



# **WithSecure Business Suite to Elements Migration Guide**

V2.00

# Contents

<b>1</b>	<b>Introduction to the migration of Business Suite to Elements.....</b>	<b>4</b>
1.1	System Overview .....	4
1.2	Configuration Steps.....	4
1.3	Health Check.....	4
1.4	Conclusion.....	5
<b>2</b>	<b>Preparing for the migration .....</b>	<b>6</b>
2.1	Creating licenses in the Elements portal.....	6
2.2	Upgrading Policy Manager to latest version .....	6
2.3	Verify supported operating systems.....	7
<b>3</b>	<b>Migrating Policy Manager policies into Elements profiles .....</b>	<b>9</b>
3.1	Using the profile migration tool.....	9
3.1.1	Overview .....	9
3.1.2	Running the migration tool (Windows) .....	9
3.1.3	Uploading the policy files to the Elements portal .....	10
3.2	Migrating profiles manually .....	10
3.2.1	Overview .....	10
3.2.2	Export a profile from Policy Manager .....	11
3.2.3	Importing a profile to Elements Security Center .....	13
<b>4</b>	<b>Checking and sanitating the imported profiles .....</b>	<b>14</b>
4.1	(Optional) Preparing a profile for Elements Connector .....	15
<b>5</b>	<b>Assigning profiles in Elements.....</b>	<b>16</b>
5.1	Setting default profiles by using Profile assignment rules .....	16
5.2	Setting default profile by using Active Directory groups .....	16
5.3	Setting default profile by using WithSecure MSI transformation tool.....	18
5.4	Manually assign profiles.....	20
<b>6</b>	<b>Preparing for the installation .....</b>	<b>21</b>
6.1	Allow network access to WithSecure domains .....	21
6.2	Creating a migration group in Policy Manager .....	21
<b>7</b>	<b>Migrating Windows devices .....</b>	<b>22</b>
7.1	Migrating using the Policy Manager.....	22
7.2	Migrating using the Active Directory GPO .....	23
<b>8</b>	<b>Migrating MacOS devices.....</b>	<b>24</b>
8.1	Pre-Migration Preparation .....	24
8.2	Migration Steps .....	24
8.3	Post-Migration .....	24
<b>9</b>	<b>Migrating Linux devices .....</b>	<b>25</b>
9.1	Pre-Migration Check .....	25
9.2	Migration Steps .....	25
9.3	Post-Migration .....	25

10 (Optional) Installing Elements Connector..... 26

10.1 Migrating from Policy Manager Proxy to Elements Connector .....26

11 Troubleshooting installation issues..... 27

# 1 Introduction to the migration of Business Suite to Elements

In this introductory chapter, we provide system administrators with a high-level overview of the migration process from Business Suite to Elements. This guide is tailored for those with intermediate technical proficiency and familiarity with system administration tasks. Our focus is on three critical areas: system overview, configuration steps, and health check procedures.

## 1.1 System Overview

The migration process involves moving from an on-premise Business Suite environment to the cloud-based Elements platform. This transition requires a comprehensive understanding of both environments. System administrators will engage with various components such as the Elements portal, Policy Manager, and different Elements Endpoint Protection tools.

- **Elements Portal:** Central hub for license management, profile creation, and deployment.
- **Policy Manager:** Key tool for managing security policies and client configurations in Business Suite.
- **Endpoint Protection Tools:** Set of tools for securing endpoints in the new Elements environment.

## 1.2 Configuration Steps

Configuration is a pivotal part of the migration process. This involves creating licenses in the Elements portal, upgrading the Policy Manager to the latest version, exporting and importing profiles, and creating installation packages.

1. **License Creation:** Generate necessary licenses in the Elements portal.
2. **Upgrade Policy Manager:** Ensure the latest version of Policy Manager is in use for compatibility and support.
3. **Profile Management:** Export profiles from the Business Suite and import them into the Elements Security Center.
4. **Installation Packages:** Use the Policy-based upgrade feature of the Policy Manager or Create MSI packages for deployment in the new environment.

## 1.3 Health Check

Conducting a thorough health check post-migration is crucial to ensure system integrity and performance. This involves verifying profile settings, firewall rules, and the functionality of the Elements Connector.

- **Profile Verification:** Check the imported profiles for correct settings and exclusions.
- **Firewall Rules:** Ensure that firewall rules are correctly configured and error-free.
- **Elements Connector:** Validate the setup and performance of the Elements Connector, especially in its role as a proxy for updates and security traffic.

## 1.4 Conclusion

By upgrading Business Suite to Elements, you will get the latest and most advanced version of our system, offering you a range of new features and capabilities. To upgrade your system to Elements, you need to go through a migration process that involves several steps. As a system administrator, you are responsible for ensuring that your system is ready for the migration, that your settings are configured correctly, and that your data is transferred and verified. This guide will provide you with detailed instructions and tips on how to complete each step of the migration process. By following this guide, you will be able to migrate your system smoothly and successfully.

## 2 Preparing for the migration

Please take the following steps into consideration while preparing for the migration.

