AMP Update Server Configuration Steps

Contents

Introduction

This document describes detailed configuration steps for Cisco Advanced Malware Protection (AMP) TETRA Update Server.

Prerequistes

- Knowledge of Server hosts such as, Windows 2012R2 or CentOS 6.9 x86_64.
- Knowledge of hosting software such as, IIS (Windows only), Apache, Nginx
- Configured Server hosts with HTTPS enabled, valid trusted certificate installed.
- Configured HTTPS Local Update Server option.

Note: For full details into enabling Local Update Server configuration and requirements, please refer to Chapter 25 of the AMP for Endpoints User Guide, available here. (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf)

Note: Server Hosts (IIS, Apache, Nginx) are third-party products and are not supported by Cisco, please refer to the support teams for respective products for questions outside the provided steps.

Warning: If AMP is configured with a Proxy server, all update traffic (including TETRA) will continue to be sent through the proxy server, directed to your local server. Ensure that the traffic is allowed passed the proxy without any modification while in transit.

Install Steps

All Platforms

1. Confirm your Hosting Server Operating System (OS).
2. Confirm your AMP for Endpoints Dashboard portal, download the Updater Software Package and configuration file.

AMP for Endpoints Console:

US - https://console.amp.cisco.com/tetra_update

EU - https://console.eu.amp.cisco.com/tetra_update

APJC - https://console.apjc.amp.cisco.com/tetra_update

Windows IIS

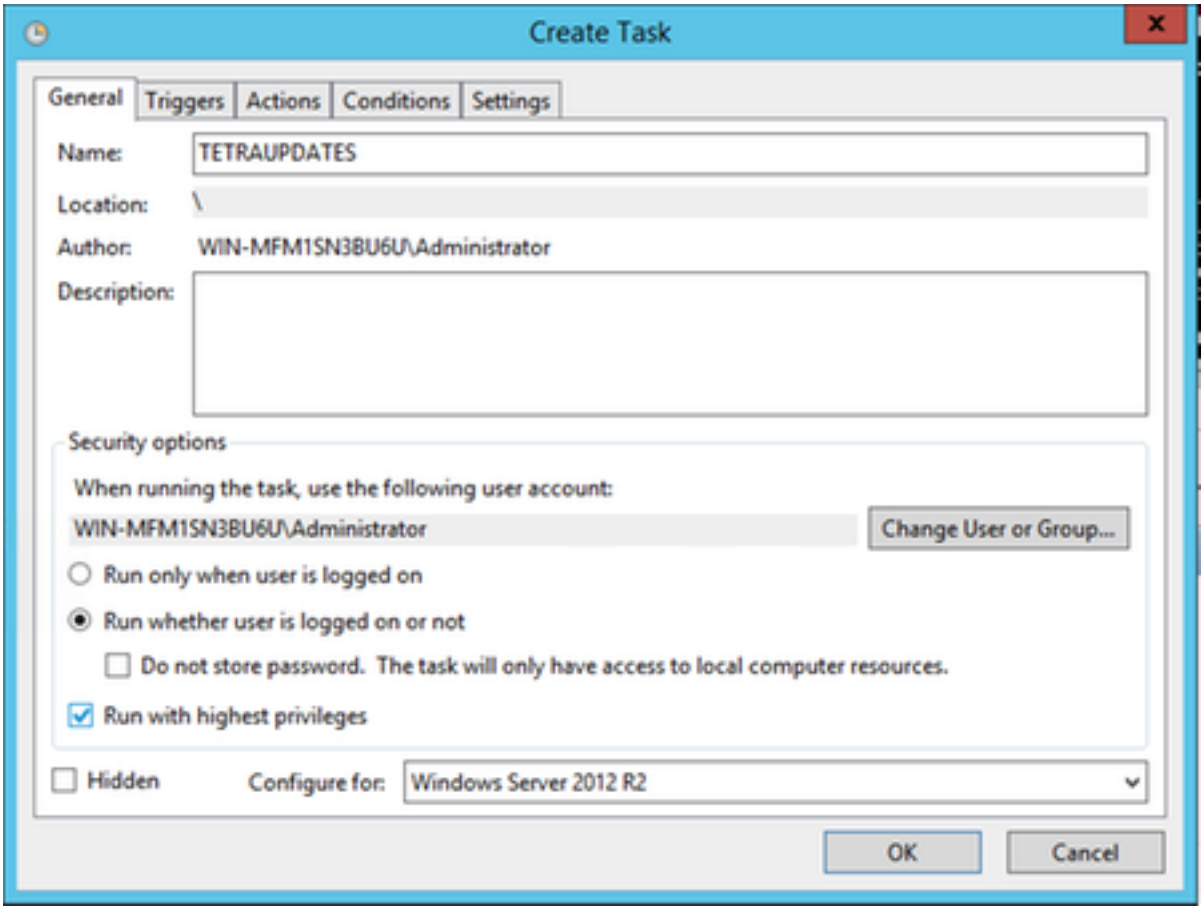
> **Note**: The steps below are based on the new IIS Application Pool to host the signatures, **not** the default Application Pool. To use the default pool, change the **--mirror** folder in the provided steps to reflect the default web hosting path (**C:\inetpub\wwwroot**)

Directory Creation

1. Create a new folder on the root drive, name it **TETRA**.
2. Copy the zipped AMP updater software package and configuration file to the **TETRA** folder created.
3. Unzip the software package in this folder.
4. Create a new folder called **Signatures** inside the TETRA folder.

