

# Der Cisco FirePOWER User Agent Database Service wird nach Anhalten nicht neu gestartet.

## Inhalt

[Einführung](#)

[Symptome](#)

[Lösung](#)

[Referenzen](#)

## Einführung

Ein Cisco User Agent kann den Microsoft Active Directory (AD)-Server überwachen und Anmelde- und Abmeldeaktivitäten melden, die von einem LDAP-Server authentifiziert werden. Ein FirePOWER Management Center (FMC) integriert diese Aktivitäten mit den von einem FirePOWER verwalteten Gerät gesammelten Sicherheitsereignissen. Dieses Dokument bietet eine Lösung für ein Problem, wenn der Benutzer-Agent nach dem Beenden des Dienstes nicht startet.

## Symptome

Sie können die Lösung für dieses Dokument verwenden, wenn Sie die folgenden Symptome bei Ihrem Benutzer-Agent-Dienst bemerken:

- Die Benutzeroberfläche des Benutzeragenten zeigt an, dass der Dienst nicht ausgeführt wird.
- In der Windows-Dienstkonsole, services.msc, wird der Cisco Benutzer-Agent-Status als leer angezeigt, und der Dienst kann nicht gestartet werden.
- Das Windows-Ereignisprotokoll zeigt einen Fehler an, der dem Beispiel "Die Vertrauensbeziehung zwischen der primären Domäne und der vertrauenswürdigen Domäne ist fehlgeschlagen" ähnelt.
- Eine Datei UserEncryptionBytes.bin wird unter C:\ mit 0 Byte Größe erstellt.
- Der Debug-Modus eines User Agent-Clients zeigt die folgenden Fehlermeldungen auf der Registerkarte Log (Protokoll) des User Agent an:

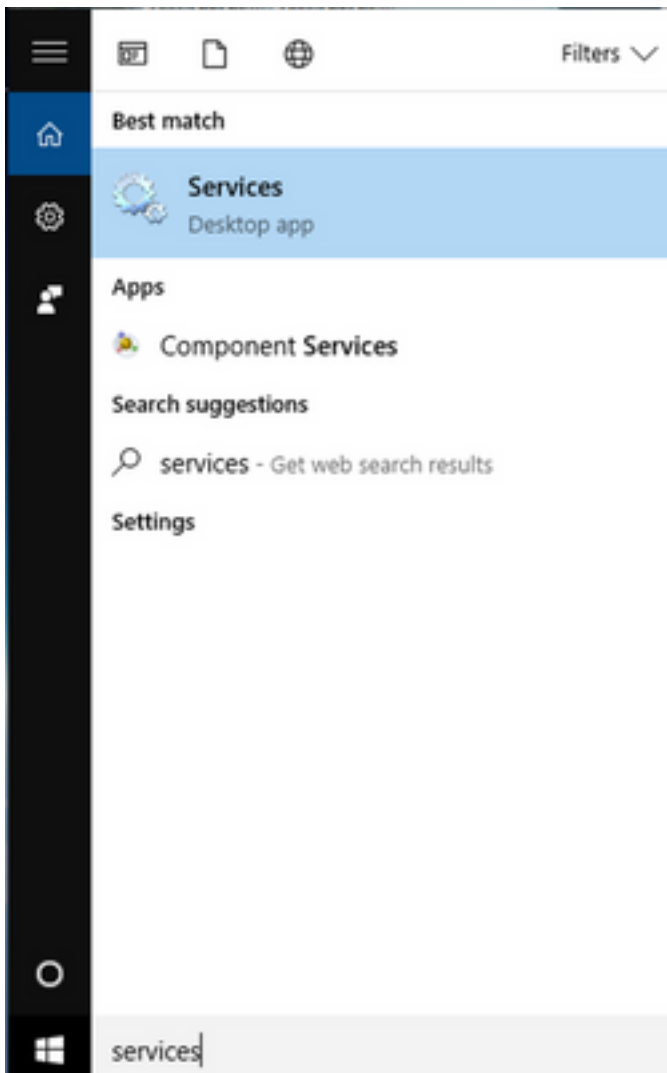
```
, "debug", "[0102] - An error occurred while fetching encryption bytes from  
'C:\UserAgentEncryptionBytes.bin':  
The trust relationship between the primary domain and the trusted domain failed.."
```

```
, "error", "[0102] - An error occurred while fetching encryption bytes from  
'C:\UserAgentEncryptionBytes.bin':  
Specified key is not a valid size for this algorithm.."
```

