Konfigurationsschritte für den AMP-Aktualisierungsserver

Inhalt

Einführung

Dieses Dokument beschreibt detaillierte Konfigurationsschritte für den TETRA Update Server (AMP) von Cisco Advanced Malware Protection.

Voraussetzungen

- Kenntnis von Server-Hosts wie Windows 2012R2 oder CentOS 6.9 x86_64.
- Kenntnisse über Hostingsoftware wie IIS (nur Windows), Apache, Nginx
- Konfigurierte Server-Hosts mit aktiviertem HTTPS, gültiges vertrauenswürdiges Zertifikat installiert.
- Option für lokalen HTTPS-Aktualisierungsserver konfiguriert.

Hinweis: Ausführliche Informationen zur Aktivierung der Konfiguration und der Anforderungen des lokalen Update-Servers finden Sie in Kapitel 25 des Benutzerhandbuchs zu AMP für Endgeräte, das hier verfügbar ist. (https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf)

Hinweis: Server-Hosts (IIS, Apache, Nginx) sind Drittanbieterprodukte und werden von Cisco nicht unterstützt. Bei Fragen, die über die angegebenen Schritte hinausgehen, wenden Sie sich bitte an die Support-Teams für die jeweiligen Produkte.

Warnung: Wenn AMP mit einem Proxy-Server konfiguriert ist, wird der gesamte Aktualisierungsdatenverkehr (einschließlich TETRA) weiterhin über den Proxyserver an den lokalen Server gesendet. Stellen Sie sicher, dass der Datenverkehr während der Übertragung den Proxy ohne Änderungen passieren darf.

Installationsschritte

Alle Plattformen

1. Bestätigen Sie das Betriebssystem des Hostservers.
2. Bestätigen Sie Ihr AMP für Endpoints-Dashboard-Portal, laden Sie das Updater-Softwarepaket und die Konfigurationsdatei herunter.

AMP für Endgeräte-Konsole:

USA - 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

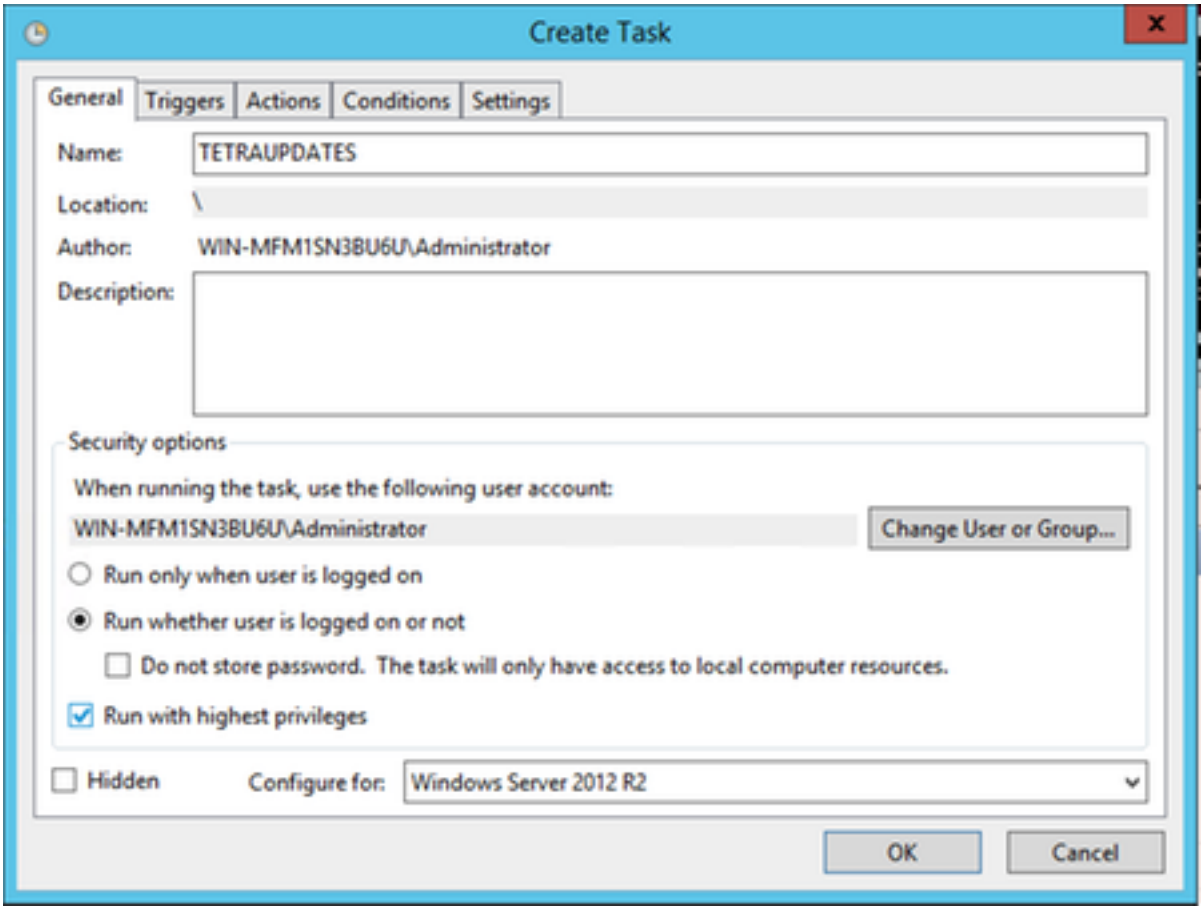
> **Hinweis**: Die folgenden Schritte basieren auf dem neuen IIS-Anwendungspool zum Hosten der Signaturen, **nicht** auf dem Standardanwendungspool. Um den Standardpool zu verwenden, ändern Sie den Ordner **—spiegeln** in den angegebenen Schritten, um den Standardpfad für das Webhosting wiederzugeben (**C:\inetpub\wwwroot**).

