

# Configure a Custom Time for TETRA Downloads

## Contents

[Introduction](#)

[Background Information](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

## Introduction

This document describes how to configure local endpoints to download TETRA updates at any desired time to meet requirements with bandwidth usage.

## Background Information

TETRA is the offline engine for Secure Endpoint which uses antivirus signatures to give protection to the endpoints. TETRA receives daily updates to its signature database to keep up with all the new threats on the wild. These updates can use significant bandwidth on large environments, therefore, each endpoint randomizes the time for the download inside the update interval which by default is set to 1 hour. Even though different update intervals are available to choose on the TETRA policy, it is not possible to choose a specific time to trigger this download process. This document provides a workaround to force TETRA to update its AV signatures with Windows Schedule jobs.

## Prerequisites

### Requirements

Basic Knowledge of Secure Endpoint policy configuration and Windows Schedule jobs.

### Components Used

- Secure Endpoint Cloud Console
- Secure Endpoint connector for Windows 8.1.3
- Windows 10 Enterprise

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, ensure that you understand the potential impact of any command.

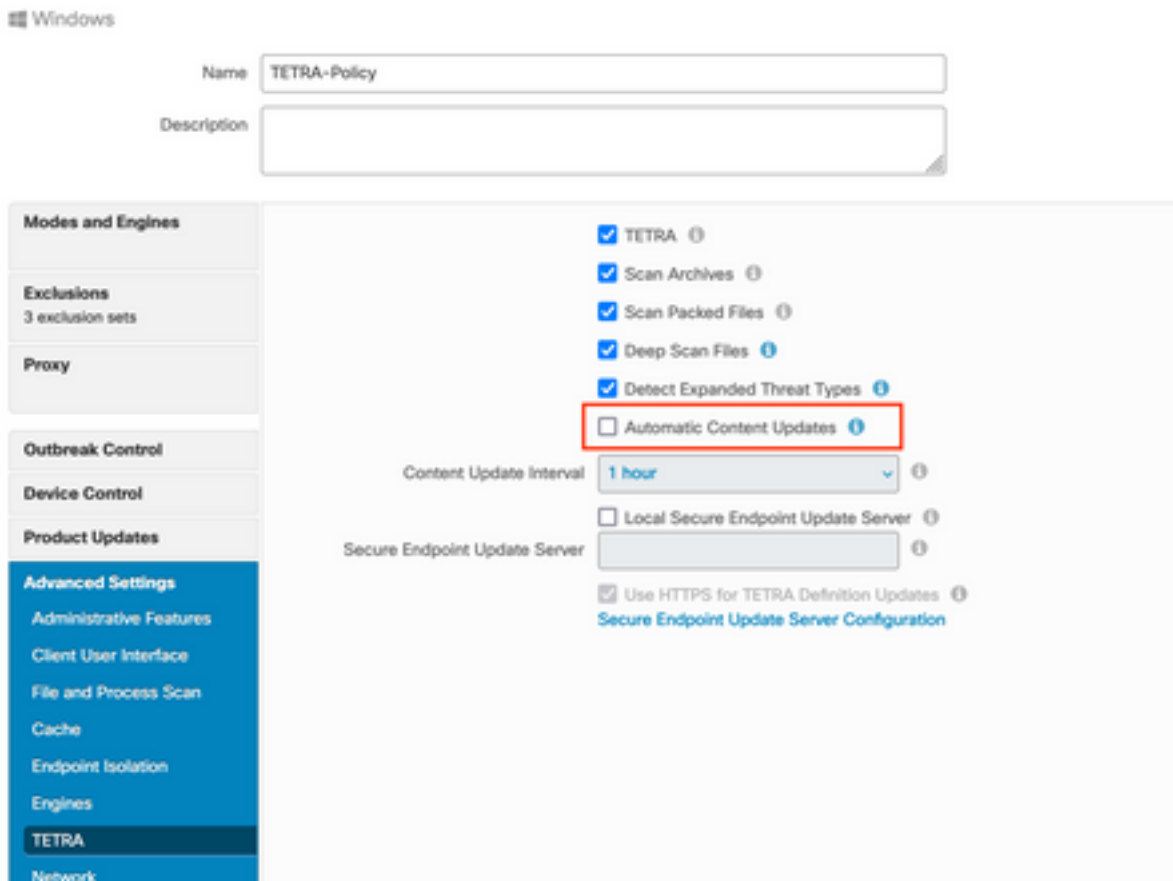
## Configure

**Warning:** As described in the background section, TETRA updates can consume significant bandwidth. By default, Secure Endpoint tries to reduce this impact and randomize the TETRA updates inside the update interval which is set to 1 hour by default. It is not recommended to force all the connectors to update the definitions at the same time, especially on large environments. This process must be used only on special situations where it is critical to control the time of the update. On any other case scenario, automatic updates are preferable.