### 2.1 Creating licenses in the Elements portal

Before we start migrating, we need to create the license in the Elements portal. If you are not familiar with the process, please check our help guide [here](#). To determine the number of licenses that you need, follow these steps:

1. Open the Business Suite Policy Manager (PM) and go to the "domain tree".
2. Select the "root" or any other group that represents a company.
3. Click on the tab "Installations" to see the current base of installation that you need to order for the customer.

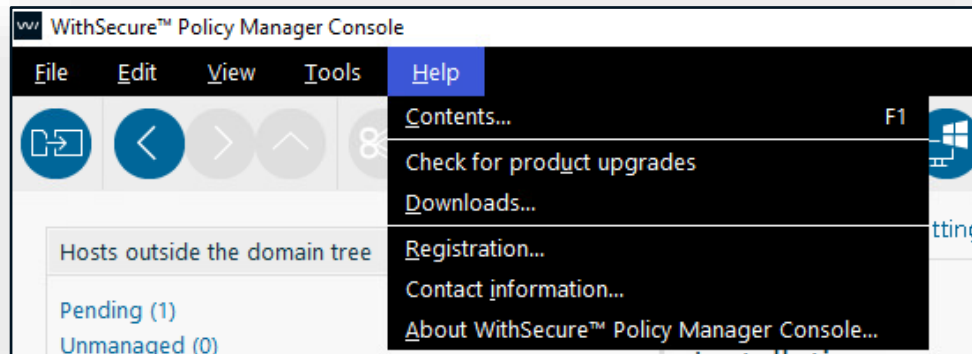
The screenshot shows the WithSecure Elements portal interface. On the left, the 'Domain tree' is visible with 'Root' selected. The main content area is titled 'Installation' and includes sections for 'Import new hosts', 'Installation packages', and 'Autodiscover Windows hosts'. A red box highlights the 'Installed products summary' table.

Product	Version	Count	Actions
WithSecure™ Client Security Premium	14.00	1	upgrade repair uninstall
WithSecure™ Client Security Premium	15.30	1	upgrade repair uninstall
WithSecure™ Client Security Premium	16.00	2	repair uninstall
<b>WithSecure™ Client Security Premium</b>	<b>Total</b>	<b>4</b>	
WithSecure™ Atlant for Offload Scanning Server	1.00	2	
<b>WithSecure™ Atlant for Offload Scanning Server</b>	<b>Total</b>	<b>2</b>	
WithSecure™ Policy Manager Proxy	15.30	1	
<b>WithSecure™ Policy Manager Proxy</b>	<b>Total</b>	<b>1</b>	
WithSecure™ Email and Server Security Premium	15.00	1	upgrade uninstall
<b>WithSecure™ Email and Server Security Premium</b>	<b>Total</b>	<b>1</b>	
WithSecure™ Server Security Premium	15.30	2	upgrade repair uninstall
WithSecure™ Server Security Premium	16.00	1	repair uninstall
<b>WithSecure™ Server Security Premium</b>	<b>Total</b>	<b>3</b>	
WithSecure™ Scanning and Reputation Server	12.20	1	
<b>WithSecure™ Scanning and Reputation Server</b>	<b>Total</b>	<b>1</b>	

### 2.2 Upgrading Policy Manager to latest version

To ensure a smooth migration, you need to run the latest version of PM. This needs to be done for the best support of profile migration from Business Suite. You can check your current version by following these steps:

1. Open the PM and go to "Help > About WithSecure Policy Manager Console".



2. Compare your version number with the latest version available on the support and download website:  
<https://www.withsecure.com/en/support/product-support/business-suite/policy-manager#download>
3. If your version is older, please upgrade to the latest version before continuing.



Note: In version 16.xx you are not able to upgrade/update the management console only. Instead, you must upgrade the entire Policy Manager Server.

## 2.3 Verify supported operating systems

Before starting the migration process, make sure that all devices have a supported operating system. For example, Windows Vista, Windows 7 or Windows Server 2008 are not supported and

should not be used for migration. WithSecure only supports the operating systems that are still supported by their vendors.

You can find the system requirements for WithSecure products below:

- WithSecure Policy Manager: [Policy Manager Server | Policy Manager | 16.00 | WithSecure User Guides](#)
- WithSecure Client Security: [System requirements | Client Security for Windows | 16.00 | WithSecure User Guides](#)
- WithSecure Server Security: [System requirements | Server Security | 16.00 | WithSecure User Guides](#)
- WithSecure Elements Endpoint Protection for Computers: [System requirements | Elements Endpoint Protection for Computers | Latest | WithSecure User Guides](#)
- WithSecure Elements Endpoint Protection for Servers: [System requirements | Elements Endpoint Protection for Servers | Latest | WithSecure User Guides](#)



## 3 Migrating Policy Manager policies into Elements profiles

There are two different ways to migrate Policy Manager policies into Elements profiles:

1. Using the profile migration tool (see 3.1)
2. Migrating profiles manually (see 3.2)

Depending on your environment and needs, you can choose one or the combination of both.