Verzeichniserstellung

1. Erstellen Sie einen neuen Ordner auf dem Root-Laufwerk, nennen Sie ihn **TETRA**.
2. Kopieren Sie das gezippte AMP-Aktualisierungspaket und die Konfigurationsdatei in den erstellten **TETRA-**Ordner.
3. Entpacken Sie das Softwarepaket in diesem Ordner.
4. Erstellen Sie einen neuen Ordner mit dem Namen **Signaturen** im TETRA-Ordner.

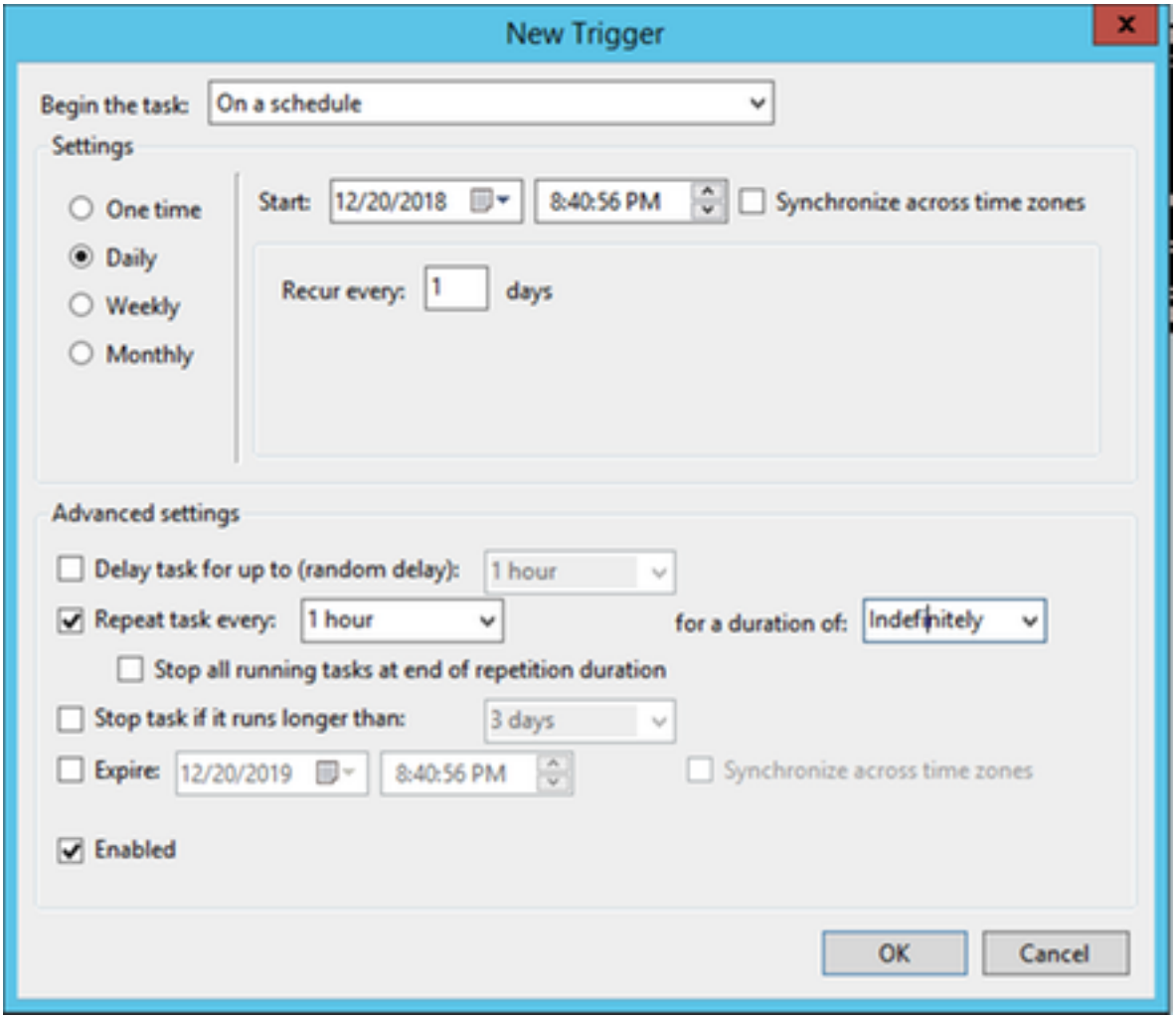
Task-Erstellung aktualisieren

1. Öffnen Sie die Befehlszeile, und navigieren Sie zum *C:\TETRA* Ordner.***cd C:\TETRA.***
2. Führen Sie den Befehl ***update-win-x86-64.exe fetch —config="C:\TETRA\config.xml" —once —spiegelt C:\TETRA\Signatures aus.***
3. Öffnen Sie den Taskplaner, und erstellen Sie eine neue Aufgabe. (Aktion > Aufgabe erstellen), um die Aktualisierungssoftware bei Bedarf automatisch mit den folgenden Optionen auszuführen:
4. Wählen Sie die Registerkarte Allgemein. Geben Sie einen Namen für die Aufgabe ein.Wählen Sie **Ausführen aus, ob ein Benutzer angemeldet ist oder nicht**.Wählen Sie **Mit den höchsten Berechtigungen ausführen aus.**Wählen Sie **das Betriebssystem** aus dem Dropdown-Menü **Konfigurieren aus.**



