# Suspicious Object List Exporter and Importer User Guide

The Trend Micro Control Manager™ Suspicious Object List Exporter and Importer tools allow you to export and import Control Manager Suspicious Object lists without having to sign in to the Control Manager management console.

- Suspicious Object List Exporter: Exports Suspicious Object lists from the Control Manager server in multiple file formats.
- Suspicious Object List Importer: Imports properly formatted comma-separated value (CSV) suspicious object data into Control Manager.

Use the Exporter and Importer tools to synchronize suspicious object data across multiple Control Manager servers and supported third-party applications to enhance your protection against unknown and emerging threats.

# Using Suspicious Object List Exporter

Use the Suspicious Object List Exporter tool to export Control Manager Suspicious Object lists in multiple file formats. By default, the Suspicious Object List Exporter tool exports suspicious object data in XML format.

For details on how to change the output file format, see *Modifying the Configuration File on page 6*.

---

**Important**

The Suspicious Object List Exporter tool requires Control Manager 6.0 Service Pack 3 Patch 2 or later.

To download the latest installation package, see http://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=latest&clkval=4202&lang_loc=1.

---

**Procedure**

1. Install Hotfix 3453 on the Control Manager server.

2. Open a command prompt.

3. Use the following command to locate the directory which contains the `SuspiciousObjectExporter.exe` file:

   **`cd <Control Manager installation directory>\SOTools`**

4. Execute `SuspiciousObjectExporter.exe` using the following command:

   **`SuspiciousObjectExporter.exe [/s <Start ID> /e <End ID>] [/f <y | n>] [/d]`**

Note

Running **`SuspiciousObjectExporter.exe`** without any parameters displays usage details and prompts you to provide <Start ID> and <End ID> values.

| PARAMETER | DESCRIPTION | EXAMPLE |
|---|---|---|
| /s <Start ID> | Indicates the ID of the first object to export<br><br>**Note**<br>• Requires that you specify the /e <End ID> value<br>• Specifying a value of 0 indicates the start of the list | • `SuspiciousObjectExporter.exe /s 0 /e 0`<br>Exports all suspicious objects and locks the command line interface during the export process<br>• `SuspiciousObjectExporter.exe /s 3 /e 8`<br>Exports suspicious objects starting from ID 3 to ID 8 and locks the command line interface during the export process<br>• `SuspiciousObjectExporter.exe /s 0 /e 4`<br>Exports suspicious objects starting from the beginning of the list to ID 4 and locks the command line interface during the export process |

| PARAMETER | DESCRIPTION | EXAMPLE |
|---|---|---|
| /e <End ID> | Indicates the ID of the last object to export<br><br>**Note**<br>• Requires that you specify the /s <Start ID> value<br>• Specifying a value of 0 indicates the end of the list | • `SuspiciousObjectExporter.exe /s 0 /e 0`<br>Exports all suspicious objects and locks the command line interface during the export process<br>• `SuspiciousObjectExporter.exe /s 3 /e 8`<br>Exports suspicious objects starting from ID 3 to ID 8 and locks the command line interface during the export process<br>• `SuspiciousObjectExporter.exe /s 4 /e 0`<br>Exports suspicious objects starting from ID 4 to the end of the list and locks the command line interface during the export process |

| PARAMETER | DESCRIPTION | EXAMPLE |
|---|---|---|
| /f <y \| n> | Specifies whether to lock the command line interface during the export process<br><br>**Note**<br>Optional parameter; if not specified, the default is "yes"<br><br>**Important**<br>You must specify the following parameter in the **Add arguments (optional)** field when scheduling automatic exports using the `SuspiciousObjectExporter.exe` tool, a PowerShell script, or a batch script in Windows Task Scheduler:<br>**`/f n`** | • **`SuspiciousObjectExporter.exe /f y`**<br>Exports all suspicious objects and locks the command line interface during the export process<br>• **`SuspiciousObjectExporter.exe /s 0 /e 0 /f y`**<br>Exports all suspicious objects and locks the command line interface during the export process<br>• **`SuspiciousObjectExporter.exe /f n`**<br>Exports all suspicious objects and unlocks the command line interface during the export process |
| /d | Use to enable debug mode<br><br>**Note**<br>Optional parameter normally used by Support to identify errors | **`SuspiciousObjectExporter.exe /d`**<br>Exports all suspicious objects with additional debugging logs |

5. To view the exported Suspicious Object list, go to the `<Control Manager installation directory>\SOTools\` directory and open the `SuspiciousObjectList.xml` file.

6. To view all export logs, go to the `<Control Manager installation directory>\SOTools\` directory and open the `ExportRecord.txt` file.

