

**F-Secure Elements Connector
Getting Started Guide**

Contents

Chapter 1: F-Secure Elements Connector.....	3
1.1 Installing Elements Connector.....	4
1.1.1 Command-line parameters and MSI properties.....	4
1.2 Configuring API access for Elements Connector.....	4
1.3 Creating and assigning a profile for Elements Connector.....	5
1.4 Troubleshooting.....	5

F-Secure Elements Connector

Topics:

- [Installing Elements Connector](#)
- [Configuring API access for Elements Connector](#)
- [Creating and assigning a profile for Elements Connector](#)
- [Troubleshooting](#)

Elements Connector is an on-premise agent that allows you to connect the traffic between managed endpoints in your environment, F-Secure cloud services, and third-party security monitoring services.

For companies using security monitoring services such as Splunk, Elements Connector provides security information and event management (SIEM) message forwarding from F-Secure cloud services. The information forwarded to such third-party services can be customized with the F-Secure Elements APIs.

Note: F-Secure Elements Connector supports endpoints that are isolated from the internet, for example letting you cache Software Updater and malware definition updates.

1.1 Installing Elements Connector

Follow these instructions to install F-Secure Elements Connector in your managed environment.

Note: F-Secure Elements Connector is currently only available for Windows.

System requirements:

- One of the following Windows operating systems:
 - Windows Server 2008 R2 with latest SP1; Standard, Enterprise or Web Server editions
 - Windows Server 2012; Essentials, Standard or Datacenter editions
 - Windows Server 2012 R2; Essentials, Standard or Datacenter editions
 - Windows Server 2016; Essentials, Standard or Datacenter editions
 - Windows Server 2019; Essentials, Standard or Datacenter editions (Server Core is supported)
 - Windows 10
- Processor: Dual-core 2GHz CPU or higher
- Memory: 4 GB RAM
- Disk space: 10 GB of free disk space
- Network: 100 Mbit network

To download and install Elements Connector:

1. In the F-Secure Elements Endpoint Protection portal, go to the **Downloads** page and click **MSI** under **F-Secure Elements Connector > Windows**.
2. Save the download .msi file to the computer where you want to install Elements Connector.
3. On the command line, locate the installation .msi file and run the following command:

```
installer.msi VOUCHER=<subscription key>
```

Replace <subscription key> with a valid subscription key for Elements Connector. You can find your subscription key on the **Subscriptions** page in the PSB management portal.

4. Complete the installation wizard.

After installation, you have to configure the API access and assign a profile with the event forwarding settings before using the product.

1.1.1 Command-line parameters and MSI properties

When installing F-Secure Elements Connector using an .msi package, you can use the command-line parameters and MSI properties listed here.

MSI property	Explanation
VOUCHER	Sets the subscription key. Format: VOUCHER=<subscription key>
PROXY_SERVER	Overrides proxy to use for downloads. Format: PROXY_SERVER=<url>

1.2 Configuring API access for Elements Connector

When you have installed F-Secure Elements Connector, you have to configure some settings to make sure that the API access works.

1. Generate your API key:

- a) Log in to the F-Secure Elements Endpoint Protection portal as a partner account administrator.
 - b) Select **Get management API key** from the **Account** menu.
This starts the **Management API key** wizard.
 - c) Make note of the generated API key and the API server URL to use for your user account.
2. Create a `<ProgramData>\F-Secure\NS\ElementsConnector\data\api-access.properties` file.
 3. Add the following key-value pairs to the file:

```
apiUrl = <api-server-url>
apiKey = <api-key>
userName = <account-user-name>
password = <account-password>
```

Note: The user account should be the same that you specified while generating the API key.

4. Save the file.

1.3 Creating and assigning a profile for Elements Connector

To use Elements Connector for forwarding events to a third-party system, you have to create a profile that contains the necessary information.

1. In the F-Secure Elements Endpoint Protection portal, go to the **Profiles** page and select **For Connector**.
2. Click the **Actions** button for the default **F-Secure Elements Connector** profile and select **Clone profile**.
This opens the profile editor for the new, cloned profile.
3. Enter a name and description for the profile.
4. Check the current values under **General settings** and edit them if necessary.
5. Select **Event forwarding**.
6. To forward SIEM messages to a third-party system, switch on **Enable event forwarding** and enter the **SIEM system address** for the target system.
7. Select the **Message format** and **Protocol** for the forwarded messages.
8. Click **Save and publish**.
The new profile now appears on the **For Connector** profile list.
9. Go to the **Devices** page and select **Connectors**.
10. Select the device that you want to modify and select **Assign profile** in the **Actions** bar.
11. Select the profile that you want to use and click **Assign**.

The new profile is now assigned to the selected installation of Elements Connector and the SIEM messages are forwarded to the configured system.

1.4 Troubleshooting

Connector creates several log files that can help you to solve issues that you might have while using it.

All Connector logs are stored in the `<ProgramData>\F-Secure\NS\ElementsConnector\log` folder.

- `fsconnector-forwarding.log` contains information about forwarded events,
- `upstream-request.log` collects all Connector requests to F-Secure Cloud.