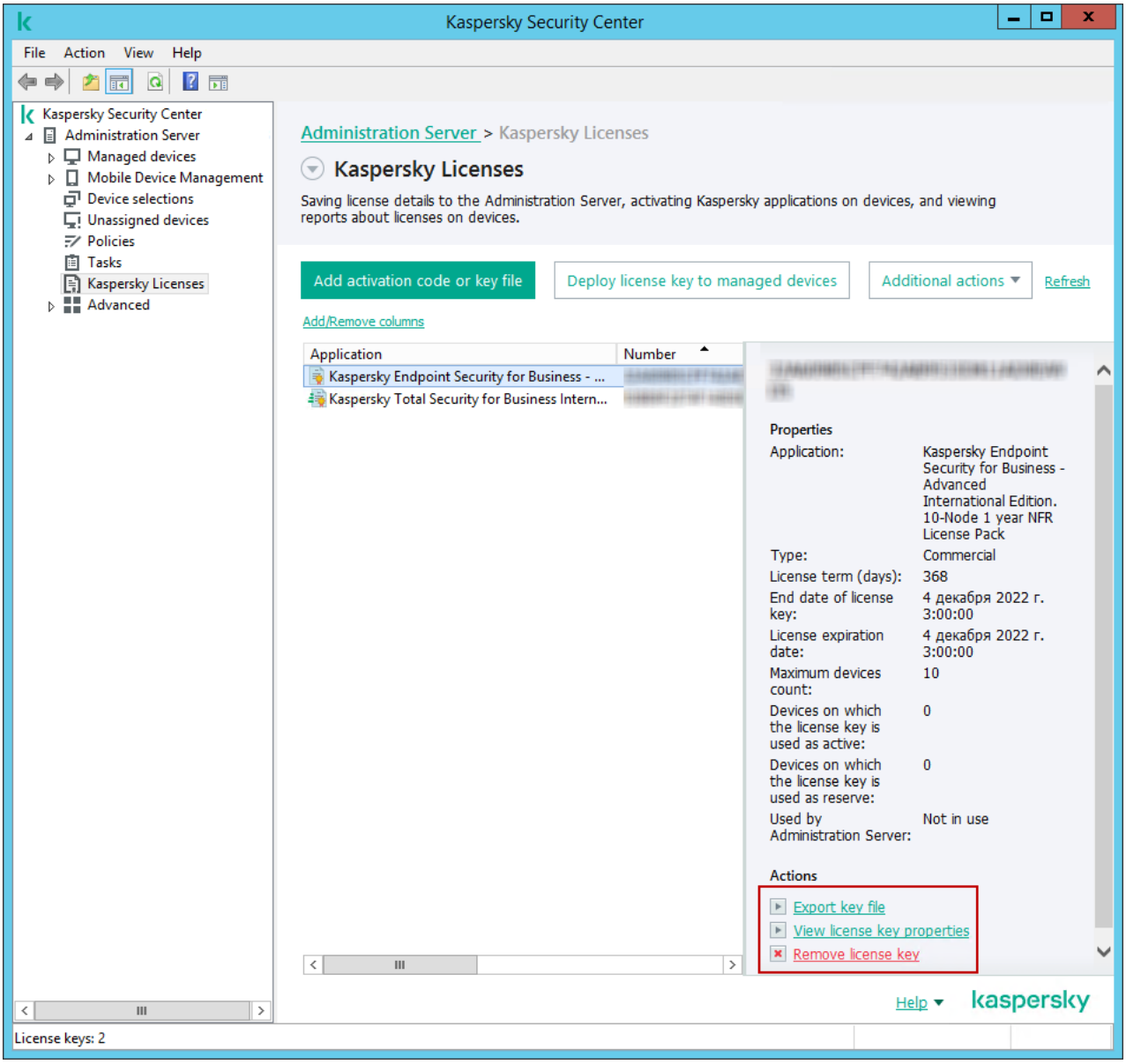
  Click this link to save the license key in the KEY file format.

- **View license key properties**

  Click this link to view more information about the license key.

- **Remove license key**

  Click this link to remove the license key.



The **Kaspersky Licenses** workspace

The following icons are displayed next to the names of license keys and indicate the type of license key use:

-  —The license key is stored in the Administration Server repository. Automatic distribution is disabled for this license key.

-  —The license key is stored in the Administration Server repository. Automatic distribution is enabled for this license key.

-  —Information about the currently used license key is received from a client device connected to the Administration Server. The file of this license key is stored outside of the Administration Server.

How to create and deploy an installation package including a license key

Installation packages allow you to install Kaspersky applications remotely by using the Kaspersky Security Center remote administration system. If you want to install an application on a client device, create an installation package for the application or use an existing one. You can also include a license key in the installation package, to activate the application after the installation automatically.

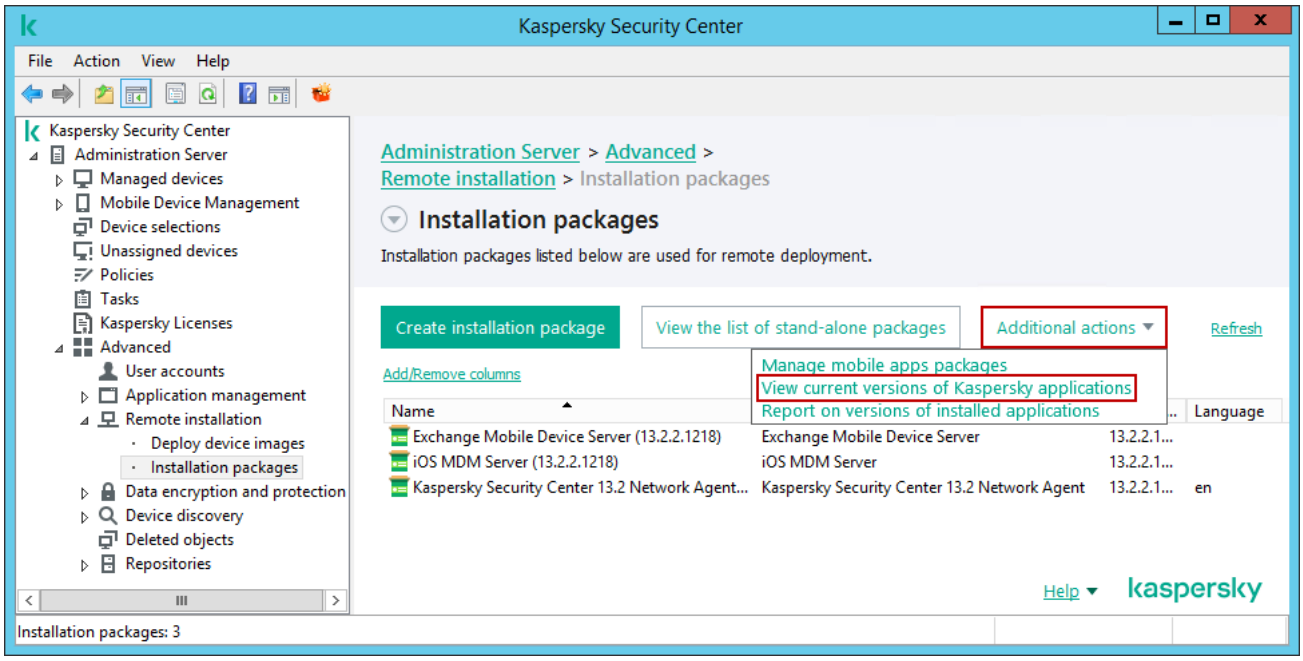
We do not recommend adding a license key to an installation package. The license key may be compromised because the shared Read access rights are enabled to the repository of installation packages.

To create an installation package including a license key:

1. In the console tree, go to **Advanced** → **Remote installation** → **Installation packages**.

2. In the **Installation packages** workspace, you can view installation packages downloaded to Kaspersky Security Center. Click the **Additional actions** button, and then from the drop-down list select **View current versions of Kaspersky applications**.