## Modifying the Configuration File

To change the default configuration settings, go to the `<Control Manager installation directory>\SOTools` directory and modify the `SuspiciousObjectExporter.exe.config` file.

| KEY | DESCRIPTION | EXAMPLE |
|---|---|---|
| outputRootFolderPath<br><br>Location: `<appSettings>` | Indicates the working directory for the `SuspiciousObjectExporter.exe` tool | • `<add key="outputRootFolderPath" value="."/>`<br><br>The tool uses the directory in which the `SuspiciousObjectExporter.exe` program resides to process the lists<br><br>• `<add key="outputRootFolderPath" value="C:\Program Files (x86)\Trend Micro\Control Manager"/>`<br><br>The tool uses the specified directory (`C:\Program Files (x86)\Trend Micro\Control Manager`) to process the lists |
| outputFolderName<br><br>Location: `<appSettings>` | Indicates the output directory for the exported Suspicious Object list file | • `<add key="outputFolderName" value="SOTools"/>`<br><br>Exports the file to the `SOTools` directory<br><br>• `<add key="outputFolderName" value="SOList"/>`<br><br>Exports the file to the `<outputRootFolderPath>\SOList` directory |

| KEY | DESCRIPTION | EXAMPLE |
|---|---|---|
| styleSheetFile<br><br>Location: `<appSettings>` | Indicates the style sheet that the tool applies to the exported list | • `<add key="styleSheetFile" value=""/>`<br><br>Exports all lists in XML format to a `*.txt` or `*.xml` file as specified by the `outputFile` key<br><br>• `<add key="styleSheetFile" value="ExportCSV.xslt"/>`<br><br>Used to export the Virtual Analyzer Suspicious Object list, User-Defined Suspicious Object list, or Exception list with a limited subset of columns in CSV format<br><br>**Important**<br><br>You can use the `ExportCSV.xslt` style sheet to export other Suspicious Object lists, however, you cannot re-import the lists back into Control Manager.<br><br>After selecting the `ExportCSV.xslt` style sheet, you can no longer configure which columns the tool exports. The tool only exports the columns specified in the style sheet.<br><br>• `<add key="styleSheetFile" value="ExportSTIX.xslt"/>`<br><br>Used to export all Suspicious Object lists in STIX format<br><br>• `<add key="styleSheetFile" value="ExportCPL.xslt"/>`<br><br>Used to export all Suspicious Object lists in CPL format |

| KEY | DESCRIPTION | EXAMPLE |
|---|---|---|
| "outputFile"<br><br>Location:<br>`<appSettings>` | Indicates the file name and extension of the exported Suspicious Object list file<br><br>Specify a new file extension to change the output file format | • `<add key="outputFile" value="SuspiciousObjectList.xml"/>`<br><br>Exports the Suspicious Object list as an `.xml` file named `SuspiciousObjectList.xml`<br><br>• `<add key="outputFile" value="SuspiciousObjectList.txt"/>`<br><br>Exports the Suspicious Object list as a `.txt` file named `SuspiciousObjectList.txt` |
| <suspiciousObjectColumns><br><br>Location:<br>`<soDataColumnSettings>` | Indicates the data columns on the selected list<br><br>Set `isEnable="true"` to export the specified data column | • `<add id="1" name="SeqID" isEnable="true"></add>`<br><br>Exports the "SeqID" data column from the selected list<br><br>• `<add id="1" name="MD5Key" isEnable="false"></add>`<br><br>Explicitly excludes the "MD5Key" data column from the selected list<br><br>**Important**<br><br>If you specified the `ExportCSV.xslt` style sheet, the tool only exports the columns specified in the style sheet. |
| <suspiciousObjectTypeList><br><br>Location:<br>`<soTypeSettings>` | Indicates the types of objects to export from the selected list<br><br>Set `isEnable="true"` to export the specified object type | • `<add value="0" description="IP" isEnable="true"></add>`<br><br>Exports all IP address type objects from the selected list<br><br>• `<add value="1" description="Domain" isEnable="false"></add>`<br><br>Explicitly excludes all "Domain" objects from the exported list |