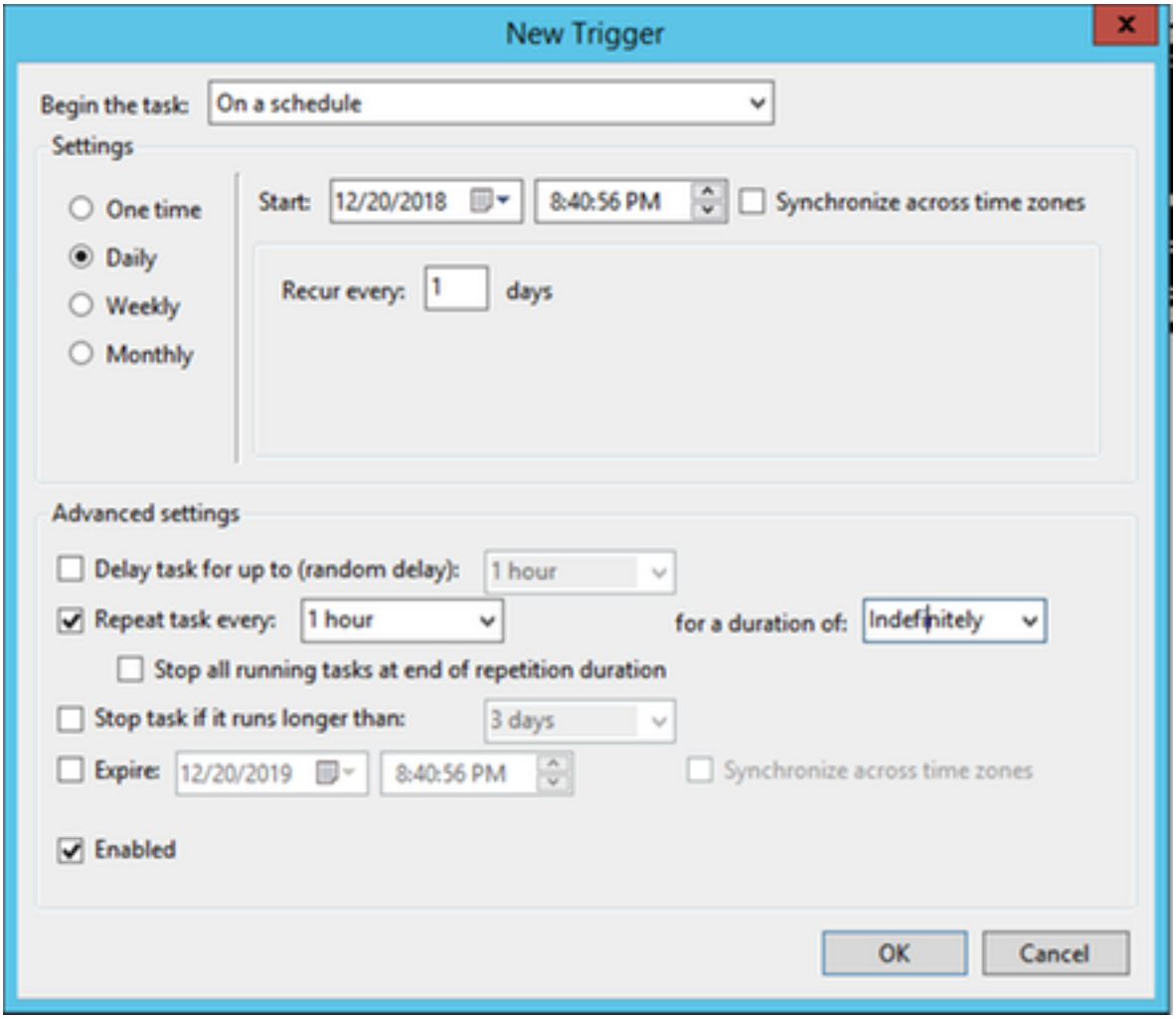
Update Task Creation

1. Open the command line and navigate to the *C:\TETRA* folder.***cd C:\TETRA***
2. Run the command ***update-win-x86-64.exe fetch --config="C:\TETRA\config.xml" --once --mirror C:\TETRA\Signatures***
3. Open the Task Scheduler and create a new Task. (Action > Create Task) to run the updater software automatically with the following options where needed:
4. Select the General tab. Enter a Name for the task.Select **Run whether user is logged on or not**.Select **Run with highest privileges.**Select **operating system** from the **Configure** drop down**.**