Choose a Secure Endpoint policy to configure for custom TETRA download time.

**Note:** Please be aware that this configuration is done on a policy basis and all the endpoints in this policy are affected. So it is recommended to put all the devices you want to control for custom TETRA updates on the same Secure Endpoint policy.

Log in to your Secure Endpoint Management Console and navigate to **Management > Policies**, then search for the policy you have chosen to use, click **edit**. Once you are on the policy configuration page, navigate to the **TETRA Section**. Under this section, un-check the **Automatic Content Updates** checkbox and **save** the policy. This is all related to configuration on the Secure Endpoint Cloud console.



The screenshot shows the configuration page for a policy named "TETRA-Policy". The left sidebar contains a navigation menu with the following items: Windows, Modes and Engines, Exclusions (3 exclusion sets), Proxy, Outbreak Control, Device Control, Product Updates, Advanced Settings (highlighted), Administrative Features, Client User Interface, File and Process Scan, Cache, Endpoint Isolation, Engines, TETRA (highlighted), and Network. The main content area is titled "TETRA" and contains the following settings:

- TETRA ⓘ
- Scan Archives ⓘ
- Scan Packed Files ⓘ
- Deep Scan Files ⓘ
- Detect Expanded Threat Types ⓘ
- Automatic Content Updates ⓘ (highlighted with a red box)
- Content Update Interval: 1 hour ⓘ
- Local Secure Endpoint Update Server ⓘ
- Secure Endpoint Update Server: ⓘ
- Use HTTPS for TETRA Definition Updates ⓘ

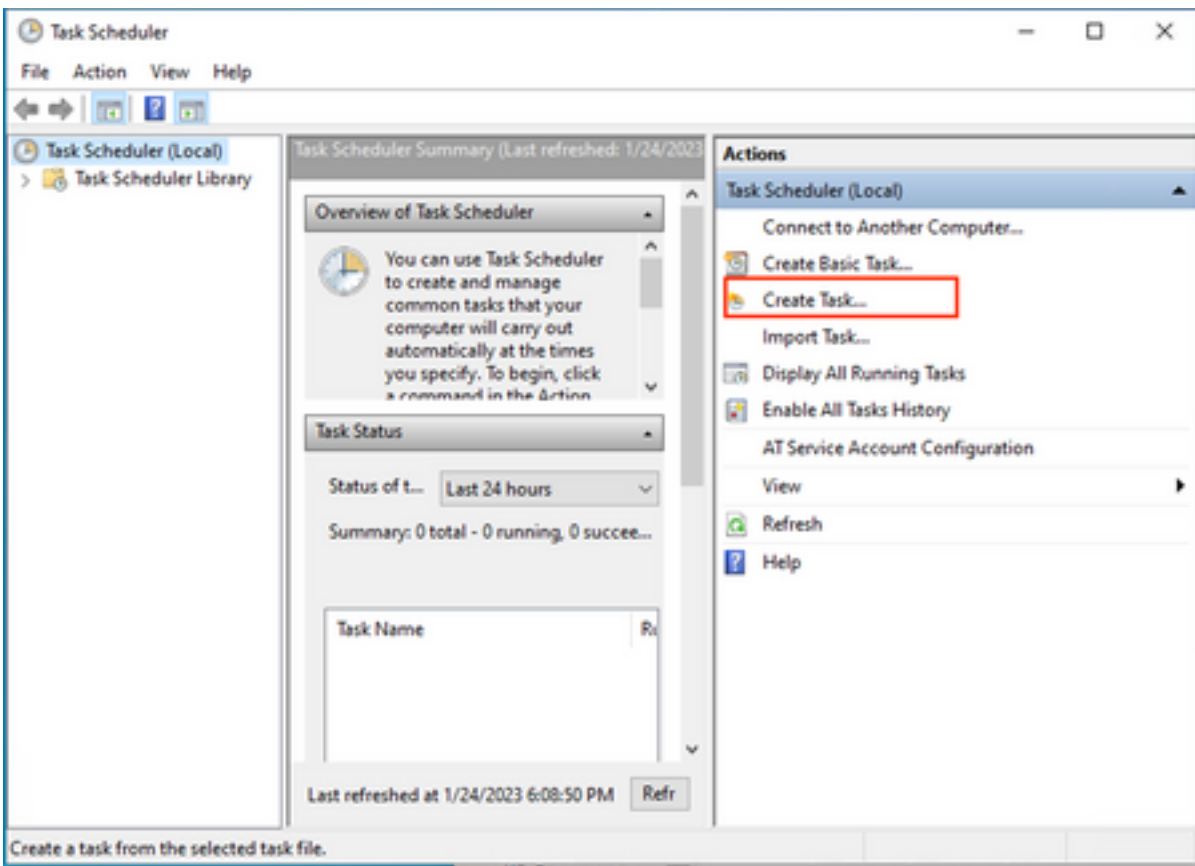
At the bottom of the TETRA section, there is a link for "Secure Endpoint Update Server Configuration".