### 3.1 Using the profile migration tool

#### 3.1.1 Overview

The migration tool is available in the WithSecure Elements portal:

<https://elements.withsecure.com/apps/bs2e/dashboard>

Please visit this link for a tutorial:

<https://withsecure.navattic.com/8430tlc>

This wizard helps you to migrate some data from Policy Manager to Elements Security Center. You can use it to import policy settings and convert them into Elements profiles. However, it does not create subscriptions, devices, or profile assignment rules.

Before importing data to Elements Security Center use a migration tool to export the data from Policy Manager:

- [Download for Windows](#)
- [Download for Linux](#)

Keep these points in mind before importing a profile:

- Make sure that you import all migration files. Otherwise, you might lose some settings in child profiles.
- If your migration file has settings for different profile types (Windows, Windows Server, Linux Server, Mac), you can clone the imported profile and then change the type of the cloned profile.
- Always publish a profile with the expected profile type. Change it if necessary.

#### 3.1.2 Running the migration tool (Windows)

1. Download the **migration-tool-1.00.98727.zip** from the link above and extract it to your preferred location (e.g. desktop)
2. Run the command prompt (cmd) as an administrator
3. Locate the migration file **pms-to-elements-migration-tool.bat** in the extracted folder (migration-tool-1.00.98727\migration-tool\bin\)

4. Use the command **net stop wspms** to stop the WithSecure Policy Manager service. “**The WithSecure Policy Manager service was stopped successfully**” should be shown.
5. Run the **pms-to-elements-migration-tool.bat** file in the command prompt to extract policy settings from the Policy Manager
6. Use the command **net start wspms** to start the WithSecure Policy Manager service.
7. By default, the policy settings will be extracted to **migration-tool-1.00.98727\migration-tool\WS-PM-Migration** as .json files. The tool is able to find the Policy Manager installation location and extract the data automatically.

### 3.1.3 Uploading the policy files to the Elements portal

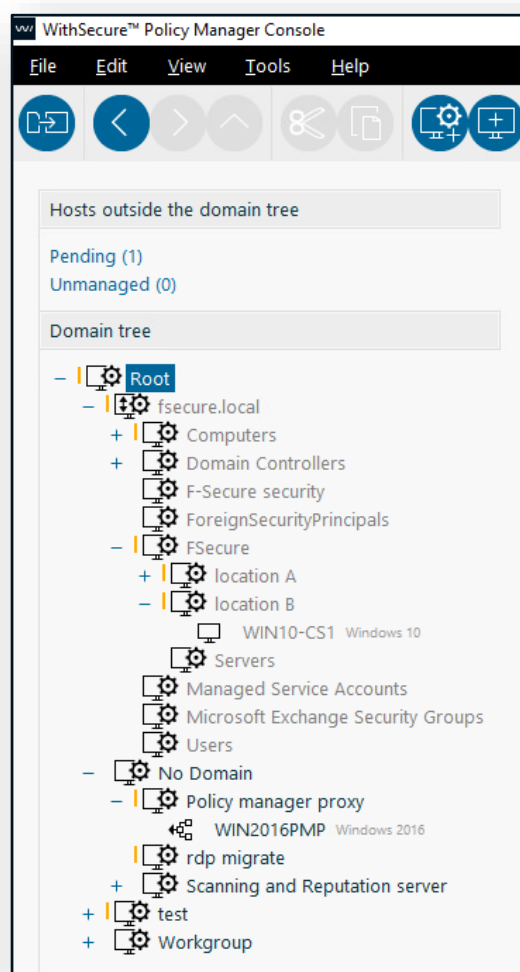
Now that the Policy Manager policy files have been extracted, the next step is to upload those to the Elements portal and to create new profiles.

1. Open the Migration from Policy Manager menu in Elements portal:  
<https://elements.withsecure.com/apps/bs2e/dashboard>
2. The .json files can be uploaded by using the **Browse...** button or drag-and-dropping.  
TIP: **Select profile type for uploaded files** option can be ignored at this stage unless all the imported profiles are the same type. The profile type can be changed one-by-one at the next stage.
3. Click **Upload profiles** to start the upload process
4. After uploading the status column might show red icon for some profiles. This happens if there is an existing profile with the same name as the imported one. In that case, consider renaming or removing.
5. Change the device types accordingly by clicking three dots (...) and **Change profile type**.
6. Click **Publish profiles**
7. Wait for the profiles to be published. In case of any errors, the status column will show a red icon. Click on the icon for more details.
8. After all profiles have been published, click on the “**Go to profiles review**” button to review newly published profiles.

## 3.2 Migrating profiles manually

### 3.2.1 Overview

Before you export profiles, you need to choose which ones you want to export. You only need to export the profiles that are different from the default Root profile. These profiles have an orange stripe 🟡 before the group or device name in the Domain tree. Note, that you can only export profiles at the device level, so if a group has an orange stripe but the underlying device not, you need to select the underlying device for exporting. This means that the profile is the same for all the devices in the entire group.