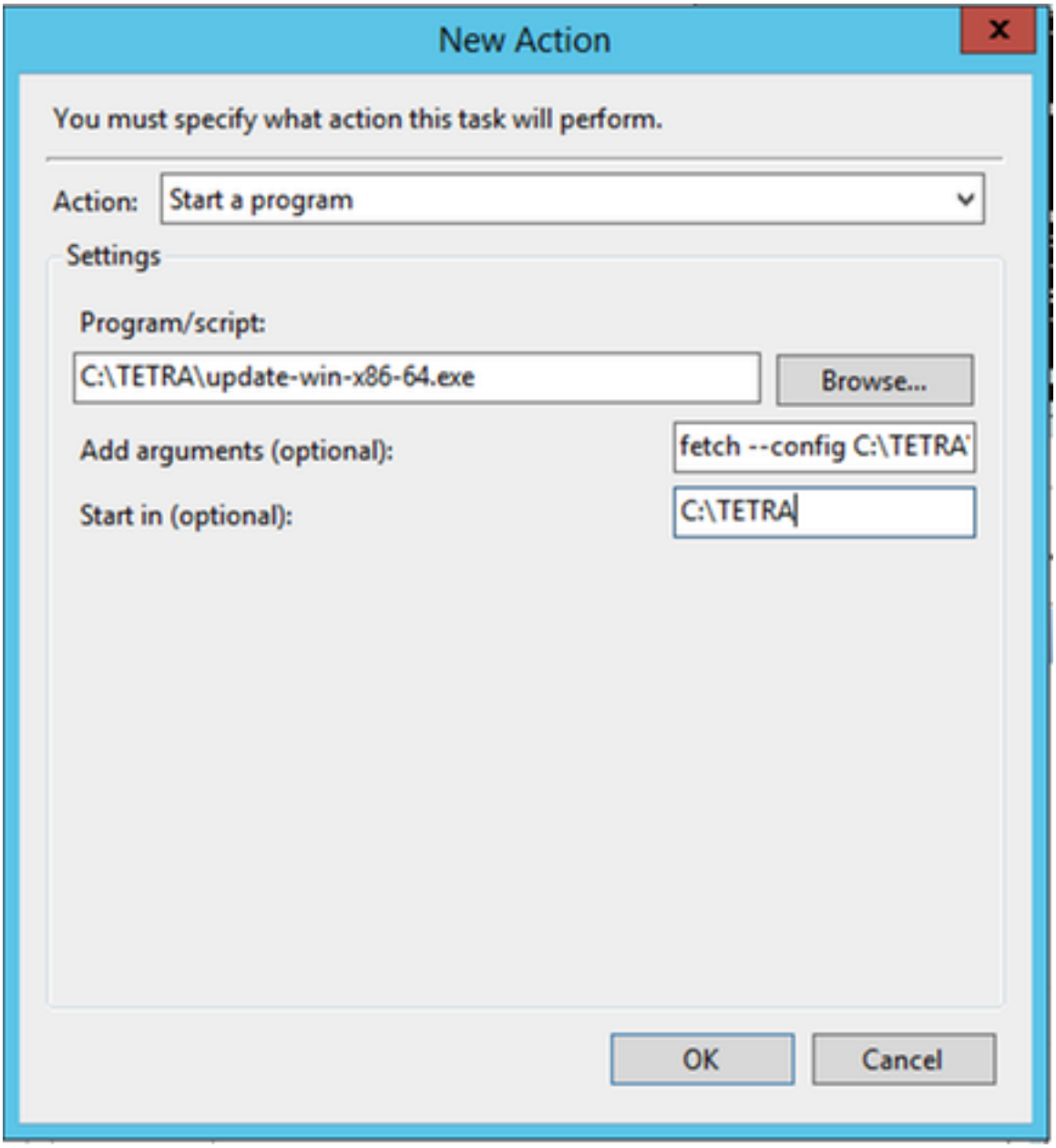
5. Select the Triggers tab.

- Click New.
- Select **On a schedule** from the **Begin the task** drop down.
- Select **Daily** under Settings.
- Check **Repeat task every** and **select 1 hour** from the drop down and select **Indefinitely** from the "**for a duration of:"**
- Verify that **Enabled** is **checked**.
- Click **Ok**.