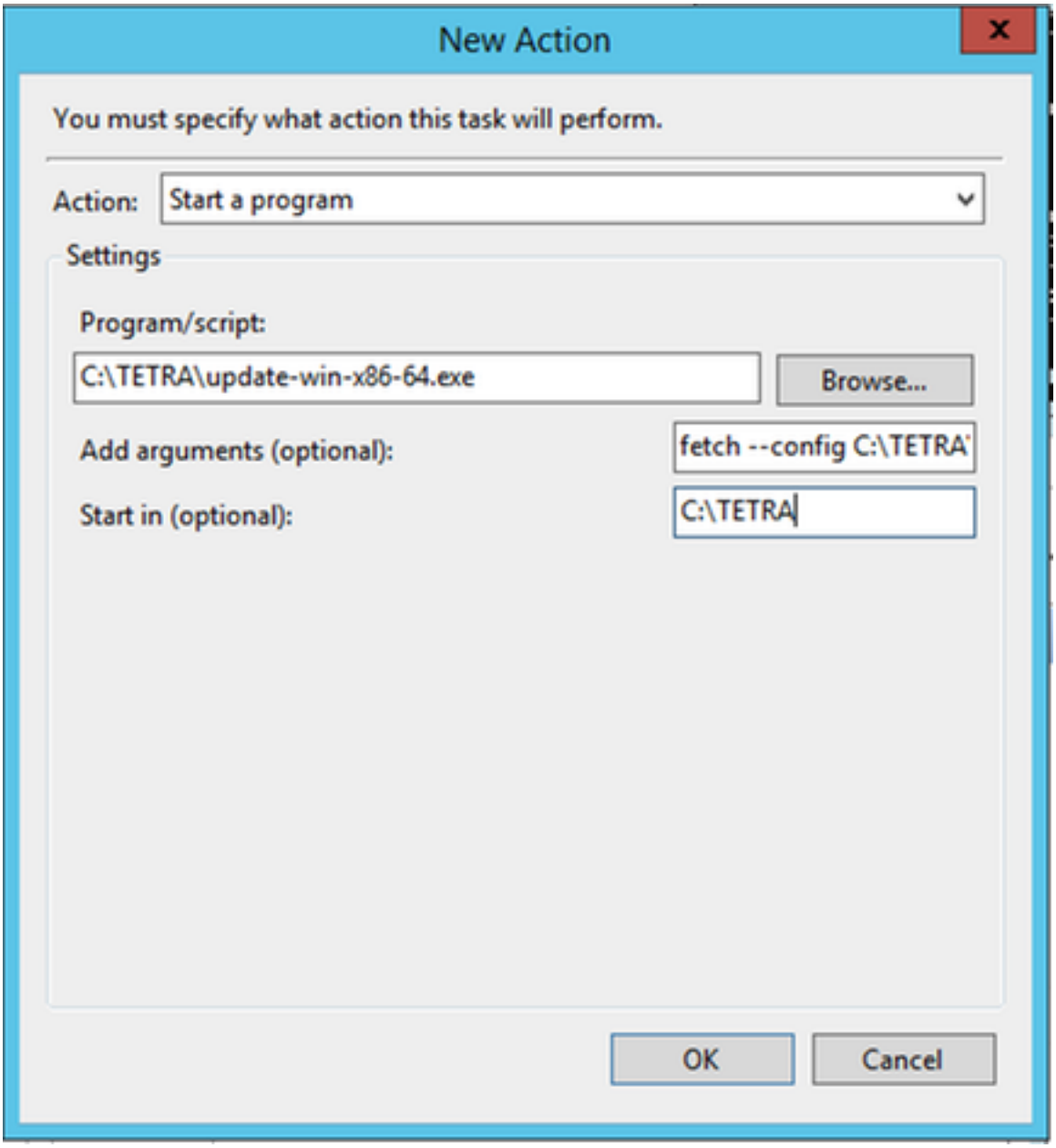
5. Wählen Sie die Registerkarte Trigger aus.

- Klicken Sie auf Neu.
- Wählen Sie **In einem Zeitplan** aus dem Dropdown-Menü **Aufgabe starten aus**.
- Wählen Sie **Täglich** unter Einstellungen aus.
- Aktivieren Sie **Task alle wiederholen**, **wählen Sie** aus dem Dropdown-Menü eine **Stunde** aus, und wählen Sie **Unbegrenzt** aus der Option **"für eine Dauer von:" aus.**
- Stellen Sie sicher, dass **Enabled (Aktiviert) aktiviert** ist.
- Klicken Sie auf **OK**.