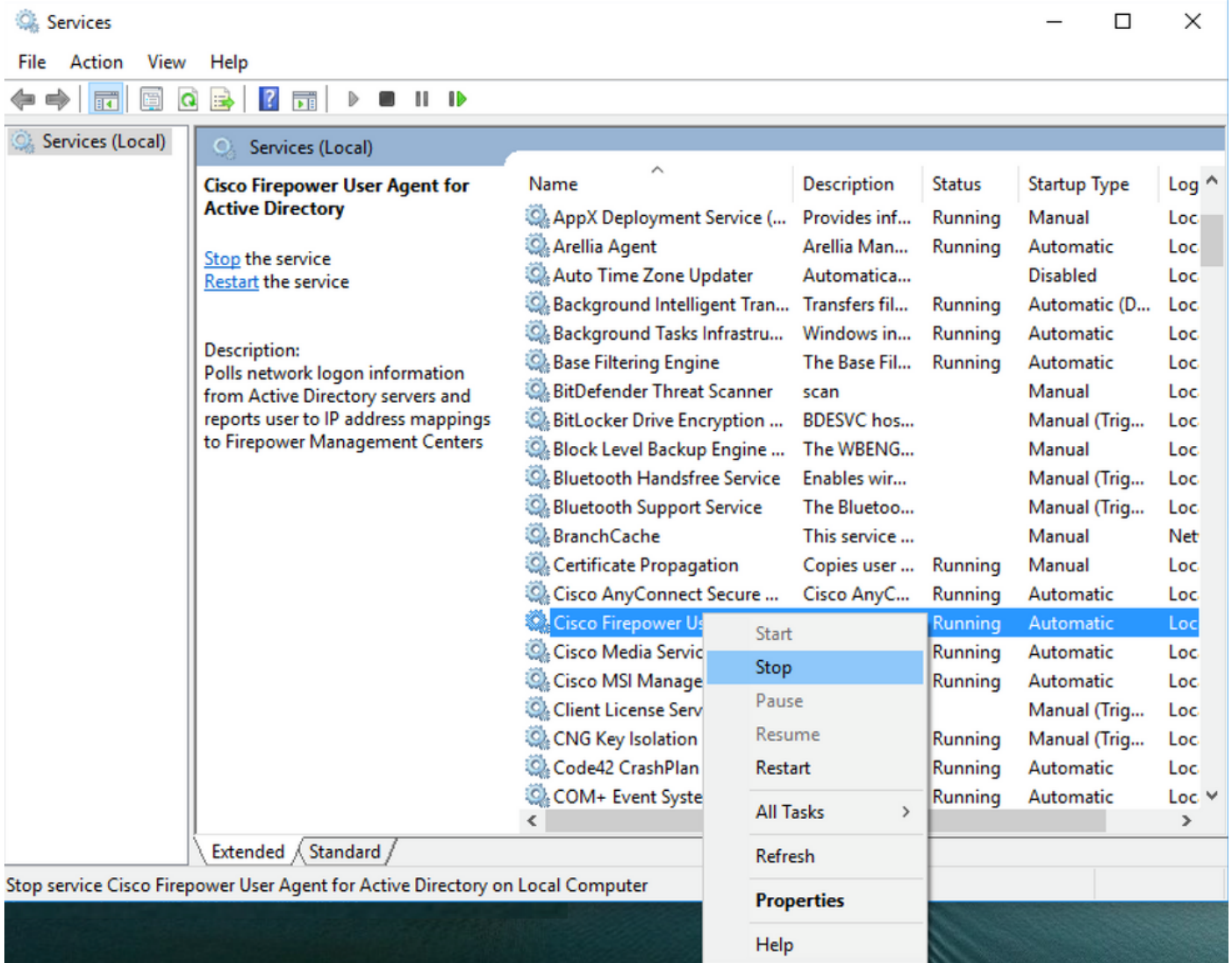
```
, "error", "[0002] - Error connecting to 10.85.3.122: System.UnauthorizedAccessException:  
Access is denied. (Exception from HRESULT: 0x80070005 (E_ACCESSDENIED))
```