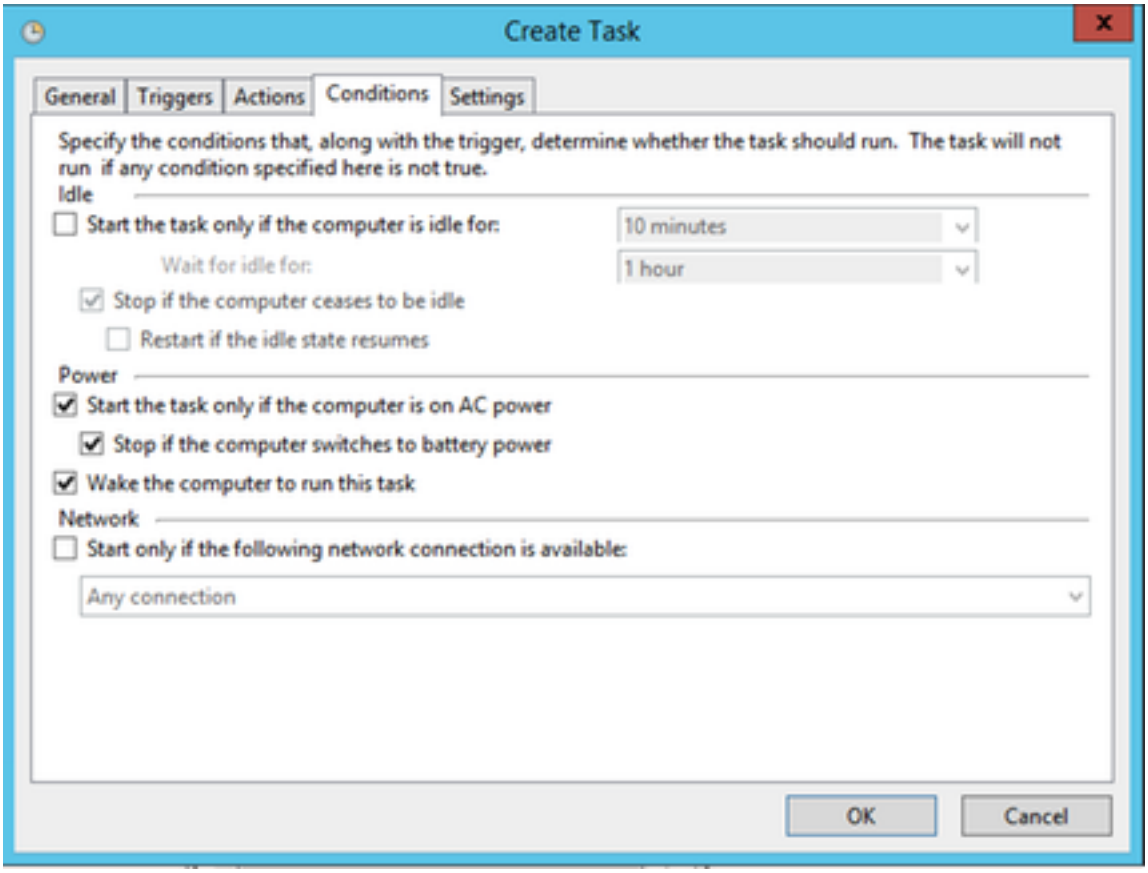
6. Select the Actions tab

- Click **New**.
- Select **Start a program** from the **Action** drop down.
- Enter ***C:\TETRA\update-win-x86-64.exe*** in the **Program/script** field.
- Enter ***fetch --config C:\TETRA\config.xml --once --mirror C:\TETRA\Signatures*** in the **Add arguments** field.
- Enter ***C:\TETRA*** in the **Start** in field
- Click **OK**



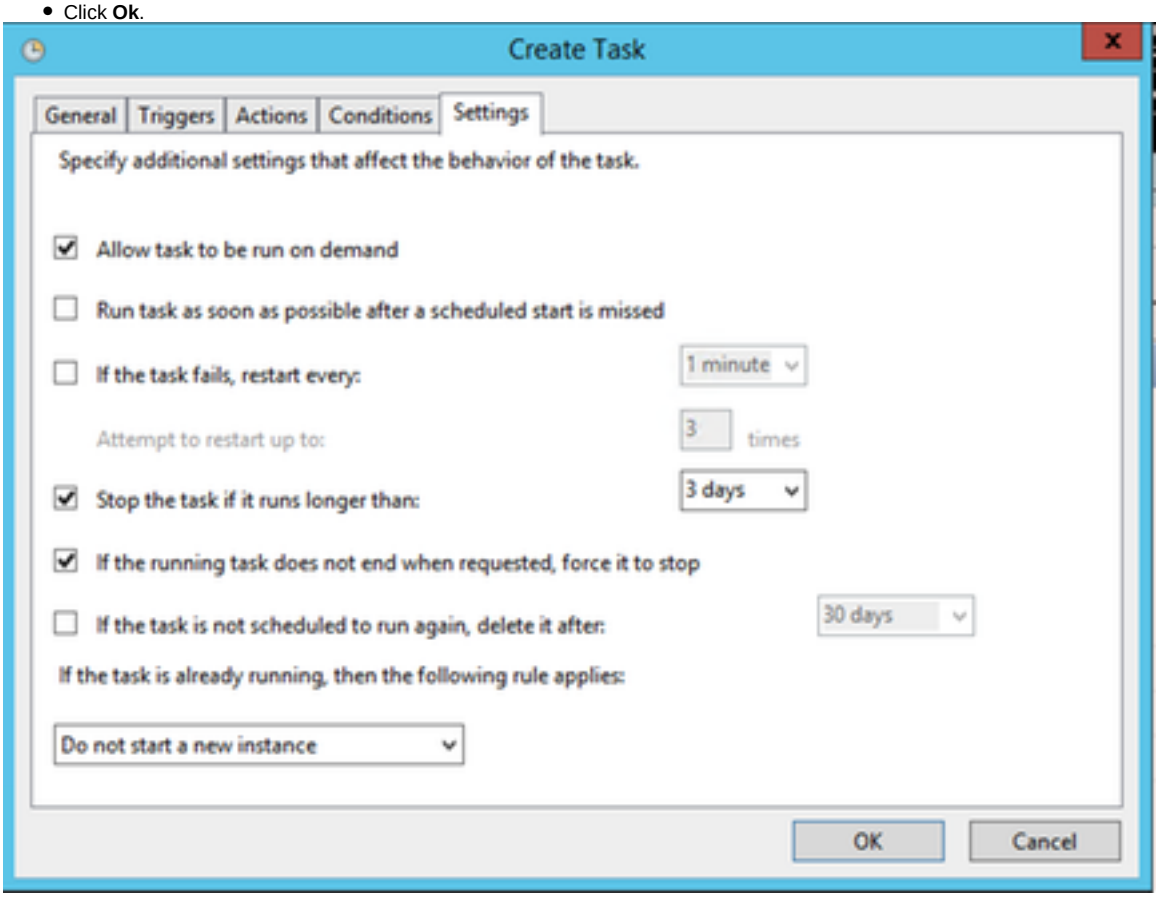
7. *[Optional]* Select the Conditions tab.