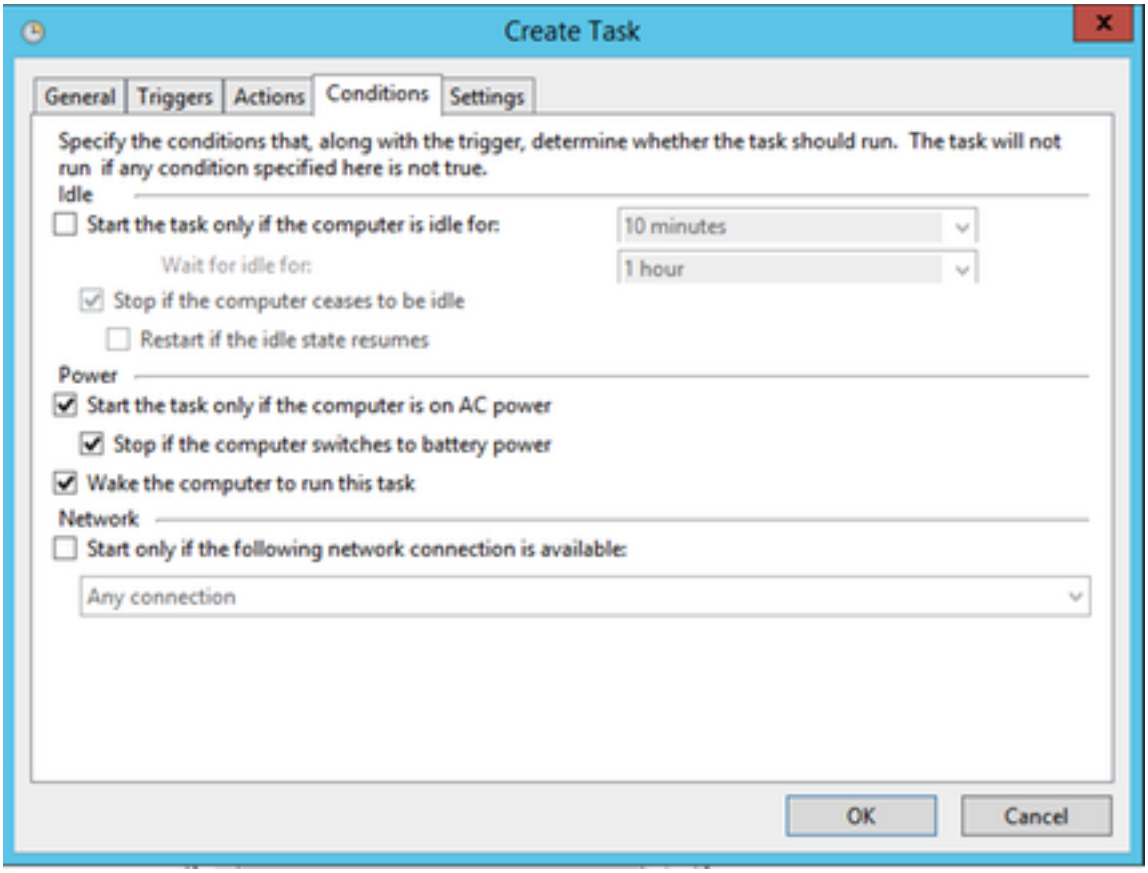
6. Registerkarte Aktionen auswählen

- Klicken Sie auf **Neu**.
- Wählen Sie **im** Dropdown-Menü **Aktion** die Option **Programm starten aus**.
- Geben Sie ***C:\TETRA\update-win-x86-64.exe*** in das Feld **Programm/Skript ein**.
- Geben Sie ***fetch —config C:\TETRA\config.xml —once —spiegeln C:\TETRA\Signatures*** im Feld **Argumente hinzufügen ein**.
- Geben Sie ***C:\TETRA*** in das Feld **Start** ein.
- Klicken Sie auf **OK**



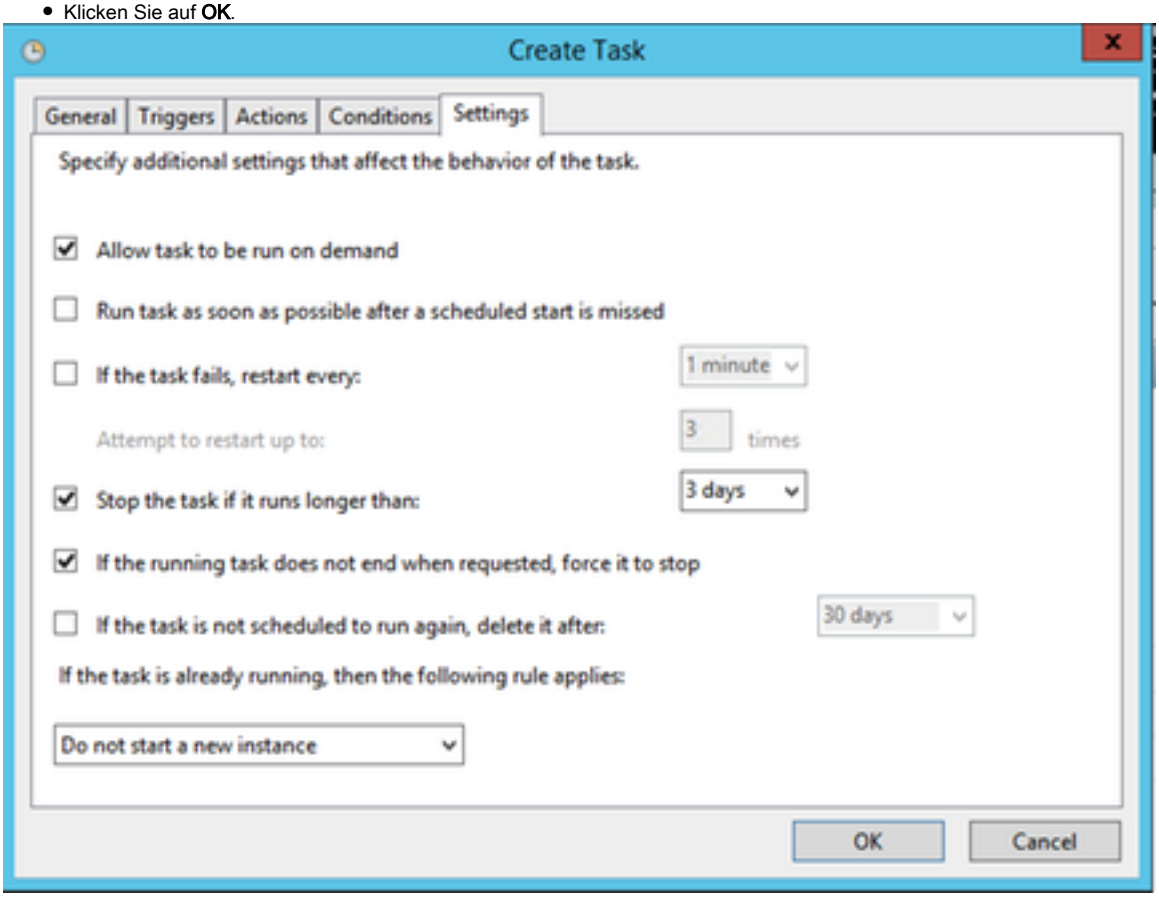
7. *[Optional]* Registerkarte Bedingungen auswählen.