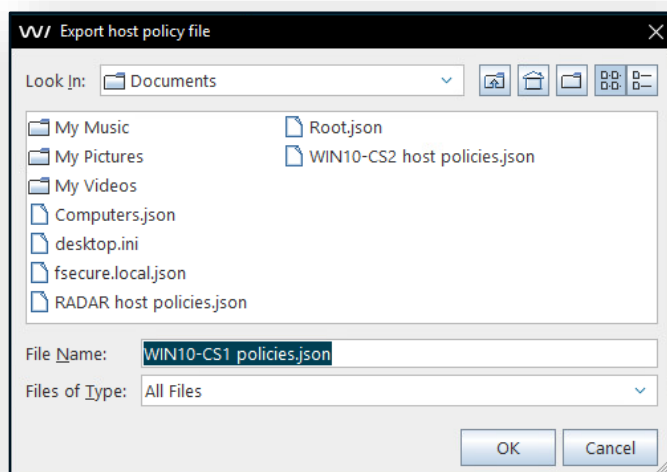
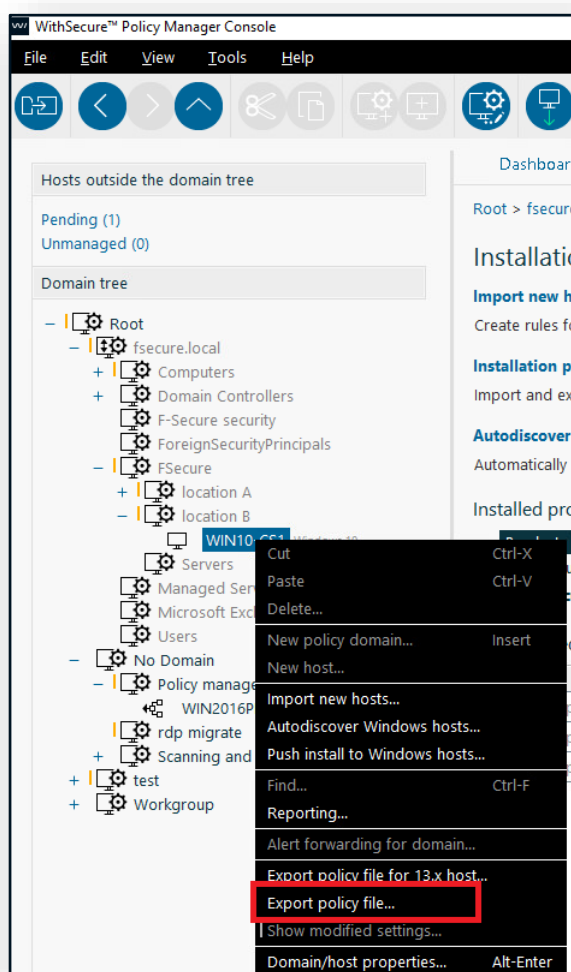
You should also verify if the profiles that are different (the ones with the orange stripe before them) need to be exported. Some of them may be the same as the others, but only missing a lock on an option. For that alone, it is not recommended to export the profile.

### 3.2.2 Export a profile from Policy Manager

To export a profile, follow these steps:

1. Right-click a device in the Policy Manager Console domain tree.
2. Select Export policy file.
3. Save the file as a JSON file with a descriptive name in a location that you can easily find later.

**Note:** exporting a policy also exports firewall rules into the exported JSON file.



### 3.2.3 Importing a profile to Elements Security Center

To import a profile, follow these steps:

1. Log in to the Elements Security Center and navigate to the Profile tab.
2. Click “Create a profile” and enter a name, type, and description for the profile.
3. Click the three dots icon and select “Import profile”. Choose the exported JSON file that you want to import.
4. Click “Save and publish” to apply the profile.
5. Click the three dots icon again and select “Lock all settings” to prevent end-users from making changes to the profile.
6. Click Save and publish again.

## 4 Checking and sanitating the imported profiles

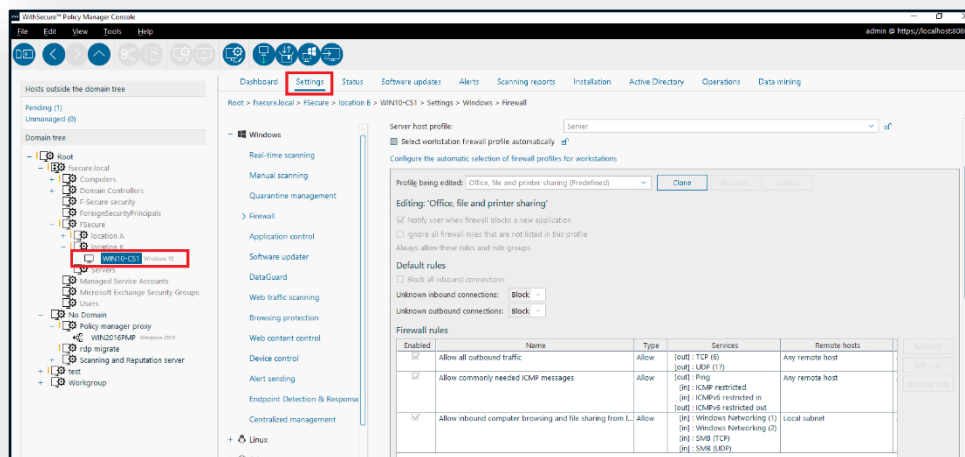
It is very important that the administrator checks the settings imported carefully before deploying them. While every care is taken during the import to merge the settings, it is the administrator's responsibility to check this.