| KEY | DESCRIPTION | EXAMPLE |
|---|---|---|
| <suspiciousObjectSourceType><br><br>Location: `<soTypeSettings>` | Indicates the suspicious object source type<br><br>Set `isEnable="true"` to export the specified object type | • `<add value="0" description="SourceType" isEnable="true"/>`<br><br>Selects the Virtual Analyzer Suspicious Object list<br><br>• `<add value="1" description="SourceType" isEnable="true"/>`<br><br>Selects the User-Defined Suspicious Object list<br><br>• `<add value="2" description="SourceType" isEnable="true"/>`<br><br>Selects the Virtual Analyzer Exception list<br><br>**Important**<br><br>• If you specified the `ExportCSV.xslt` style sheet and select the Virtual Analyzer Suspicious Object list or the User-Defined Suspicious Object list, the tool exports the following columns: **Object**, **Type**, **At Risk Endpoints/ Recipients**, **Notes** and **Scan Action**.<br><br>• If you specified the `ExportCSV.xslt` style sheet and select the Virtual Analyzer Exception list, the tool exports the following columns: **Object**, **Type**, **At Risk Endpoints/Recipients**, and **Notes**. |

# Using Control Manager to Export the Virtual Analyzer Exception List

**Important**

Control Manager only supports exporting the Virtual Analyzer Suspicious Object Exception list in CSV format.

**Procedure**

1. Go to **Administration** > **Suspicious Objects** > **Virtual Analyzer Objects**

   The **Virtual Analyzer Suspicious Objects** screen appears.

2. Click the **Exceptions** tab.

3. Click **Export All**.

   A progress screen appears.

4. When the export finishes, click **Download**.

   A confirmation box appears.

5. Click **Save**.

   The **Save As** screen appears.

6. (Optional) Specify a new location or file name.

7. Click **Save**.

## Using Control Manager to Export the User-Defined List

**Important**

Control Manager only supports exporting the User-Defined Suspicious Object list in CSV format.

**Procedure**

1. Go to **Administration** > **Suspicious Objects** > **User-Defined Objects**

   The **User-Defined Suspicious Objects** screen appears.

2. Click **Export All**.

A progress screen appears.

3. When the export finishes, click **Download**.

   A confirmation box appears.

4. Click **Save**.

   The **Save As** screen appears.

5. (Optional) Specify a new location or file name.

6. Click **Save**.

# Using Suspicious Object List Importer

Use the Suspicious Object List Importer tool to import properly formatted `*.csv` files of suspicious object data into Control Manager.

**Important**

The Suspicious Object List Importer tool requires Control Manager 6.0 Service Pack 3 Patch 2 or later.

To download the latest Control Manager installation package, see http://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=latest&clkval=4202&lang_loc=1.

### Procedure

1. Install Hotfix 3453 on the Control Manager server.

2. Open a command prompt.

3. Use the following command to locate the directory which contains the `ImportSOFromCSV.exe` file:

   ```
   cd <Control Manager installation directory>
   ```

4. Execute `ImportSOFromCSV.exe` using the following command:

**ImportSOFromCSV.exe "<full path>" {UserDefinedSO | ExceptionSO}**

Where:

- **<full path>**: Indicates the directory and file name of the properly formatted CSV file
- **{UserDefinedSO}**: Indicates the file that contains User-Defined Suspicious Object list data
- **{ExceptionSO}**: Indicates the file that contains Virtual Analyzer Exception list data

For example:

- **SuspiciousObjectImporter.exe "c:\Program Files (x86)\Trend Micro\Control Manager \importExceptionSample.csv" ExceptionSO**

  Imports the `importExceptionSample.csv` file from the `c:\Program Files (x86)\Trend Micro\Control Manager` directory to the Virtual Analyzer Exception list in Control Manager

# Using Control Manager to Import the Virtual Analyzer Exception List

Important

Control Manager only supports importing properly formatted `*.csv` files of Virtual Analyzer Exception list data.

**Procedure**

1. Go to **Administration** > **Suspicious Objects** > **Virtual Analyzer Objects**

   The **Virtual Analyzer Suspicious Objects** screen appears.

2. Click the **Exceptions** tab.

3. Click **Import**.

   The **Import Exception** screen appears.

4. Click **Browse...** and select the `*.csv` file containing the Exception list data.

5. Click **Open**.

6. Click **Import**.

   The **Import Exception** screen closes and the imported exceptions appear in the Virtual Analyzer Suspicious Object Exception list.

## Using Control Manager to Import the User-Defined List

**Important**

Control Manager only supports importing properly formatted `*.csv` files of user-defined suspicious object data.

**Procedure**

1. Go to **Administration** > **Suspicious Objects** > **User-Defined Objects**

   The **User-Defined Suspicious Objects** screen appears.

2. Click **Import**.

   The **Import User-Defined List** screen appears.

3. Click **Browse...** and select the `*.csv` file containing the user-defined suspicious object data.

4. Click **Open**.

5. Click **Import**.

The **Import User-Defined List** screen closes and the imported objects appear in the User-Defined Suspicious Object list.