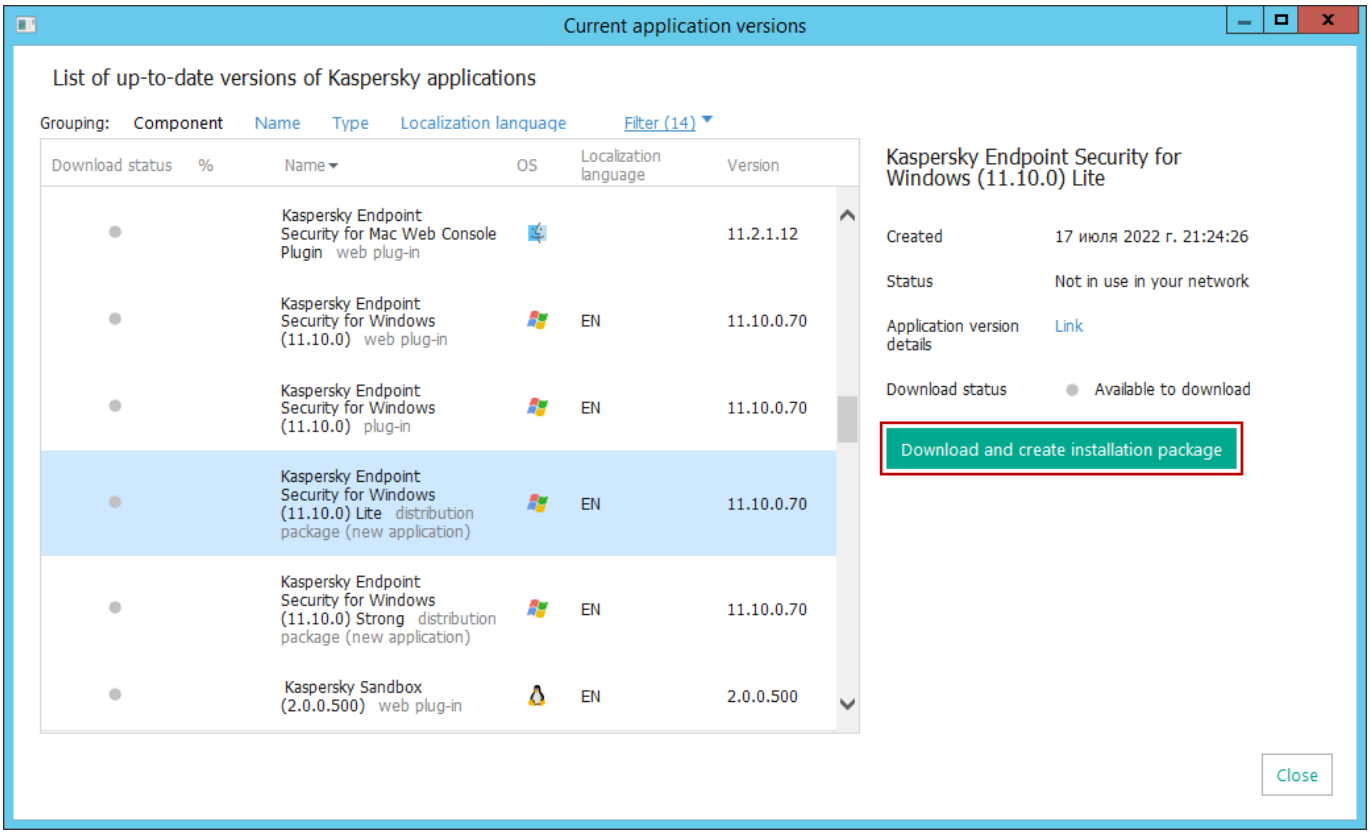
   The list of available distribution packages, plug-ins, and patches opens.



The **Installation packages** workspace

3. Select the distribution package that you want to convert to an installation package. Click the **Download and create installation package** button to download the distribution package and automatically create an installation package.

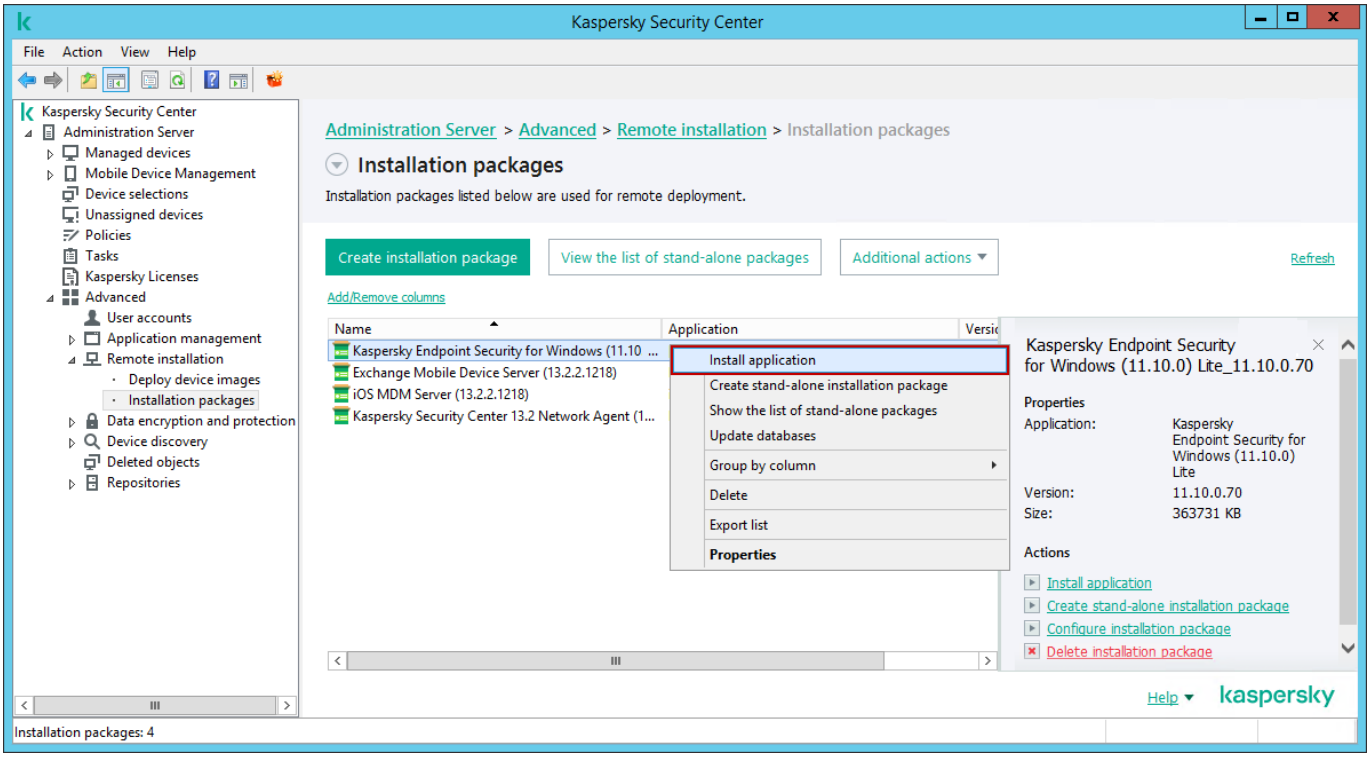
   Kaspersky Security Center saves the created installation package to the Administration Server shared folder, to the Packages subfolder. This installation package is displayed in the **Installation packages** workspace.



Creating an installation package

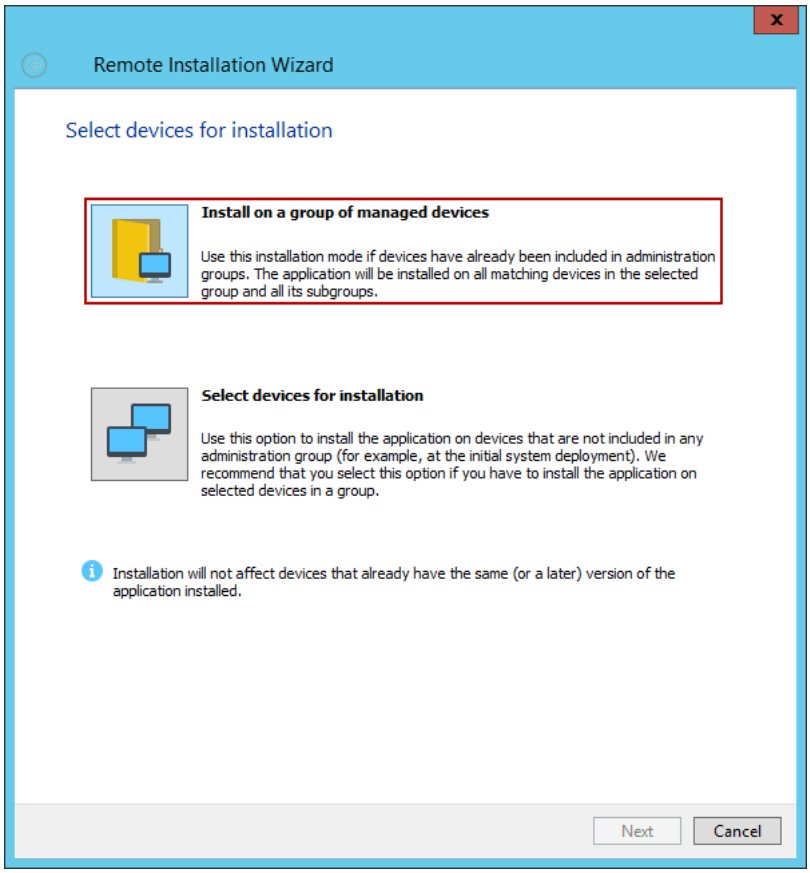
4. Right-click the installation package, and then select **Install application**.

   The Remote Installation Wizard opens.