   Aktivieren Sie die Option Computer zum Ausführen dieser Aufgabe aktivieren.



8 Wählen Sie die Registerkarte Einstellungen.

- Vergewissern Sie sich, dass **Sie keine neue Instanz starten** aktiviert ist *unter* **Wenn die Aufgabe bereits ausgeführt wird.**
- Klicken Sie auf **OK**.



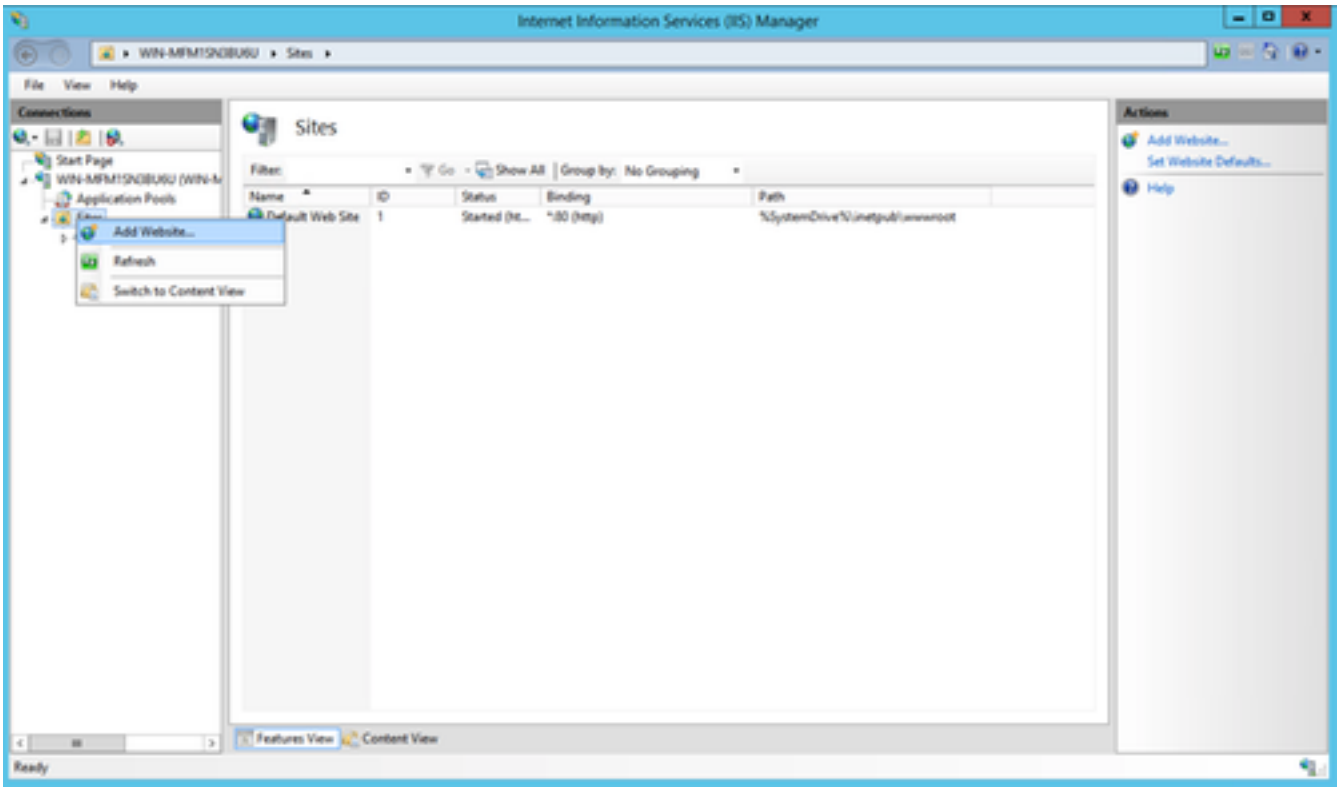
9. Geben Sie die Anmeldeinformationen für **das Konto ein, das die Aufgabe ausführen soll**.