   Check the Wake the computer to run this task option.



8 Select the Settings tab.

- Verify that **Do not start a new instance** is selected *under* **If the task is already running.**
- Click **Ok**.



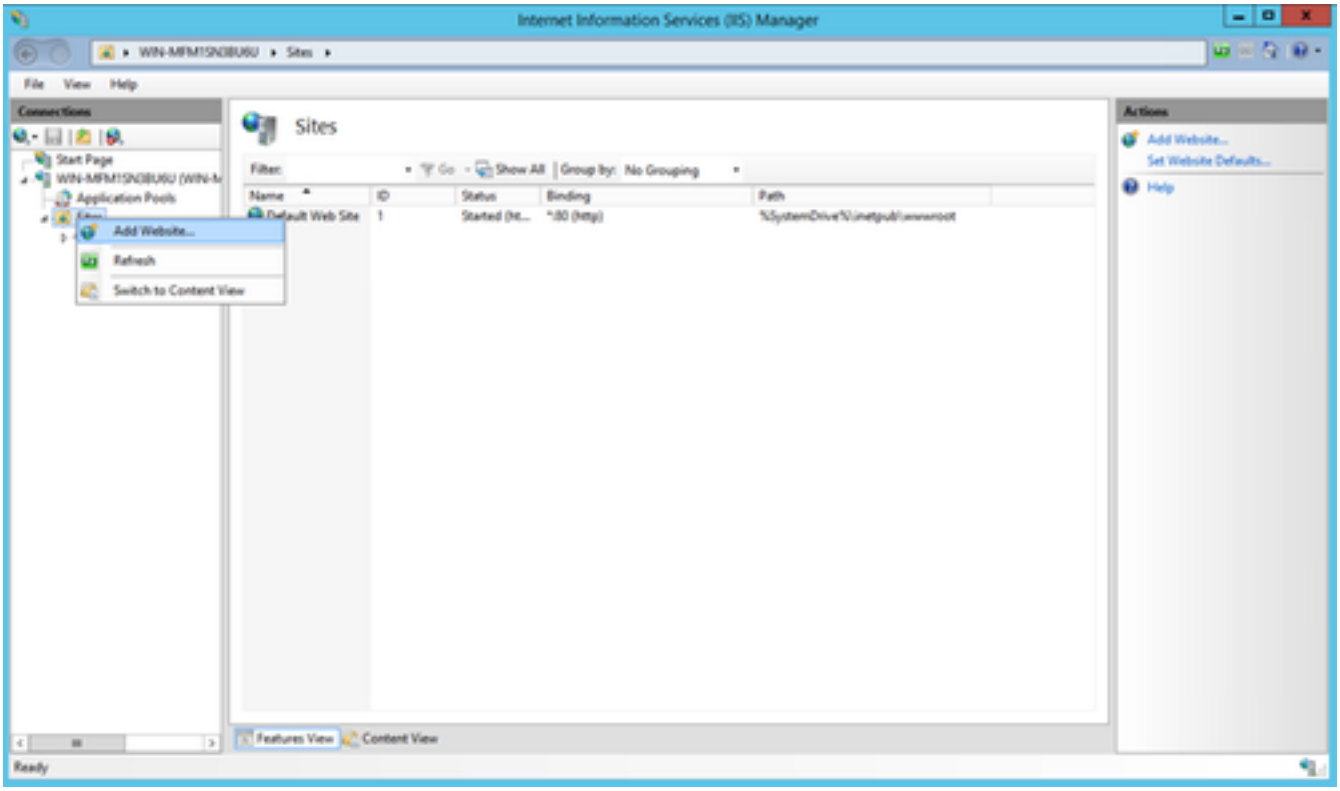
9. Enter the credentials for **the account that will run the task**.