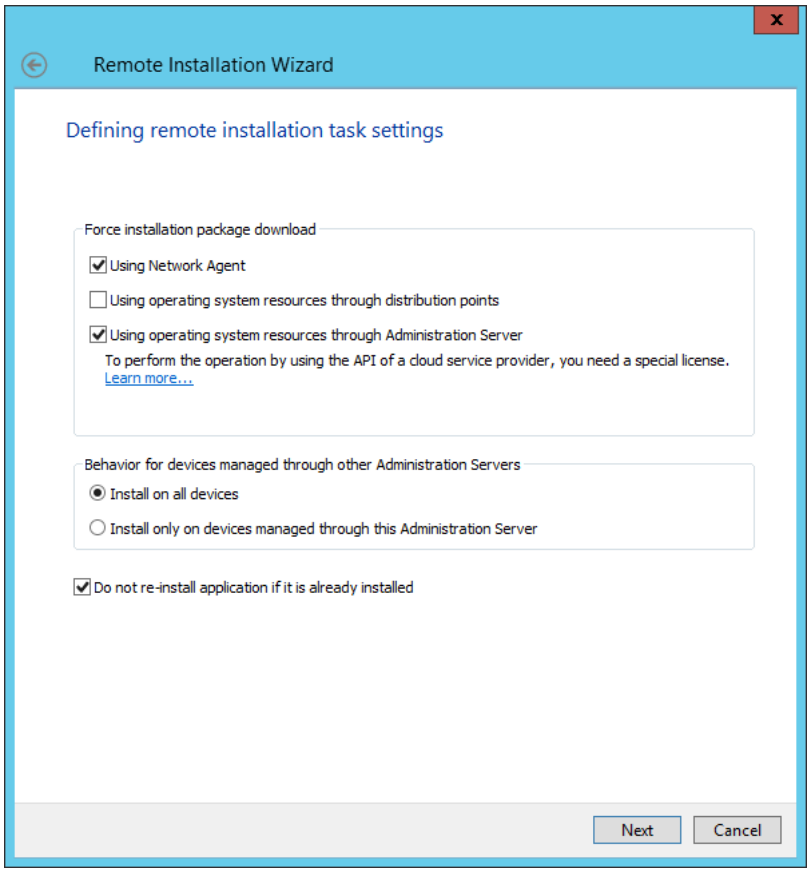
Starting the application installation

5. Click the **Install on a group of managed devices** button to specify the administration group on which to install the application.



Selecting a group of client devices for remote installation

6. In the window that opens, keep the default settings. For more information about these settings, see Installing applications using Remote Installation Wizard.

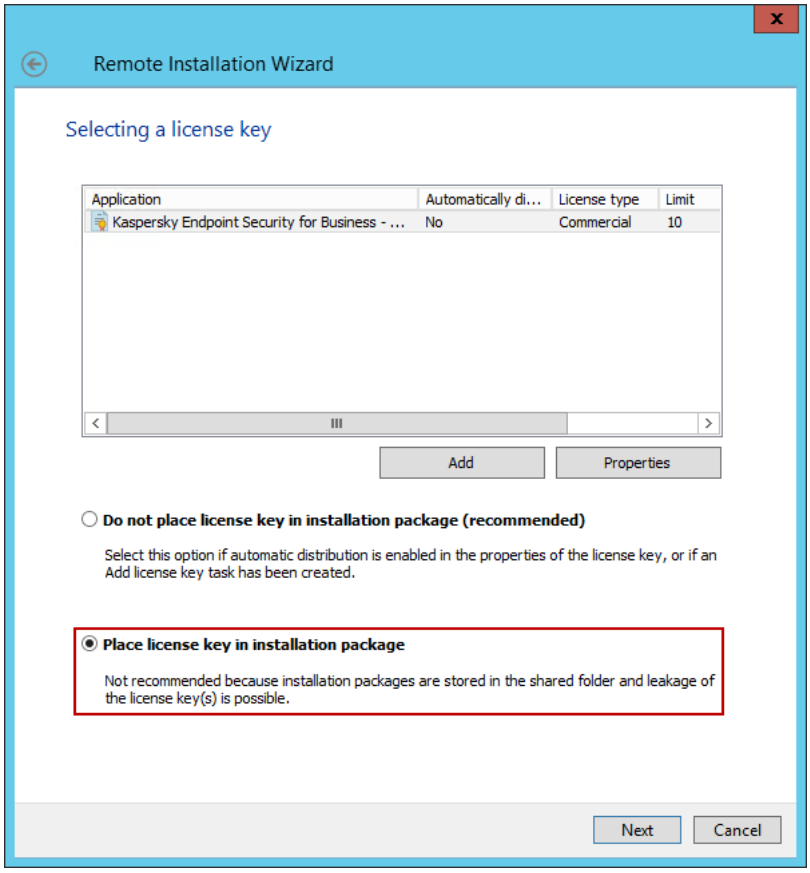


Specifying remote installation task settings

7. Select a license key that activates the application after installation.

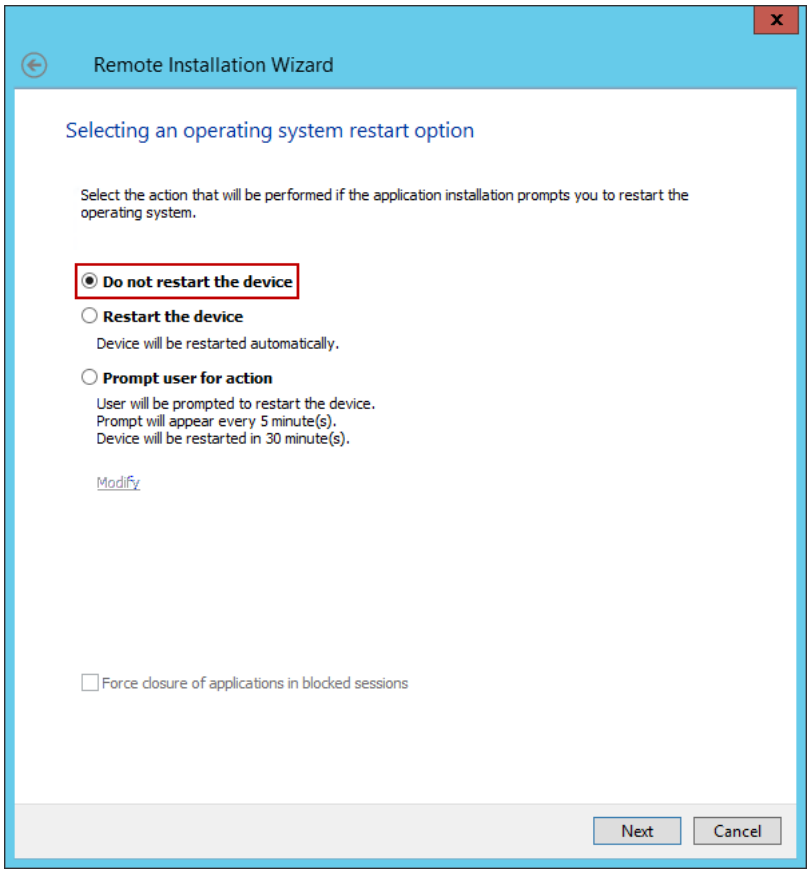
You can select a license key from the list of keys in use or add a new one. To add a new license key, click the **Add** button, and then follow the Add License Key Wizard instructions.

Choose the **Place license key in installation package** option to distribute the license key to the managed devices together with the installation package.

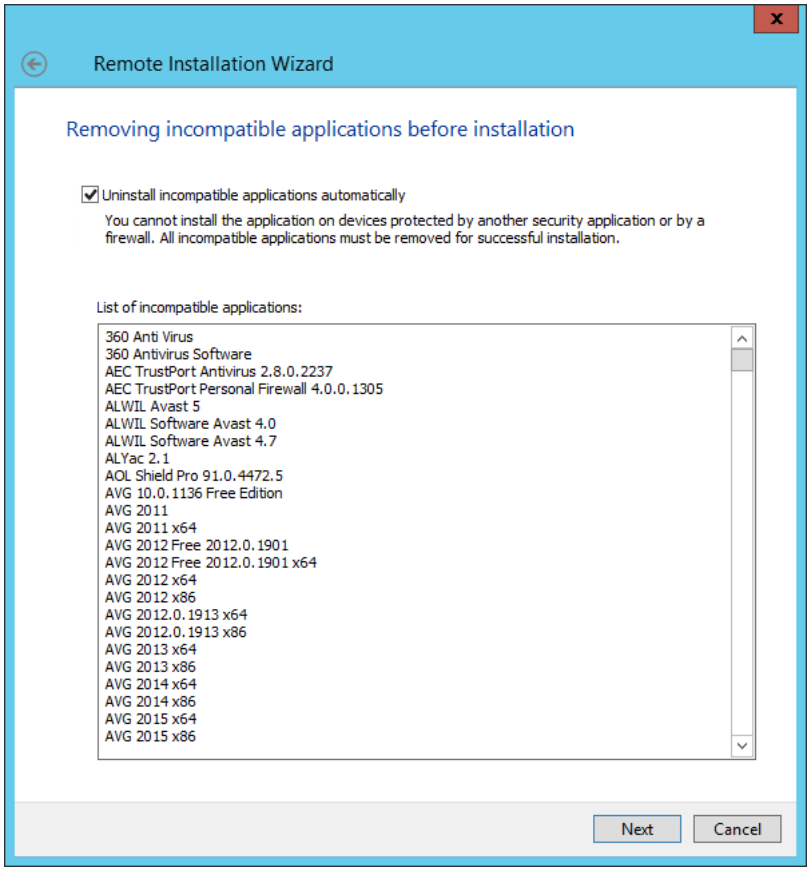


Selecting a license key

8. Select the **Do not restart the device** option in order to prevent the restart of the client devices after you install the application.