It is suggested to cross-check settings in the Policy Manager and the migrated profiles in the Elements portal. Here are some things to check:

- Check that the exclusions are written in the supported way. In the old version of the product (PM version 12.xx), you needed to use \\ for exclusions with wild cards, but in the new version, you only need one (\). You can find more information about this from the following page: [Using wildcards in exclusions in real-time scanning - WithSecure Community](#)
- Check the firewall rules in the profile. Some rules can create errors, and it will prevent you from saving the profile. A firewall setting that is not written in a correct way will have a red mark in front of the rule.

Original firewall rules can be checked in the Policy Manager:

Policy Manager Console > Choose the profile from the Domain Tree > Click Settings > Firewall



Note, that while migrating Business Suite policies to Elements, it is also recommended to review all the profile settings that have been migrated and remove any unnecessary ones.

Also, it is recommended to go through all the imported profiles in the Elements Security Center after the profiles has been imported. This is to make sure that everything has been formatted correctly and the configurations are correct.

## 4.1 (Optional) Preparing a profile for Elements Connector

If you are planning to use Elements Connector, you should also check the Connector profile. Elements Connector can act as a proxy for all the updates and security cloud traffic, as well as SWUP updates. You can also use Elements Connector to send Security Events to your SIEM system.

To create a custom Connector profile, you can follow these steps:

1. Clone the default Elements Connector profile and give it a custom name.
2. Configure the address settings according to your environment.
3. Save the profile

For installation instructions, please refer to the **Installing Elements Connector (optional)** chapter.

## 5 Assigning profiles in Elements

The recommended way to assign profiles is to use profile assignment rules in the portal. The profile assignment rules replace the default profiles. They are automatically applied to new devices that are added to the system and executed in the order that they appear in the table from top to bottom. The first rule that matches is applied to new devices. If there is no matching rule, the default rule is applied.

**Custom and default rules** are automatically applied when a new device is installed. Turn on the toggle to evaluate rules whenever device data changes.

**Outbreak rules** do not apply to new installations. These rules are only evaluated for existing devices.

The outbreak rules are always at the top of the table.

Profile assignment rules are executed in the order they are placed (until first matching rule), default rules are executed if there is no matching rule.

Drag and drop the row with rule to change position.

The complete instructions can be found from the link below:

[Adding profile assignment rules | Elements Endpoint Protection | Latest | WithSecure User Guides](#)

### 5.1 Setting default profiles by using Profile assignment rules

You can assign different profiles to different client types in the Elements EPP portal. For example, you can assign a profile that enables certain features or restricts access to certain data for a client type. To assign different profiles to different client types, follow these steps:

1. Open the **Profiles** tab and select **Profile assignment rules**.
2. You will see a list of all the client types and their assigned profiles.
3. To change the assigned profile for a client type, click on the **action button** (...) next to the client type name and select **Edit**.
4. A window will pop up with a drop-down menu of all the available profiles for that client type.
5. Select the profile that you want to assign to that client type and click on the **Save** button.
6. The window will close and the assigned profile for that client type will be updated. You can repeat this process for any other client type that you want to change.

### 5.2 Setting default profile by using Active Directory groups

1. Click on the "Add rule" button to create a profile assignment rule based on Active Directory.
2. On the right side of the portal screen, you see the popup screen "Add rule" now select in the dropdown menu "Condition" the option "Active Directory OU Manual" or "Active Directory OU Tree".
3. When you have selected:



- a. Active Directory OU Manual then go to the field “Value” and enter here the OU where your new profile needs to be assigned.

**Active Directory OU Manual**

Value for AD field can be any Active Directory Organizational Unit, either in distinguished name or slash separated format. Wildcards may also be used in either format to match any child groups. Examples of valid AD values:

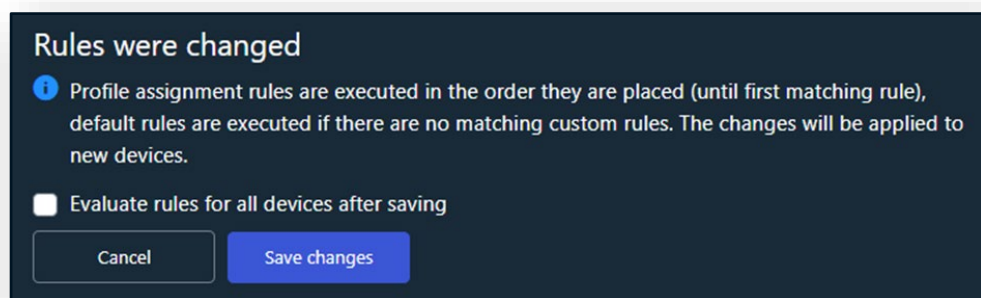
- Example 1: OU=Servers,DC=FI,DC=com
- Example 2: OU=Servers\*,DC=FI,DC=com
- Example 3: com/FI/Servers\*

- b. Active Directory OU Tree then go to the drop-down menu “Value” and select here your AD path.