IIS Manager Configuration

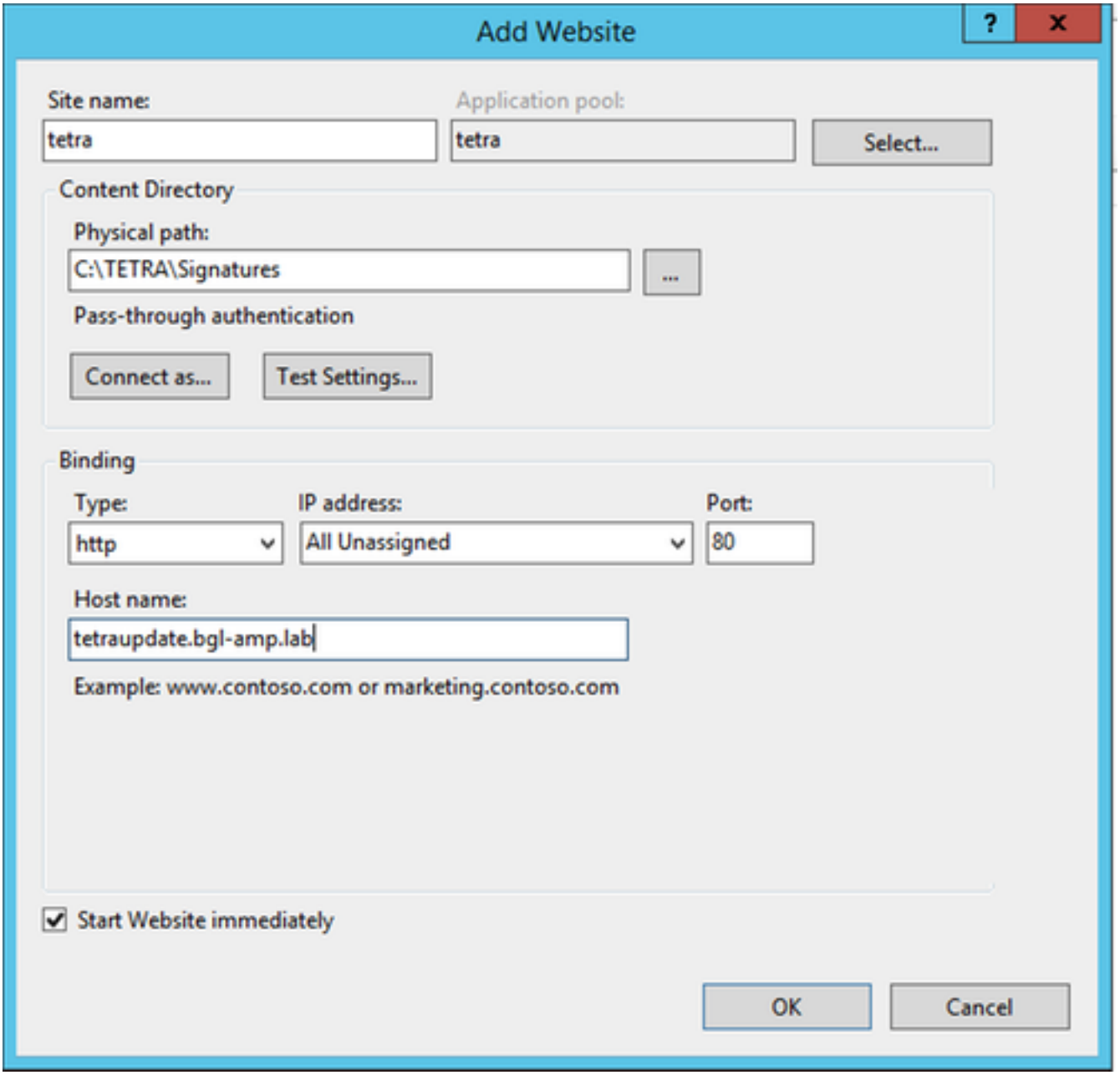
Note: Skip to step 5 when Default Application Pool is configured.