9. Select the **Uninstall incompatible applications automatically** check box to avoid installing the application on the client devices protected by another security application or firewall. For more information about the removal of incompatible applications, see Removing incompatible third-party security applications.

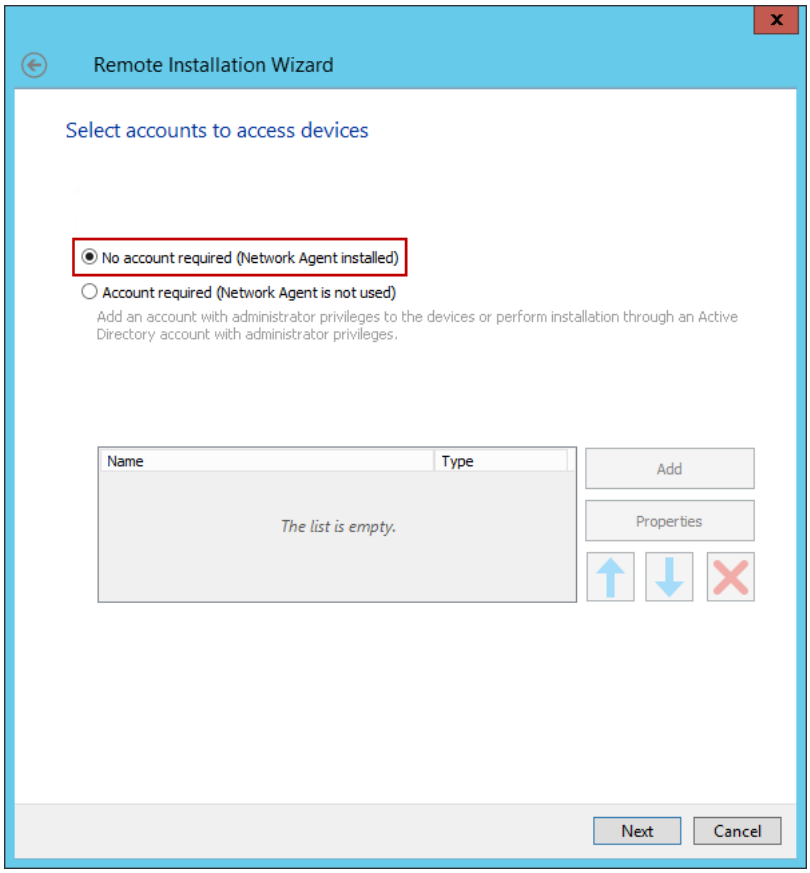


Removing incompatible applications before installation

10. Select the **No account required (Network Agent installed)** option in order to not specify the account under which Kaspersky Security Center runs the remote installation task. This task uses the account under which you run the Administration Server service.

    Note that the **No account required (Network Agent installed)** option is only available if Network Agent is installed on the client devices.

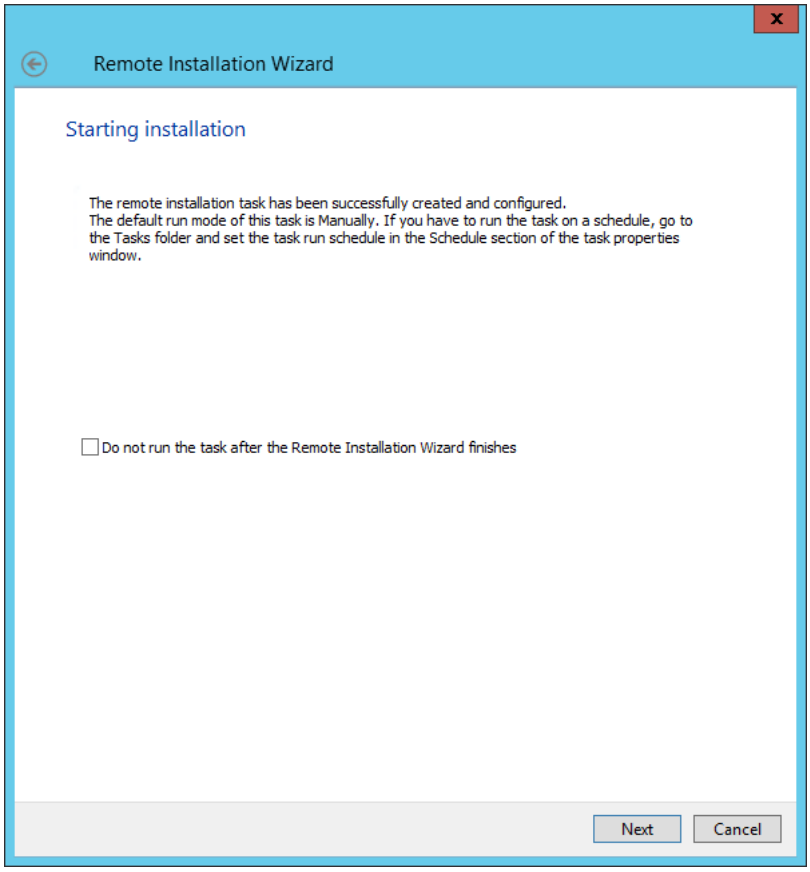
    The remote installation task is created and configured.



Selecting accounts to access devices

11. Run the remote installation task for the selected administration group. To do this, click the **Next** button.

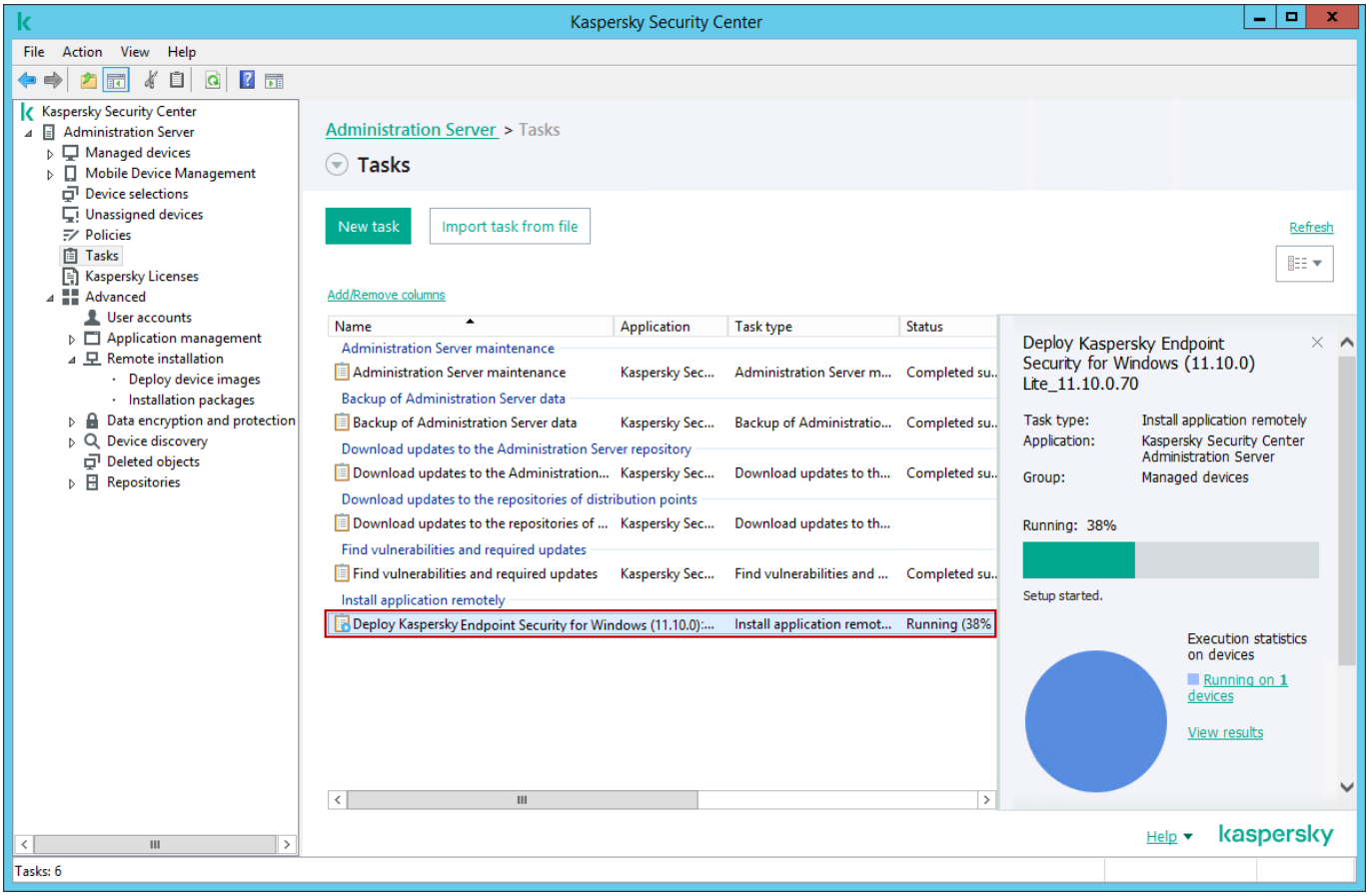
    You can select the **Do not run the task after the Remote installation wizard finishes** check box to start the task manually later.