**Active Directory OU Tree**

Value for AD field can be any Active Directory Organization Unit collected by the WithSecure agents in your network(s). It will show this in the drop-down menu.

4. Select your client type in the drop-down menu “Client type”
5. Select the profile you want to use in the drop-down menu “Assign profile”. (Only the profiles are showed that belongs to the Client type.)
6. (Optional) You can also assign labels to devices to identify them easier in the “Device” overview.
7. (Optional) You can enter in the Description field any notes that could be handy to explain the rule or give more information about the rule.
8. Click on the “Save” button.
9. Now you get the screen “Rules were changed” and you have now the option to save changes with or without checking the checkbox option for “Evaluate rules for all devices after saving”. If checkbox is enabled our product will evaluate all devices in your portal and assign the correct profile based on your profile assignment rule. If you don’t check the checkbox the rule will only apply to new devices.



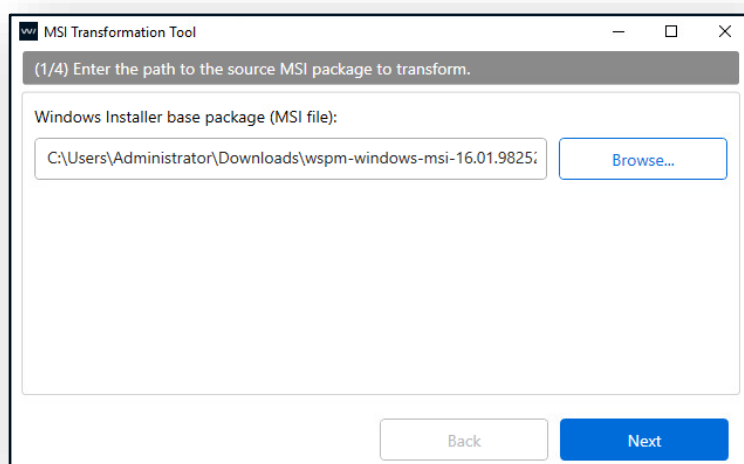
10. (Optional) You can also enable the option Change tracking that is above the rule table that will track any changes.



Change tracking: Continuously evaluate rules for the devices, and change the profile and label assignments for each device when changes in the Active Directory Organizational Unit, IP, reverse DNS, or WINS name are detected or when there are new open EDR or on public internet incidents on the device. This toggle must be turned on for the outbreak rules to be active.

## 5.3 Setting default profile by using WithSecure MSI transformation tool

1. Download the WithSecure MSI Transformation tool (FsMsiTool.exe) here: [https://download.withsecure.com/msitool/FsMsiTool\\_ui.exe](https://download.withsecure.com/msitool/FsMsiTool_ui.exe)
2. Run the tool. After you have run the tool, a wizard opens.
3. On the first page, specify the path to the source MSI package, and select Next.



4. On the next page, specify PROFILE\_ID (that can be found when you open the needed profile) and or more MSI properties, and select Next.

Profile For Windows Computers  
B. A. T. (Boer Alle Technieken)

Assigned computers: 0  
Last edited: 10/17/23 11:08 AM  
Profile ID: 229503486

Profile name: test  
Description:   
Type:

General settings  
This tab contains settings that are shared by all security features in WithSecure™ Elements Agent

Search: Type here to search for a specific setting...

General settings  
Early access to client software ☐  
Show user interface to clients ☐  
Automatic updates ☒  
Use HTTP proxy ☐ From users browser settings  
Manually defined proxy address

Done

MSI Transformation Tool

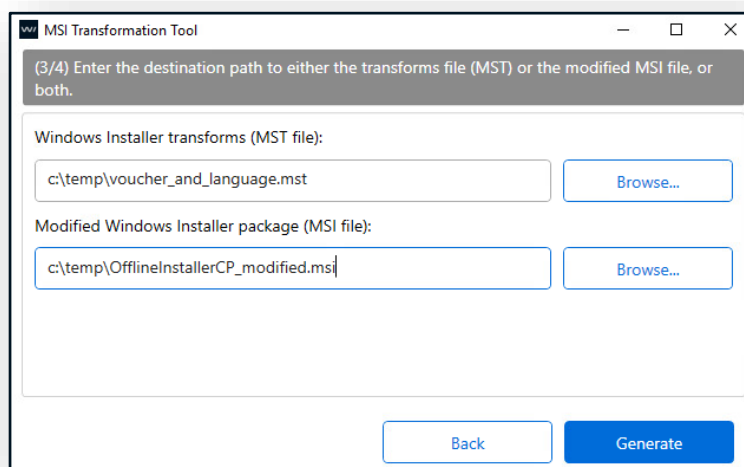
(2/4) Enter MSI properties to add or update in the source MSI file.