1. Navigate to (IIS) Manager (**Under Server Manager > Tools**)

2. Expand the right-hand column until the **Sites folder** is visible, **Right Click and select Add Website**.



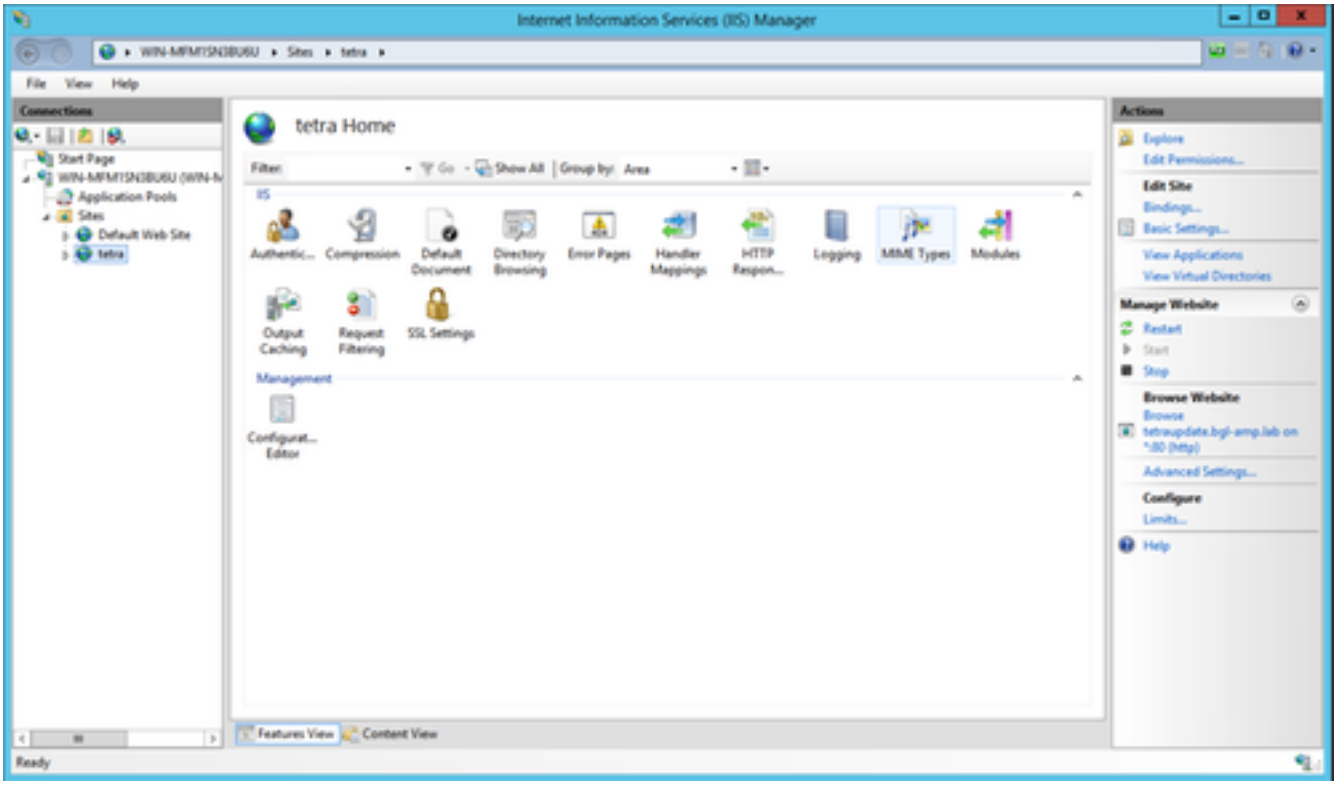
3. Choose a name of choice. For the Physical Path select the ***C:\TETRA\Signatures*** folder where the signatures were downloaded.



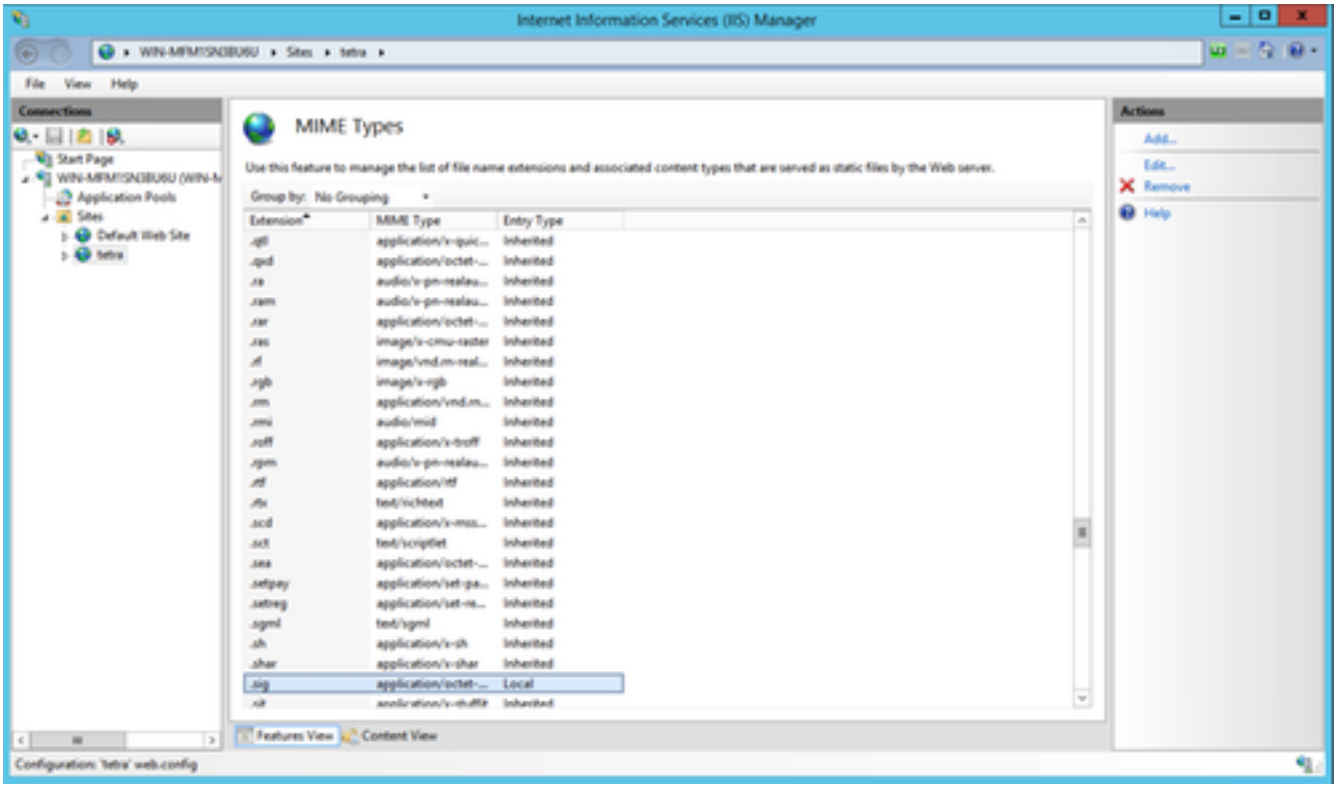
4. Leave Bindings alone. **Configure a separate hostname** and server name, chosen names must be resolvable by clients. This is the URL which you will configure in the policy.