Starting the application installation on the client devices

12. Wait until the task is started successfully, and then close the Wizard.

    The **Tasks** workspace automatically opens. Here, you can view the task progress. The task name corresponds to the name of the installation package for the application: *Deploy <Installation package name>*.



The remote installation task progress

As a result, the application installation package with a license key is created. The application is installed remotely on the specified administration group and is activated automatically after the installation.

How to upgrade the Kaspersky Endpoint Security for Business solution

If you use Kaspersky Endpoint Security for Business Select, you can upgrade it to one of the following solutions:

- Kaspersky Endpoint Security for Business Advanced
- Kaspersky Total Security for Business

After the upgrade, additional features are available, such as data encryption, adaptive anomaly control, and patch management. You can view a full list of features and study the feature comparison for every Kaspersky Endpoint Security for Business solution on a web page of any solution, for example, on the Kaspersky Endpoint Security for Business Select page.

To upgrade the Kaspersky Endpoint Security for Business solution:

1. Purchase a license for one of the following solutions, depending on which features you want to get:
   - Kaspersky Endpoint Security for Business Advanced
   - Kaspersky Total Security for Business
2. Add a license key to the Kaspersky Security Center Administration Server repository.
3. Activate the license key in the Administration Server properties.
4. Distribute the license key to your managed devices.

How to enable data encryption on managed devices

The section contains information on how to enable File Level Encryption and Full Disk Encryption in Kaspersky Endpoint Security for Windows installed on Windows-based managed devices. These types of encryption prevent the leakage of sensitive data when a corporate device is lost or stolen. If your company uses data encryption on corporate devices, an unauthorized user does not have access to encrypted files. For more information about File Level Encryption and Full Disk Encryption, see the Kaspersky Endpoint Security for Windows Help.

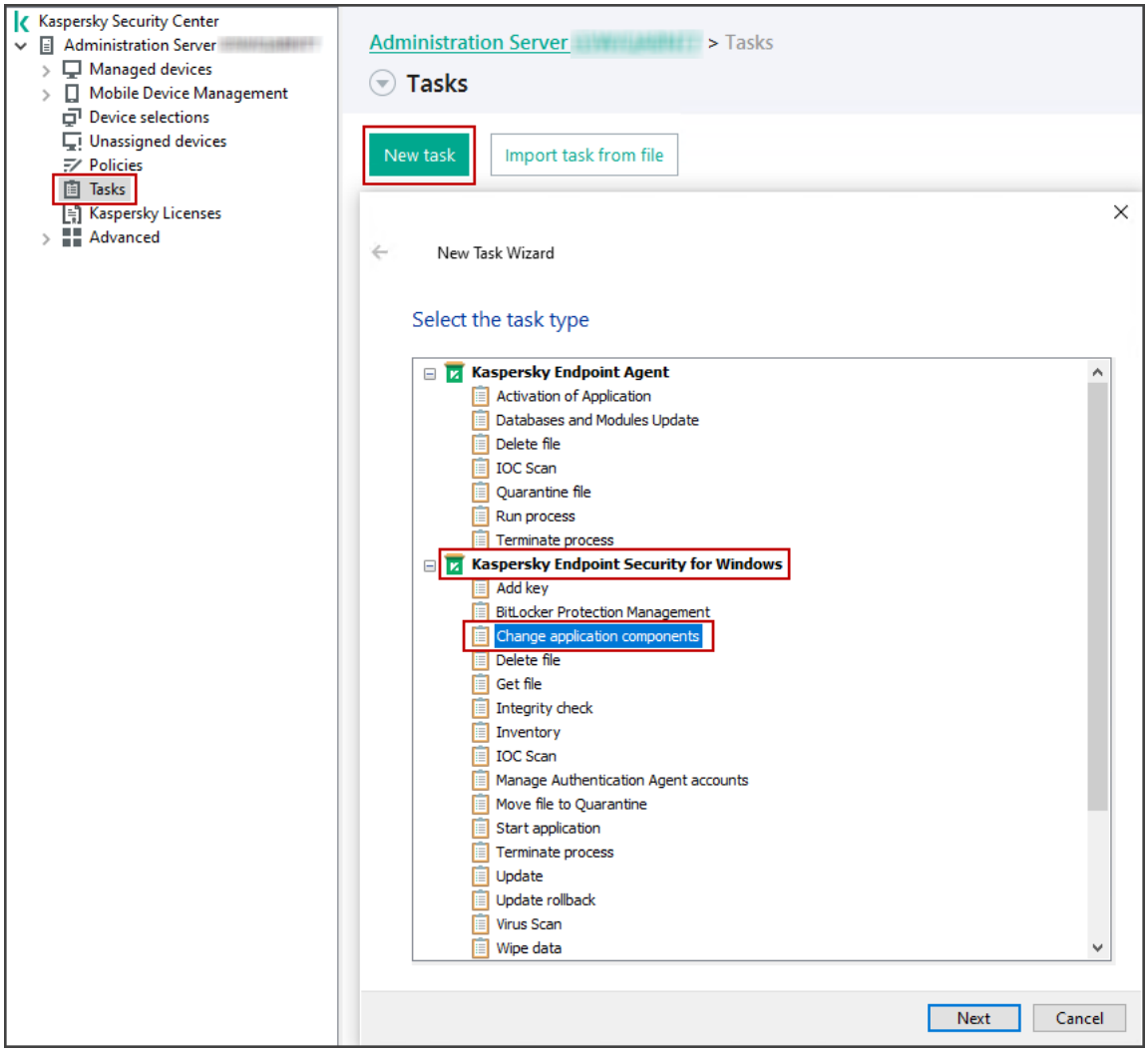
Before you enable data encryption, make sure that you have the following prerequisites met:

- You have purchased the Kaspersky Endpoint Security for Business Advanced or Kaspersky Total Security for Business license. If you use Kaspersky Endpoint Security for Business Select, upgrade it. Kaspersky Endpoint Security for Business Select does not support data encryption.
- Kaspersky Endpoint Security for Windows with Strong encryption (AES256) is installed on your managed devices. If Kaspersky Endpoint Security for Windows with Lite encryption (AES56) is installed instead, reinstall the application. To do this, create an installation package, and then run the *Install application remotely* task. Use the distribution package that includes Strong encryption (AES256).

To enable data encryption on managed devices:

1. In Kaspersky Security Center, in MMC-based Administration Console, go to the **Tasks** section.
2. Click the **New task** button.

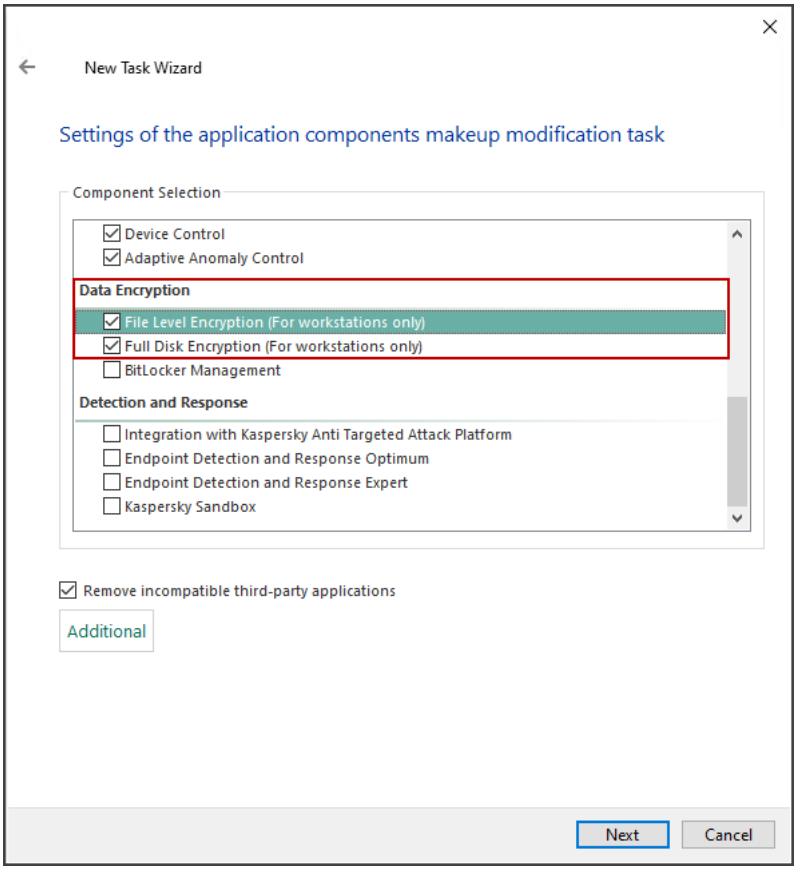
   The New Task Wizard opens.
3. Select the *Change application components* task for Kaspersky Endpoint Security for Windows.