For the next configuration piece, access your Windows device and open a new Notepad file to add these lines:

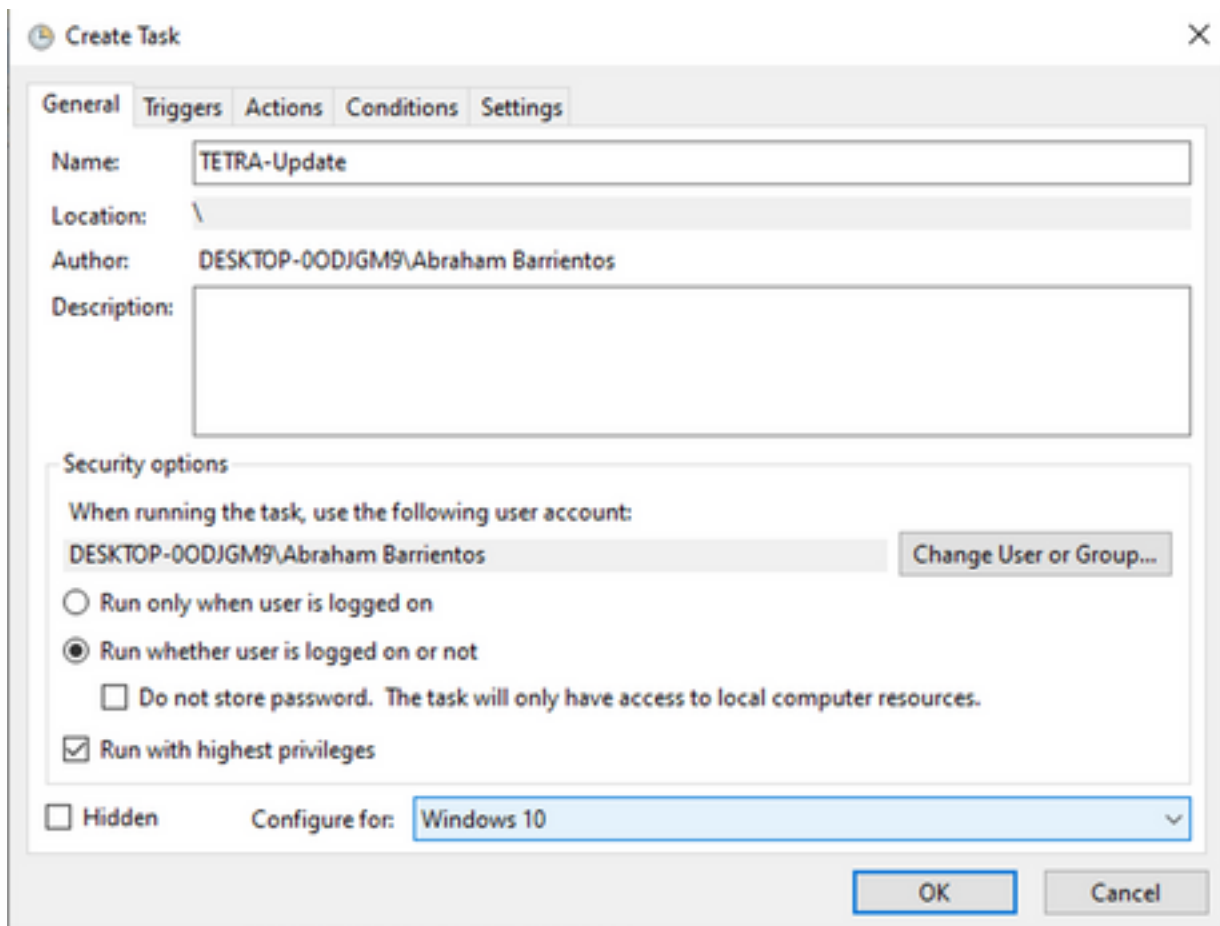
```
cd C:\Program Files\Cisco\AMP\8.1.3.21242
sfc.exe -forceupdate
```