5. Select the site and navigate to **MIME Types** and **add the following MIME Types**:

- .gzip, Application/octet-stream
- .dat, Application/octet-stream
- .id, Application/octet-stream
- .sig, Application/octet-stream



6. Navigate to the **web.config file** (located in the mirror folder), add the following lines to the top of the file.



When finished the *C:\TETRA\Signatures\web.config* file contents will appear as such when viewed in a text editor. (Syntax and spacing need to remain the same as the example provided.)

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
<directoryBrowse enabled="true" showFlags="Extension" />
        <staticContent>
            <mimeMap fileExtension="." mimeType="applicaton/octet-stream" />
```

```
            <mimeMap fileExtension=".gzip" mimeType="applicaton/octet-stream" />
            <mimeMap fileExtension=".dat" mimeType="application/octet-stream" />
            <mimeMap fileExtension=".id" mimeType="application/octet-stream" />
            <mimeMap fileExtension=".sig" mimeType="application/octet-stream" />
        </staticContent>
    </system.webServer>
</configuration>
```

> **Note**: The AMP for Endpoints Connector requires the presence of the Server HTTP Header in the response for proper operation. If the Server HTTP Header has been disabled, the Web server may need additional configuration specified below.

The url-rewrite extension must be installed. Add the following XML snippet to the server configuration at /[MIRROR_DIRECTORY]/web.config:

```
<rewrite>
  <rules>
   <rule name="Rewrite fetch URL">
    <match url="^(.*)_[\d]*\/avx\/(.*)$" />
    <action type="Redirect" url="{R:1}/avx/{R:2}" appendQueryString="false" />
   </rule>
  </rules>
</rewrite>
```

> **Note**: Perform this change manually with a text editor or with the IIS manager by using the URL Rewrite module. The Rewrite module can be installed from the following URL (https://www.iis.net/downloads/microsoft/url-rewrite)

When finished the *C:\TETRA\Signatures\web.config* file contents will appear as such when viewed in a text editor. (Syntax and spacing need to remain the same as the example provided.)

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
<directoryBrowse enabled="true" showFlags="Extension" />
<rewrite>
<rules>
<rule name="Rewrite fetch URL">
<match url="^(.*)_[\d]*\/avx\/(.*)$" />
        <action type="Redirect" url="{R:1}/avx/{R:2}" appendQueryString="false" />
</rule>
</rules>
        </rewrite>
        <staticContent>
            <mimeMap fileExtension="." mimeType="applicaton/octet-stream" />
            <mimeMap fileExtension=".gzip" mimeType="applicaton/octet-stream" />
            <mimeMap fileExtension=".dat" mimeType="application/octet-stream" />
            <mimeMap fileExtension=".id" mimeType="application/octet-stream" />
            <mimeMap fileExtension=".sig" mimeType="application/octet-stream" />
        </staticContent>
    </system.webServer>
</configuration>
```

Apache / Nginx

> **Note**: The steps provided assumes you are serving the signatures from the default directory of the web hosting software.

1. **Create a new folder** on your *root* drive named **TETRA.**
2. **Unzip** the downloaded scripts package in this folder.
3. Run the command ***Chmod +x update-linux**** to give the scripts executable permission.
4. Run the command to fetch the TETRA update files.

sudo ./update-linux-x86-64 fetch --config config.xml --once --mirror /var/www/html/:

This command may vary depending on your directory structure.

5. To automate the server's update process, add a cron job to the server:

0 * * * * /TETRA/update*-linux-*x86-64 fetch --config /TETRA/config.xml --once --mirror /var/www/html/

6. Continue to follow the steps under **Policy configuration** in order to configure your policy to use the Update server.

Policy configuration

1. Navigate to the policy to use the Update Server and under ***Advanced Settings > TETRA*** select: Checkbox for Local AMP Update ServerThe hostname or IP for the update server in the format of <hostname.domain.root> or IP address.

Caution: Do not include any protocols before or any subdirectories after otherwise, this will result in an error while downloading.

[Optional] Checkbox **Use HTTPS for TETRA Definitin Updates:** if the local server is configured with a proper certificate and for the connectors to use HTTPS.

Verification

Navigate to the **C:\inetpub\wwwroot\, C:\TETRA\Signature,** or **/var/www/html directory** and verify the updated signatures are visible, the signatures are downloaded from the server to the end client by either waiting until the next sync cycle or manually deleting the existing signatures and then waiting for the signatures to download. The default is a 1-hour interval to check for an update.

Related Information

- **Technical Support & Documentation - Cisco Systems**
- **Cisco AMP for Endpoints - TechNotes**
- **Cisco AMP for Endpoints - User Guide**

.