4. In the **Data encryption** section, keep the default options enabled, and then select the following options:

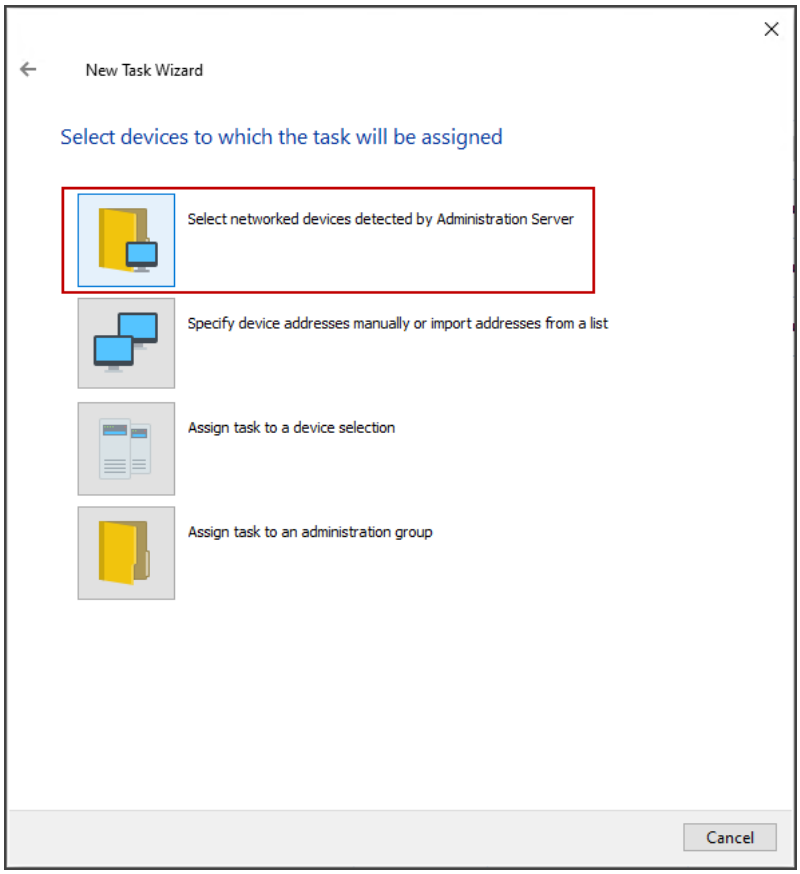
   - **File Level Encryption (For workstations only)**
   - **Full Disk Encryption (For workstations only)**

   These options define the components that are to be added to Kaspersky Endpoint Security for Windows.



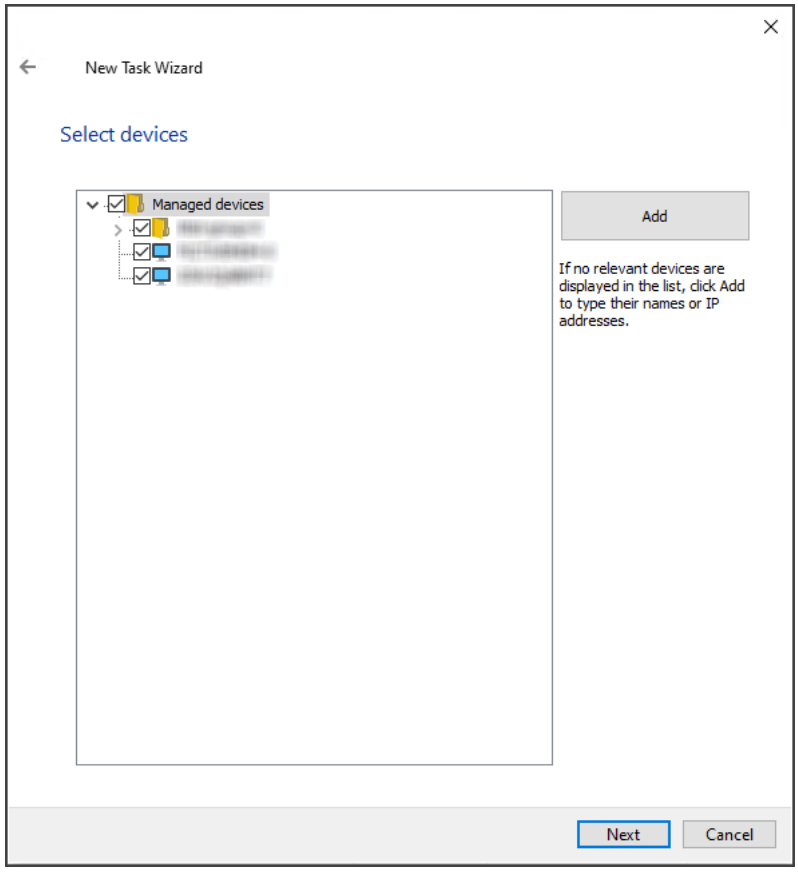
Adding the data encryption components to Kaspersky Endpoint Security for Windows

5. Click the **Select networked devices detected by Administration Server** button to specify client devices on which the new components are to be installed.



Selecting a group of client devices on which the data encryption components are to be installed

6. Select managed devices where you want to enable File Level Encryption and Full Disk Encryption. If the list does not contain the needed devices, click the **Add** button to add them to the list.



Selecting managed devices where you want to enable data encryption

7. Specify a schedule to run the task to enable data encryption:

- **Scheduled start:**

  Select the schedule according to which the task runs, and configure the selected schedule.

  - **Once**

    The task runs once, on the specified date and time.

  - **Manually**

    The task does not run automatically. You can only start it manually.

    By default, this option is selected.

  - **When new updates are downloaded to the repository**

    The task runs after updates are downloaded to the repository. You do not need to download updates to run the task for enabling data encryption, so you may select another option.

  - **On virus outbreak**

    The task runs after a *Virus outbreak* event occurs. Select the types of applications that monitor virus outbreaks from the list below:

    - Anti-virus for workstations and file servers
    - Anti-virus for perimeter defense
    - Anti-virus for mail systems

    By default, all application types are selected.

    As Kaspersky Endpoint Security for Windows is an application for workstations and file servers, you can cancel the selection of inappropriate variants.

  - **On completing another task**

    The current task starts after another task completes. You can select how the previous task should be completed (successfully or with error) to trigger the start of the current task. For example, you may want to run the *Manage devices* task with the **Turn on the device** option and, after it completes, run the task for enabling data encryption.

- **Run missed tasks**

This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If you specified the **Manually** or **Once** value in the task schedule, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

If this option is disabled, only scheduled tasks run on client devices. For the **Manually** or **Once** values in the schedule, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.

- **Use automatically randomized delay for task starts**

  If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

  The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However, when task settings are edited or the task is started manually, the calculated value of the task start time changes.