Please note that you need to use the Secure Endpoint version ( 8.1.3.21242v for this example ) that matches the current installed version on the endpoint. If you are not sure of the version, you can click the **Secure Endpoint** user interface gear icon and then **Statics Tab** to check on the current version. Once you have added these lines to the notepad, click **File** and then click on **Save As**. Then click **Save as a Type** and select **All files**. Finally, type the name of the file and save it as .BAT extension. If you want to save the file under C:\ folder, you need to execute notepad with Admin privileges. As a side note you can execute the BAT file to force the TETRA update for as a test.

Open the Schedule Task Open Task Scheduler on your windows machine and click **Create a Task** button located on the right column.



Under **General Tab**, type the name for this Task and select **Run whenever user is logged or not**. Check **Run with the highestst privelages** check-box. Under **configure for** option, choose the OS that applies. For this demonstration, Windows 10 was used.



Under **Triggers** tab click **New Trigger**. On the New trigger configuration page, you can customize the time when you want TETRA to update its signatures. For this example, a daily schedule which runs at 1 PM local machine time was used. Start date option defines when this task becomes active. Once you are done with the schedule settings, click **ok**.

Edit Trigger

Begin the task: On a schedule

Settings

One time

Daily

Weekly

Monthly

Start: 1/24/2023 1:00:00 PM  Synchronize across time zones

Recur every: 1 days

Advanced settings

Delay task for up to (random delay): 1 hour

Repeat task every: 1 hour for a duration of: 1 day

Stop all running tasks at end of repetition duration

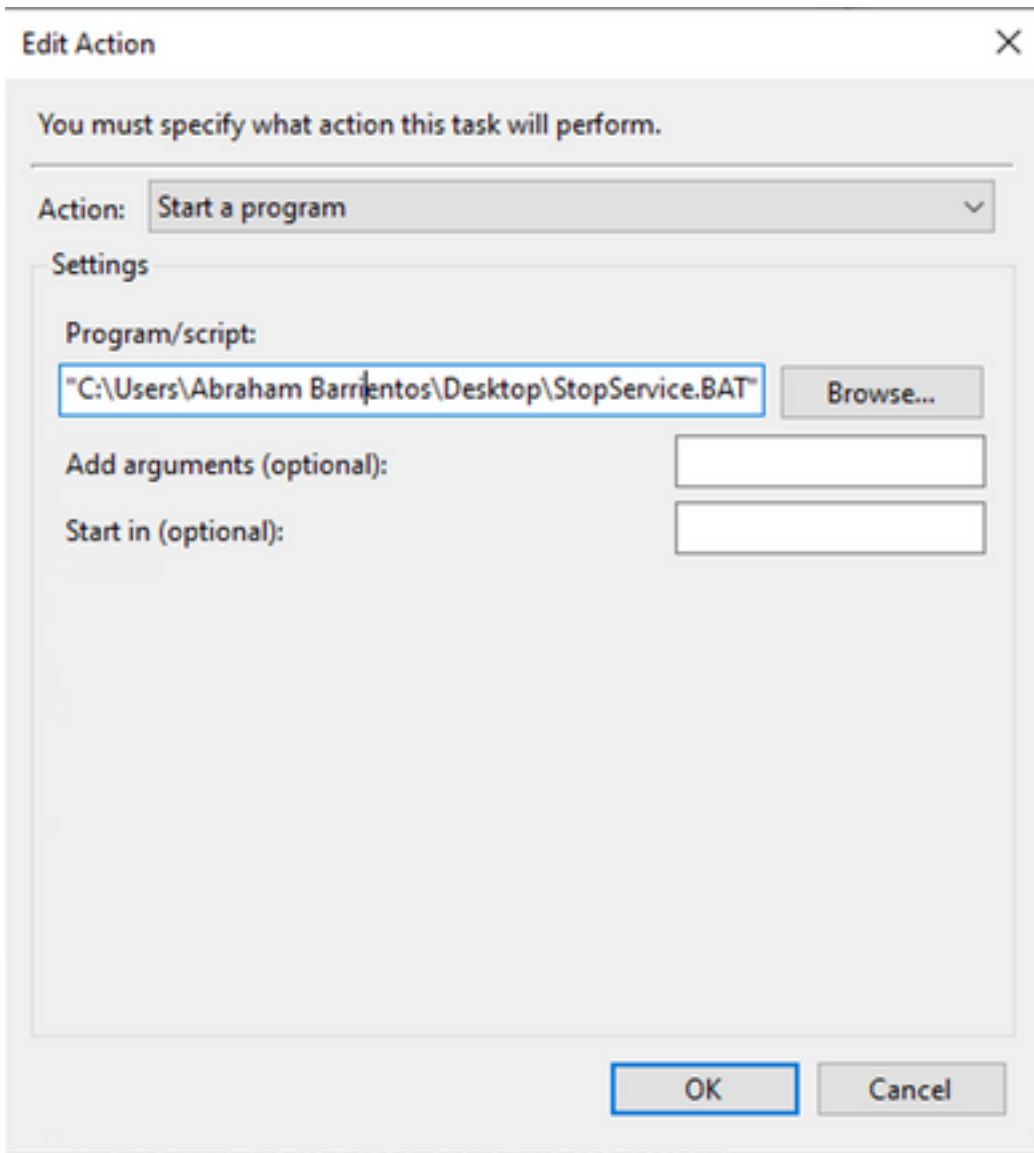
Stop task if it runs longer than: 3 days

Expire: 1/24/2024 6:50:59 PM  Synchronize across time zones

Enabled

OK Cancel

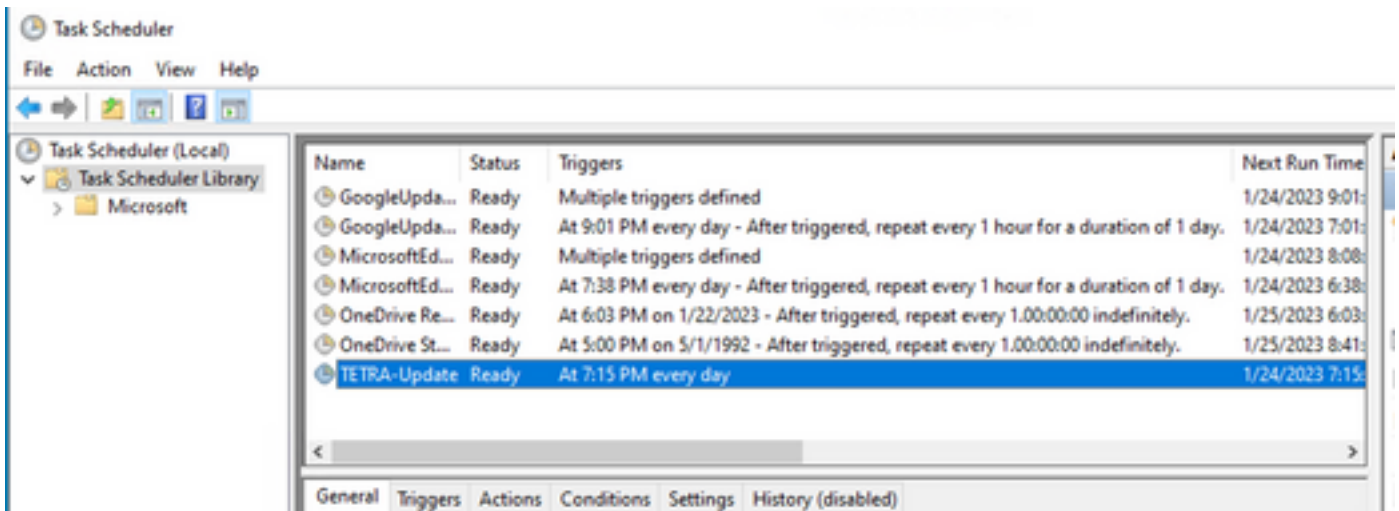
On the **Actions** Tab click **New Action**. On the **New Action** tab choose **Start a program** for the **Action** setting. Under Program/Settings click **Browse**, and search then select the BAT script. Click **Ok** to create the action. Leave the rest of settings default and click **Ok** to create the Task.