IIS-Manager-Konfiguration

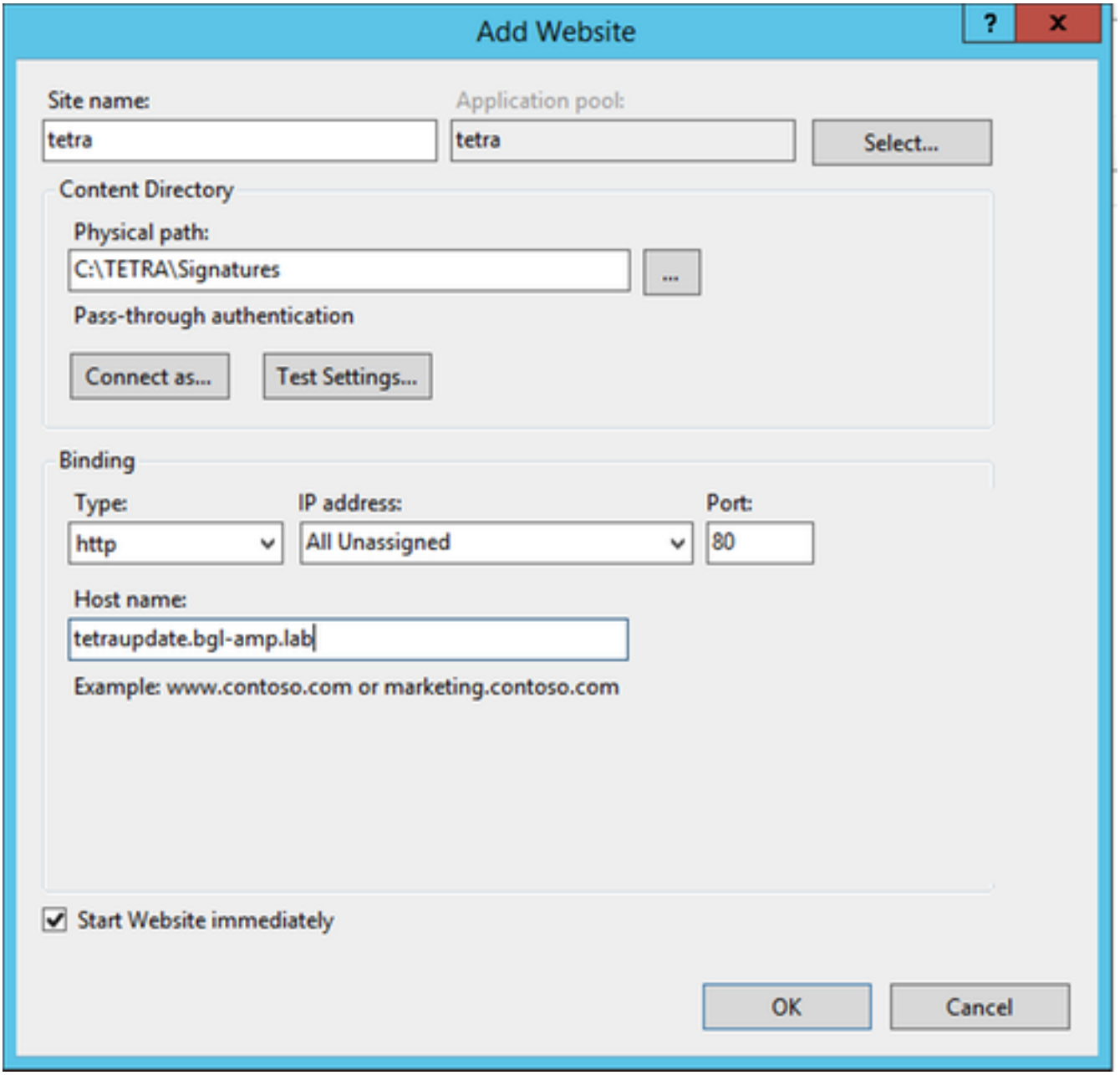
Hinweis: Fahren Sie mit Schritt 5 fort, wenn der Standard-Anwendungspool konfiguriert wurde.

1. Navigieren Sie zum (IIS)-Manager (**Unter Server Manager > Tools**).

2. Erweitern Sie die rechte Spalte, bis der **Ordner Sites** angezeigt wird, **klicken Sie mit der rechten Maustaste, und wählen Sie Website hinzufügen aus**.