PROFILE\_ID 229503486 Add

MSI Property Name MSI Property Value Remove

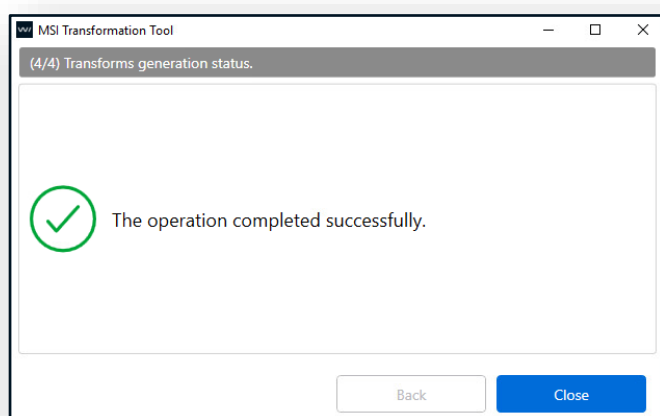
Back Next

- On the third page, specify the output .mst file or .msi package path. You can specify only one or both paths.



**Note:** Embedding the properties into the MSI package simplifies the installation, but it invalidates the digital signature. If you want to preserve the digital signature, use the MST file.

6. Select *Generate* to generate the output files.



## 5.4 Manually assign profiles

1. Under Devices, select the devices that you want to assign a profile.
2. At the bottom of the page, select Assign > Assign profile.
3. From the drop-down menu, select the profile that you want to use.
4. Select Assign.

## 6 Preparing for the installation

### 6.1 Allow network access to WithSecure domains

For most customers, WithSecure Elements products will function correctly without needing to know which servers the products connect to. However, some administrators tightly control which network addresses they allow their clients to connect.

WithSecure recommends, where possible, that administrators allow outbound access to all address under the **withsecure.com** and **fsapi.com** domains.

WithSecure cannot guarantee the functionality of the products if access to these addresses is blocked.

For more detailed information, please visit:

[Network addresses for WithSecure Elements \(cloud-managed products\) - WithSecure Community](#)

### 6.2 Creating a migration group in Policy Manager

It is recommended to first create a migration group in Policy Manager, so that the migration process can be done in more controlled and phased manner. This can be achieved by creating a group in Policy Manager and cut-and-pasting selected clients into that group, which will then be migrated.

Please follow the following steps:

1. Create a new policy domain and give it a name – Elements Migration, for example
2. Select the devices that will be piloted for migration and copy-paste them into the migration group
3. Continue with the installation for the “pilot” group (see the next chapter)

After the migration has been completed successfully for the pilot group, you can start creating more groups, adding client into those groups and continuing with the migration process.

Once the client has been installed in the Elements Portal, it can be removed from the Policy Manager as it doesn't reply status anymore into the Policy Manager server.

## 7 Migrating Windows devices

There are several ways to install the product, depending on your preferences and environment.

You can find all the supported deployment methods on the following page:

[Common deployment methods | Elements Endpoint Protection | Latest | WithSecure User Guides](#).

You can choose the one that suits your needs and environment best.

### 7.1 Migrating using the Policy Manager


**You can use the Policy Manager to upgrade the current clients.** This is a convenient way to manage the installation from a central console. You can find more details on how to do this on [Migrating computers | Elements Endpoint Protection | Latest | WithSecure User Guides](#)

To apply the **.jar** file and migrate, you need a Policy Manager console and the **.jar** file that you can download from the following link: <https://download.withsecure.com/PSB/bs2cp/bs2elements.jar>.

To migrate:

1. Open the Policy Manager console and select the group of computers that you want to migrate.
2. Select the **Installation** tab.  
The **Installation** page opens.
3. Under Policy-based installation, select **Install....**  
The **Choose installation package** window opens.
4. Select **Import...** to import the installation packages.  
The available **.jar** file is shown.
5. Select the **.jar** file, and then select **Import**.  
Policy Manager imports the **.jar** file and shows the package details.
6. Select **OK** to apply the **.jar** file.
7. In the **Installation options** window that opens, do the following:
  - a. Enter a valid subscription key.
  - b. Select the installation language, and then select **Finish**.

**Note:** Do not distribute the installation packages yet. At this point, it is recommended to distribute the migration file only to the migration “pilot” group that has been created earlier to catch any issues that may occur during the installation process.

8. In the **Installation window**, select the  icon at the top-left corner to distribute the policies to the selected computers.  
The selected computers are migrated, and the policies are distributed to them.

Note: The selected computers may have to be restarted to complete the installation.