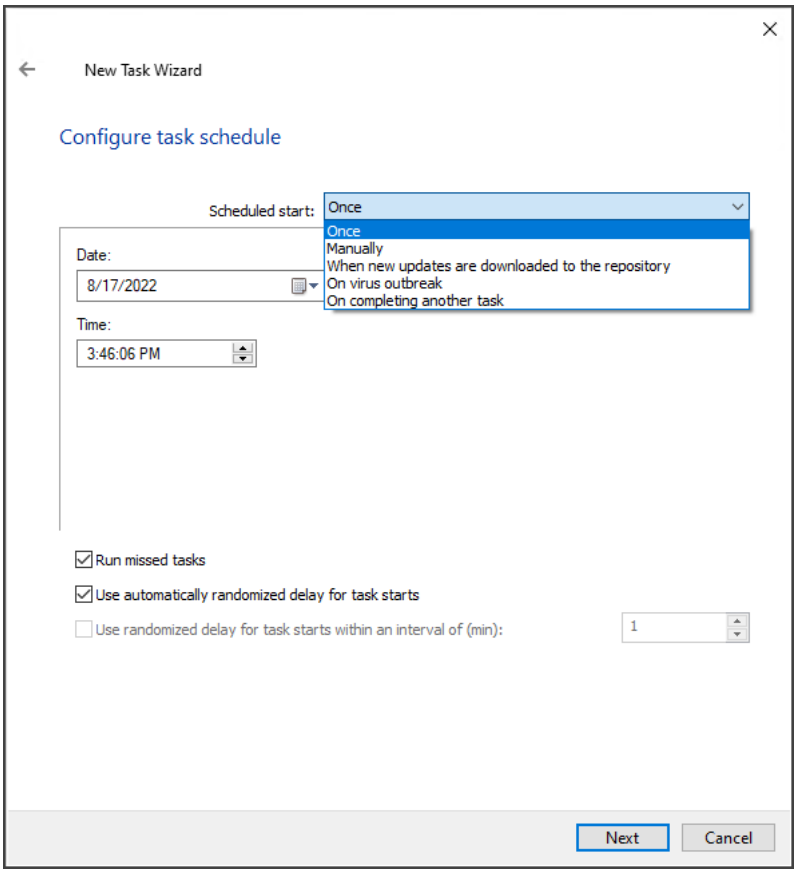
  If this option is disabled, the task starts on client devices according to the schedule.

- **Use randomized delay for task starts within an interval of (min)**

  If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

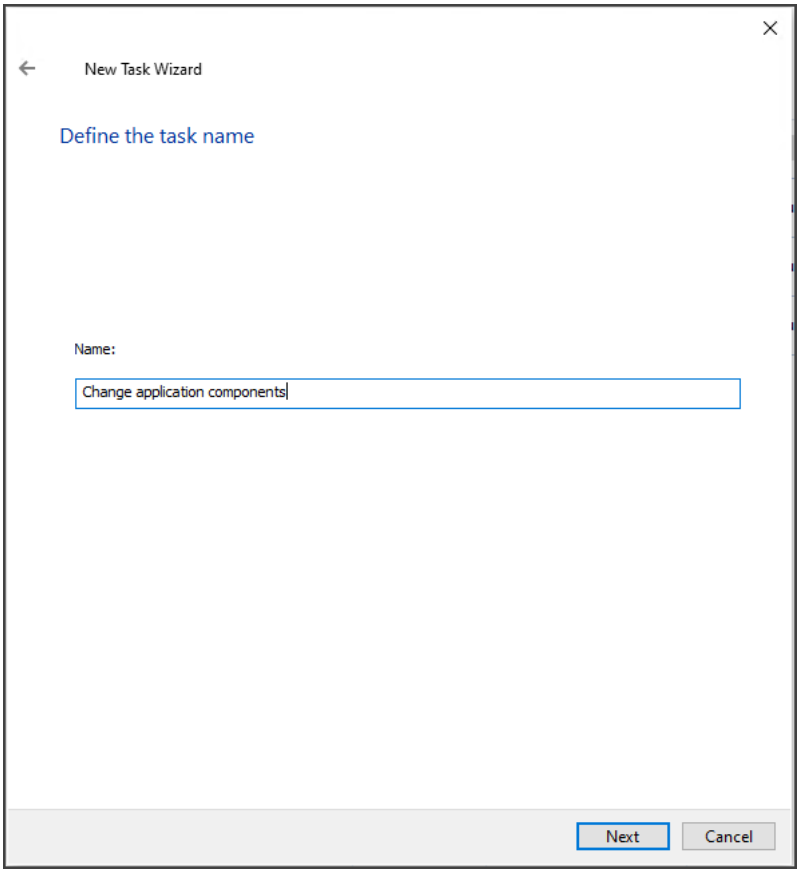
  If this option is disabled, the task starts on client devices according to the schedule.

  By default, this option is disabled. The default time interval is one minute.



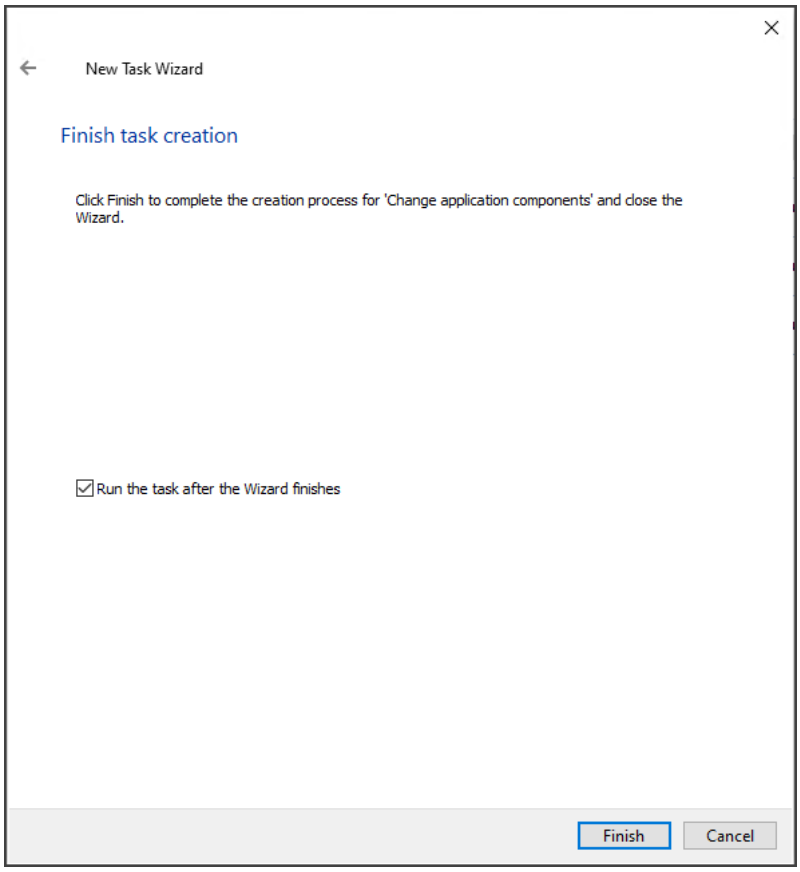
Configuring the task schedule

8. Specify the task name. You can keep the default name.



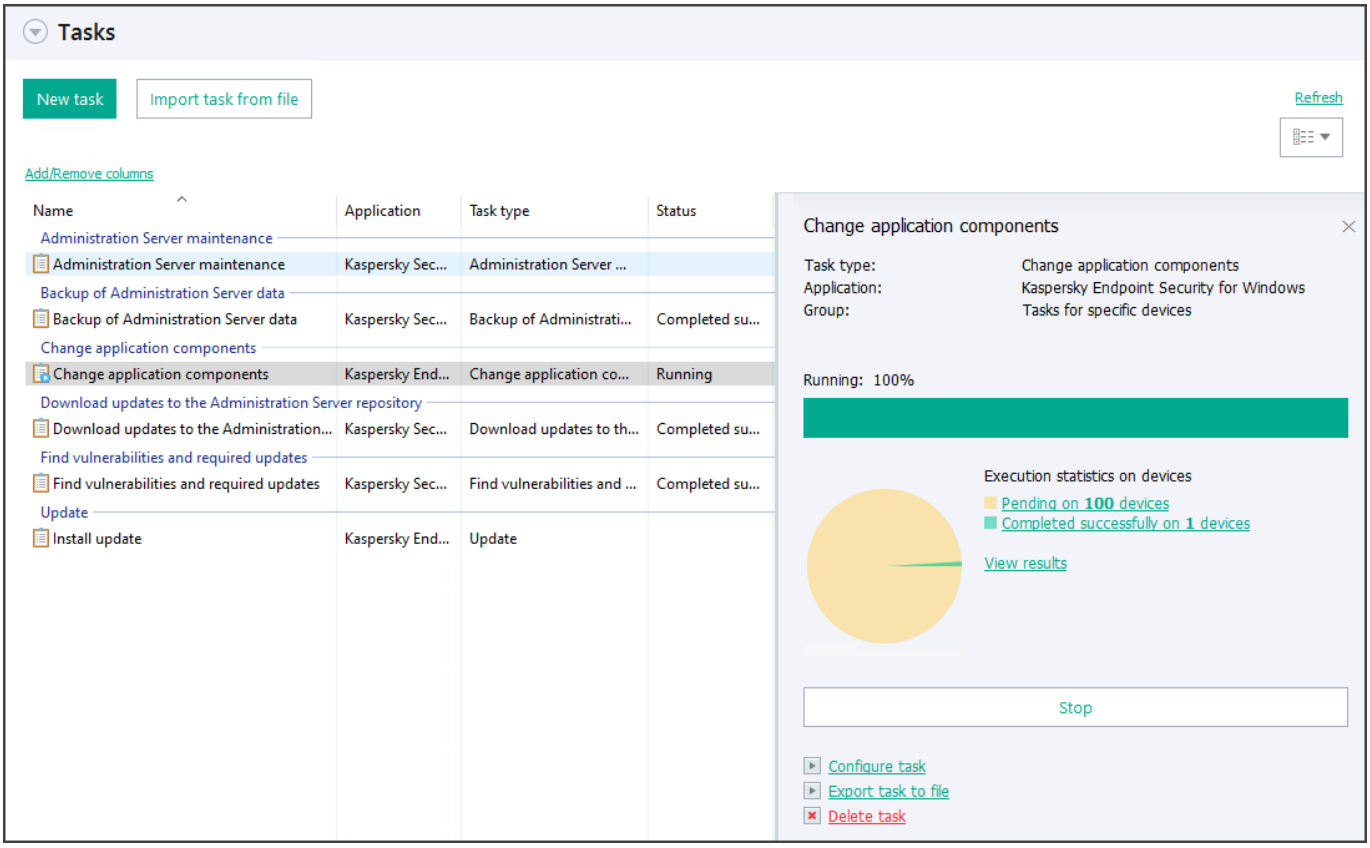
Specifying the task name

9. Select the **Run the task after the wizard finishes** option, and then finish the New Task Wizard.



Finishing the New Task Wizard and launching the created task

After you have created a task, it appears in the **Tasks** section. You can click on the task to check its status.