Finally, this Task Scheduler requires administrative credentials to create the task since "Run with highest privileges" was selected. After authentication with admin credentials, the task is ready to run and execute to tell Secure Endpoint service when to update TETRA accordingly to the schedule configured.

## Verify

Click **Task Scheduler Library** folder in the left column. Verify the schedule has been created and listed as expected.



You can check the latest TETRA definition number downloaded by the connector under **Secure Endpoint User interface > statics** tab. You can use this number to compare the latest definitions available on the console under **Management > Av Definitions summary** to find out if device is up to date with the latest definitions. Another alternative is to monitor the "Definitions Last Updated" value for the particular endpoint in the Secure Endpoint Console.

DESKTOP-00DJGM9 in group Jobbarrie_Proxy		Definitions Up To Date	
Hostname	DESKTOP-00DJGM9	Group	Jobbarrie_Proxy
Operating System	Windows 10 Enterprise (Build 19045.2486)	Policy	TETRA-Policy
Connector Version	8.1.3.21242	Internal IP	
Install Date	2023-01-23 13:01:50 CST	External IP	
Connector GUID	22277c92-e5f5-4dcb-894c-392d4428b5c0	Last Seen	2023-01-24 20:24:25 CST
Processor ID	0f8bfbf000006f1	Definition Version	TETRA 64 bit (daily version: 89889)
Definitions Last Updated	2023-01-24 20:24:25 CST	Update Server	tetra-defs.amp.cisco.com
Cisco Secure Client ID	N/A		

[Events](#)
[Device Trajectory](#)
[Diagnostics](#)
[View Changes](#)

## Troubleshoot

When definitions are not updated as expected, you can take a look at the logs to search for a TETRA update error. To do this, enable debug mode on the Secure Endpoint user interface under the Advanced tab prior to the Schedule task trigger time. Let the connector run on this mode for at least 20 min after the Schedule Task Trigger and then take a look into the latest **sfcx.exe.log** file located under **C:\Program Files\Cisco\AMPX.X.X** (where X.X.X is Current version of Secure Endpoint on the system).

The ForceWakeUpdateThreadAbout shows us that TETRA is triggered by our Schedule Job to update as expected. If you do not see this log, then it can be an issue related to the windows schschedule task configuration.

```
(99070187, +0 ms) Jan 24 20:30:01 [3544]: ForceWakeUpdateThreadAbout to force update thread awake. Forcing tetra def update.
(99070187, +0 ms) Jan 24 20:30:01 [1936]: UpdateThread: Tetra ver string retrieved from config:
(99070781, +0 ms) Jan 24 20:30:02 [1936]: UpdateTetra entered...
(99070781, +0 ms) Jan 24 20:30:02 [1936]: UpdateTetra: elapsed: cur: 1674621002, last: 0, interval:180
```

In the case where Schedule Job successfully triggers TETRA to update definitions, you need to search for any related TETRA error on the logs. This is an example of a TETRA error code 2200 which means the service got interrupted during the update process. How to troubleshoot general TETRA errors is outside the scope of this document, however, the links at the end of this document are useful Cisco Articles about Troubleshoot TETRA error codes.

```
ERROR: TetraUpdateInterface::update Update failed with error -2200
```

## Related Information

- [Troubleshooting TETRA definitions update failures](#)
- [Cisco Secure Endpoint - Tetra Definitions Update Failure with 3000 Error](#)
- [TETRA Error Codes - Windows](#)