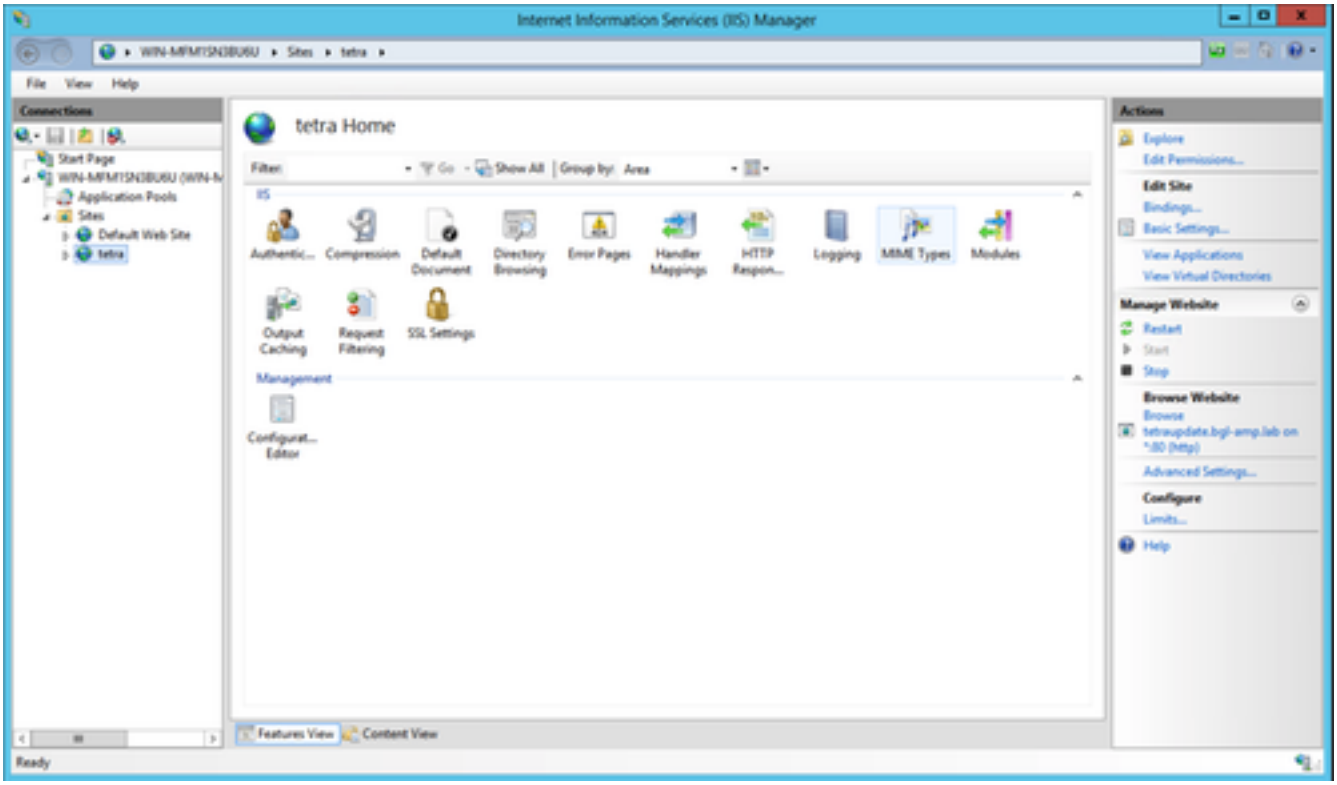
3. Wählen Sie einen gewünschten Namen aus. Wählen Sie für Physical Path den Ordner *C:\TETRA\Signatures* aus, in dem die Signaturen heruntergeladen wurden.



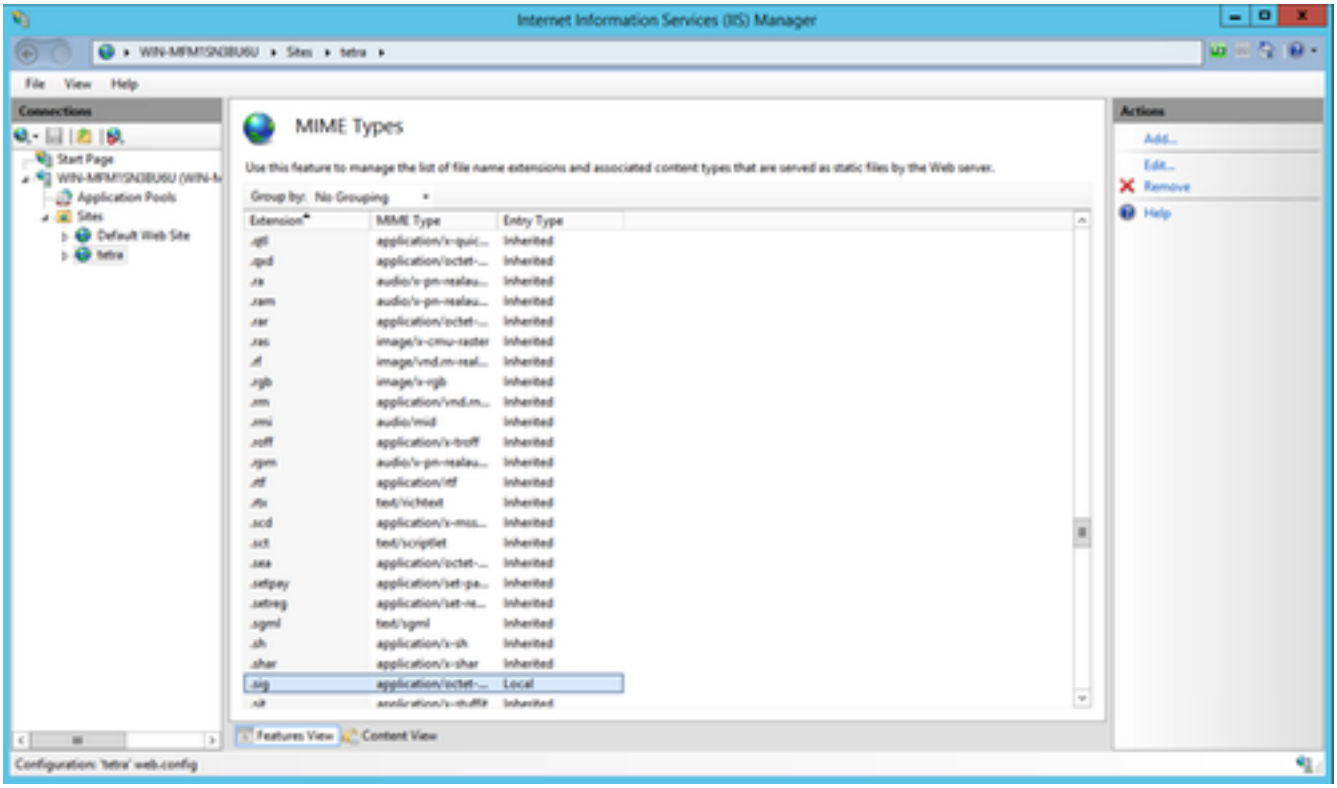
4. Lassen Sie Bindungen allein. **Konfigurieren Sie einen separaten Hostnamen** und einen separaten Servernamen. Ausgewählte Namen müssen von Clients auflösbar sein. Dies ist die URL, die Sie in der Richtlinie konfigurieren werden.