Checking the task status

10. When the task is completed successfully, make sure that Kaspersky Endpoint Security for Windows installed on your managed devices has the File Level Encryption and Full Disk Encryption features. To do this, view the encryption status.

As a result, you enabled the File Level Encryption and Full Disk Encryption components in Kaspersky Endpoint Security for Windows on your managed devices. Now, you can encrypt your files and start Kaspersky Disk Encryption. If you have technical problems while enabling data encryption in Kaspersky Security Center, contact technical support.

How to troubleshoot issues with connecting Network Agent to Administration Server

You can check the connection and obtain detailed information about the settings of the connection between a client device and Administration Server by using the klnagchk utility. When Network Agent is installed on a device, the klnagchk utility is automatically copied to the Network Agent installation folder.

The klnagchk utility can detect the following potential issues with connecting Network Agent to Administration Server:

- After startup, the klnagchk utility first outputs the result of connecting to the Network Agent:
  - If the connection between Administration Server and the Network Agent was established successfully, the following result is displayed:

    ```
    Starting utility 'klnagchk'...
    ...
    Attempting to connect to Administration Server...OK
    Attempting to connect to Network Agent...OK
    Network Agent is running.
    ```

  - If the klnagent service does not work or it continuously restarts, you need to reinstall the Network Agent and get traces of the installation.

    For example, if the following result is displayed, you have to reinstall the Network Agent:

    ```
    Starting utility 'klnagchk'...
    ...
    Attempting to connect to Administration Server...OK
    Attempting to connect to Network Agent...Error - Network Agent is not running.
    ```

    > You cannot always rely on information about the status of the Network Agent service from the klnagchk output. For example, if you did not enable the **Start application during installation** check box when you installed the Network Agent, the klnagchk output will not show any information about the Network Agent service. In this case, you can use the following PowerShell command:
    >
    > `Get-Service klnagent`

  - If in the `Attempting to connect to Administration Server...` line of the command output, an error about connecting to Administration Server is displayed, pay attention to the specified error text and the device connection address in the result line of sending the ICMP (the address displayed after the `An attempt to send ICMP packet to the Administration Server` line).

    Connection errors to Administration Server or a connection gateway are usually caused by the following:

    - Connecting client devices that are not included in the allowlist of IP addresses.
    - Filtering traffic on the network equipment, on the operating system firewall, or in the security applications for endpoints.
    - Problems with the client device, services, or the client device is turned off.
    - Routing network traffic is enabled.
    - Hijacking network traffic with certificate substitution (MITM attacks).

- If you have problems with network availability of the Administration Server SSL port (by default, 13000), for example, when your client device is located outside of the main network and is connected to Administration

Server through the connection gateway, you can check the availability of the port 13000 by using the telnet or akconnect tool.

If you use a firewall that decrypted the traffic between the Network Agent and Administration Server (SSL/TLS deep inspection), problems with network availability of the Administration Server SSL port may occur. In this case, switch the Administration Server port to 14000 by using the klmover utility as follows:

```
klmover -address administrationserveraddressorIP -pn 14000 -nossl
```

After that, check the availability of port 14000 by using the telnet or akconnect tool. If port 14000 is available, then using the SSL/TLS deep inspection may lead to the problems with network availability of port 13000.

- If you have an SSL connection error or timeout connection error, you can use the OpenSSL tool to check whether the TLS connection is established.

  Run the following command to check the SSL connection (TLS 1.0):

  ```
  openssl s_client -connect KSCServername:13000 -tls1 >tls1check.txt
  ```

  Example of the OpenSSL output when a problem with TLSv1 traffic occurs:

  ```
  CONNECTED(000001F4)
  write:errno=10054
  ---
  no peer certificate available
  ---
  No client certificate CA names sent
  ---
  SSL handshake has read 0 bytes and written 137 bytes
  Verification: OK
  ---
  New, (NONE), Cipher is (NONE)
  Secure Renegotiation IS NOT supported
  Compression: NONE
  Expansion: NONE
  No ALPN negotiated
  SSL-Session:
    Protocol  : TLSv1
    Cipher    : 0000
    Session-ID:
    Session-ID-ctx:
    Master-Key:
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1694581538
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
  ```

  Run the following command to check the SSL connection (TLS 1.2):

  ```
  openssl s_client -connect KSCServername:13000 -tls1_2 >tls1_2check.txt
  ```

  Example of the OpenSSL output when a problem with TLSv1.2 traffic occurs:

  ```
  CONNECTED(000001F4)
  write:errno=0
  ---
  no peer certificate available
  ---
  No client certificate CA names sent
  ---
  SSL handshake has read 0 bytes and written 227 bytes
  Verification: OK
  ---
  ```

```
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
  Protocol  : TLSv1.2
  Cipher    : 0000
  Session-ID:
  Session-ID-ctx:
  Master-Key:
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  Start Time: 1694581395
  Timeout   : 7200 (sec)
  Verify return code: 0 (ok)
  Extended master secret: no
```

For more information, refer to Troubleshooting the connection problems between the Network Agent for Windows and the Administration Server.

How to restore Administration Server data from a backup created on an earlier DBMS version

If you created a backup copy of Administration Server data when using the MariaDB DBMS of an earlier version, and then recover data on a device with a later version of MariaDB, an error may occur.

This error may occur when backing up data of Administration Server included in Kaspersky Security Center Linux 15.0 or earlier.

To restore Administration Server data from the backup made on an earlier MariaDB version:

1. Go to the backup folder that you specified when you created a backup, and then open the kavsqldb.bkp file.
2. In the kavsqldb.bkp file, remove the line `CONSTRAINT `CONSTRAINT_1` CHECK (`nPerm` is not null or `nRole` is not null)` and a comma from the previous line.

```
--
-- Table structure for table `acl_acl`
--

DROP TABLE IF EXISTS `acl_acl`;

DROP VIEW IF EXISTS `acl_acl`;
CREATE TABLE `acl_acl` (
  `nId` int(11) NOT NULL AUTO_INCREMENT,
  `nPolicy` int(11) DEFAULT NULL,
  `nObjId` int(11) DEFAULT NULL,
  `nObjType` int(11) DEFAULT NULL,
  `nUser` int(11) NOT NULL,
  `nPerm` int(11) DEFAULT NULL,
  `nRole` int(11) DEFAULT NULL,
  `bReadOnly` tinyint(1) DEFAULT NULL,
  `bInerasable` tinyint(1) DEFAULT NULL,
  `nVsId` int(11) DEFAULT NULL,
  PRIMARY KEY (`nId`),
  KEY `FK_acl_acl_pol` (`nPolicy`),
  KEY `FK_acl_acl_user` (`nUser`),
  KEY `FK_acl_acl_role` (`nRole`),
  KEY `IX_acl_acl_nObjType_nObjId` (`nObjType`,`nObjId`),
  CONSTRAINT `FK_acl_acl_pol` FOREIGN KEY (`nPolicy`) REFERENCES `pol_policy` (`policy_id`) ON DELETE CASCADE ON UPDATE CASCADE,
  CONSTRAINT `FK_acl_acl_role` FOREIGN KEY (`nRole`) REFERENCES `acl_role` (`nId`) ON DELETE CASCADE ON UPDATE CASCADE,
  CONSTRAINT `FK_acl_acl_user` FOREIGN KEY (`nUser`) REFERENCES `acl_trustee` (`nId`) ON DELETE CASCADE ON UPDATE CASCADE,
  CONSTRAINT `CONSTRAINT_1` CHECK (`nPerm` is not null or `nRole` is not null)
) ENGINE=InnoDB AUTO_INCREMENT=274 DEFAULT CHARSET=ascii COLLATE=ascii_general_ci;

--
```

3. Recover Administration Server data by using the klbackup utility.