## 7.2 Migrating using the Active Directory GPO

You can use the Active Directory to upgrade the current clients. This is a useful way to deploy the product to a large number of devices in a domain. You can find more instructions on how to do this on [Deployment via Active Directory GPO | Elements Endpoint Protection | Latest | WithSecure User Guides](#)

- You can use the WithSecure MSI transformation tool to create a MSI file that contains the necessary information for the installation. This is a handy way to customize the installation settings and parameters. You can find more information on how to use this tool on [Using the WithSecure MSI transformation tool | Elements Endpoint Protection | Latest | WithSecure User Guides](#)

## 8 Migrating MacOS devices

This guide provides a clear step-by-step process for migrating from Business Suite's Client Security for Mac to Elements Mac Protection.

### 8.1 Pre-Migration Preparation

1. **Verify System Requirements:**
  - Before initiating the migration, confirm that your Mac meets the system requirements for Elements Mac Protection. You can find the requirements [here](#).

### 8.2 Migration Steps

1. **Uninstall Business Suite Client Security for Mac:**
  - Locate and run the 'Uninstall Client Security.app' from the folder: **/Applications/F-Secure**.
  - Follow the on-screen instructions to remove the Client Security software completely.
2. **Install Elements Mac Protection:**
  - After uninstalling the previous software, proceed to install Mac Protection for Elements.
  - Detailed installation instructions are available [here](#).

### 8.3 Post-Migration

Once the new software is installed, conduct a thorough check to ensure that Elements Mac Protection is operational and that all settings are correctly configured.



## 9 Migrating Linux devices

Migrating from Business Suite (BS) Linux to Elements Linux Protection requires a fresh installation approach. Unlike Windows, it's not possible to directly export and import policy rules for Linux systems. Additionally, compatibility should be checked as some Linux distributions supported in the old version may not be supported in Elements.

### 9.1 Pre-Migration Check

1. **Verify System Requirements:** Before proceeding, confirm that your Linux distribution is supported in the new version. Reference the system requirements [here](#).

### 9.2 Migration Steps

1. **Uninstall Business Suite Linux Security:**
  - Navigate to the uninstallation guide for Business Suite Linux Security [here](#).
  - Follow the instructions to completely remove the old Linux Security software.
2. **Install Elements Linux Protection:**
  - Download the required Linux binary from the 'Downloads' section in Endpoint Protection.
  - For installation instructions, refer to the guide [here](#).

#### Example Installation Commands

- **Using the Generic Installer:**
  - Download the "Generic" .tar file from the Elements Portal.
  - Execute the following command: `./f-secure-linuxsecurity-installer --subscription-key SUBSCRIPTION-KEY --profile-id PROFILE-ID .`
- **For .rpm or .deb Installations:**
  - Assign a profile during activation with this command: `/opt/f-secure/linuxsecurity/bin/activate --psb --subscription-key SUBSCRIPTION-KEY --profile-id PROFILE-ID .`

### 9.3 Post-Migration

After completing the migration process, ensure to verify the installation and configuration to confirm that the Elements Linux Protection is functioning as intended.

## 10 (Optional) Installing Elements Connector

Elements Connector is an on-premise product that serves three purposes.

- Elements Connector optimizes traffic between the managed endpoints in your environment and WithSecure services by caching Software Updater, malware definition updates, and program upgrades. If you download all these updates directly from the internet, your device consumes a huge amount of external traffic. To reduce the costs, you can use WithSecure caching endpoint, which downloads the requested files only once and then distributes them to the devices within your network.
- The Elements Connector Ultimate proxy acts as a proxy for all traffic between WithSecure endpoints and cloud services simplifying firewall configurations and allowing the use of WithSecure products in semi-closed environments.
- For companies that use security monitoring services such as Splunk, Elements Connector provides security events forwarding from WithSecure cloud services to security information and event management (SIEM).

### 10.1 Migrating from Policy Manager Proxy to Elements Connector

Elements Connector in its proxy role replaces WithSecure Policy Manager Proxy. The most important improvements over the previous product are automatic upgrades and support for centralized manageability from the WithSecure Elements Security Center.

System requirements for the Elements Connector can be found below:

[System requirements](#) | [Elements Connector](#) | [Latest](#) | [WithSecure User Guides](#)

Instructions on how to replace Policy Manager Proxy with Elements Connector or how to perform a clean installation can be found below:

[Replacing F-Secure Endpoint Proxy on Windows](#) | [Elements Connector](#) | [Latest](#) | [WithSecure User Guides](#)

In case the direct replacement fails, a fresh installation of the Elements Connector is recommended.

## 11 Troubleshooting installation issues

After starting the migration process, the freshly migrated clients can be found in the Device view of Elements Security Center. It is recommended to check the Connectivity status in the portal, to verify if there are any connectivity issues.

Also, there is a Connectivity tool available, which can be used to directly from the device to determine if it has any connection issues:

<https://download.withsecure.com/connectivitytool/ConnectionChecker.exe>

Please note that directly after the migration, the devices often show “Malware Protection: Malfunction”. This happens when the client is still downloading the detection database and will change after everything has been downloaded and installed successfully. Usually, the Capricorn engine takes the most time.