5. Wählen Sie die Site aus, navigieren Sie zu **MIME Types**, und **fügen Sie die folgenden MIME-Typen hinzu**:

- .gzip, Anwendung/Oktett-Stream
- .dat, Anwendung/Oktett-Stream
- .id, Application/Oktett-Stream
- .sig, Application/Oktett-Stream



6. Navigieren Sie zur **Datei web.config** (im Ordner spiegeln), und fügen Sie die folgenden Zeilen am Anfang der Datei hinzu.



Nach Beendigung wird der *C:\TETRA\Signatures\web.config*-Dateiinhalt als solcher angezeigt, wenn er in einem Texteditor angezeigt wird. (Syntax und Abstand müssen mit dem angegebenen Beispiel übereinstimmen.)

Hinweis: Der AMP für Endpoints-Connector benötigt für den ordnungsgemäßen Betrieb das Vorhandensein des Server-HTTP-Headers in der Antwort. Wenn der Server-HTTP-Header deaktiviert wurde, benötigt der Webserver möglicherweise eine zusätzliche Konfiguration, die unten angegeben ist.

Die Erweiterung url-rewrite muss installiert werden. Fügen Sie der Serverkonfiguration unter /[MIRROR_DIRECTORY]/web.config den folgenden XML-Ausschnitt hinzu:

```
<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>
```

Hinweis: Führen Sie diese Änderung manuell mit einem Text-Editor oder mit dem IIS-Manager durch, indem Sie das Modul URL Rewrite verwenden. Das Rewrite-Modul kann über die folgende URL installiert werden (https://www.iis.net/downloads/microsoft/url-rewrite):

Nach Beendigung wird der *C:\TETRA\Signatures\web.config*-Dateiinhalt als solcher angezeigt, wenn er in einem Texteditor angezeigt wird. (Syntax und Abstand müssen mit dem angegebenen Beispiel übereinstimmen.)

Apache/Nginx

Hinweis: Bei den angegebenen Schritten wird davon ausgegangen, dass Sie die Signaturen aus dem Standardverzeichnis der Webhosting-Software bereitstellen.

1. **Erstellen Sie einen neuen Ordner** auf Ihrem *Stammlaufwerk* mit dem Namen **TETRA.**
2. **Entpacken Sie** das heruntergeladene Skriptpaket in diesem Ordner.
3. Führen Sie den Befehl ***Chmod +x update-linux**** aus, um die ausführbare Berechtigung der Skripte zu erhalten.
4. Führen Sie den Befehl aus, um die TETRA-Aktualisierungsdateien abzurufen.

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

This command may vary depending on your directory structure.

5. Um den Aktualisierungsprozess des Servers zu automatisieren, fügen Sie dem Server einen Cron-Auftrag hinzu:

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

6. Fahren Sie mit den Schritten unter **Richtlinienkonfiguration fort**, um Ihre Richtlinie für die Verwendung des Aktualisierungsservers zu konfigurieren.

Richtlinienkonfiguration

1. Navigieren Sie zur Richtlinie, um den Aktualisierungsserver zu verwenden, und wählen Sie unter ***Erweiterte Einstellungen > TETRA*** folgende Option aus: Kontrollkästchen für lokalen AMP-AktualisierungsserverDer Hostname oder die IP-Adresse für den Aktualisierungsserver im Format <hostname.domain.root> oder IP-Adresse.

Vorsicht: Schließen Sie keine Protokolle vor oder Unterverzeichnisse nach anderen, das führt zu einem Fehler beim Herunterladen.

[Optional] Kontrollkästchen **HTTPS für Aktualisierungen der TETRA-Definition verwenden:** wenn der lokale Server mit einem entsprechenden Zertifikat konfiguriert ist und die Verbindungen HTTPS verwenden.

Überprüfung

Navigieren Sie zum Verzeichnis C:\inetpub\wwwroot\, C:\TETRA\Signature oder /var/www/html, und überprüfen Sie, ob die aktualisierten Signaturen sichtbar sind. Die Signaturen werden vom Server auf den Endclient heruntergeladen, indem Sie entweder auf den nächsten Synchronisierungszyklus warten oder die vorhandenen Signaturen manuell löschen und dann auf den Download der Signaturen warten. Der Standardwert ist ein 1-Stunden-Intervall, in dem nach einer Aktualisierung gesucht wird.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems
- Cisco AMP für Endgeräte - Technische Hinweise
- Cisco AMP für Endgeräte - Benutzerhandbuch

.