## Lösung

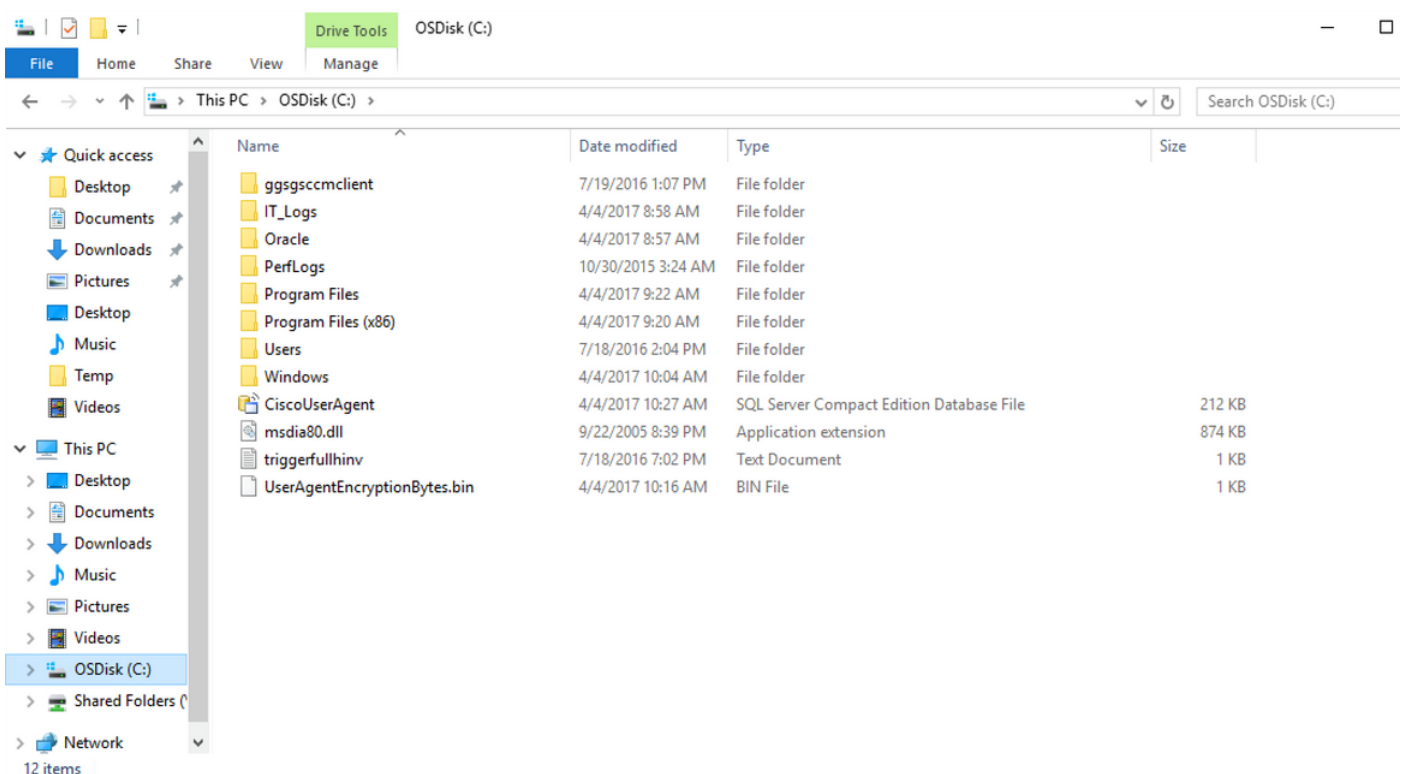
**Schritt 1:** Führen Sie die Microsoft Windows Services Console, services.msc, aus. Sie können einen Windows-Dienst deaktivieren oder aktivieren.



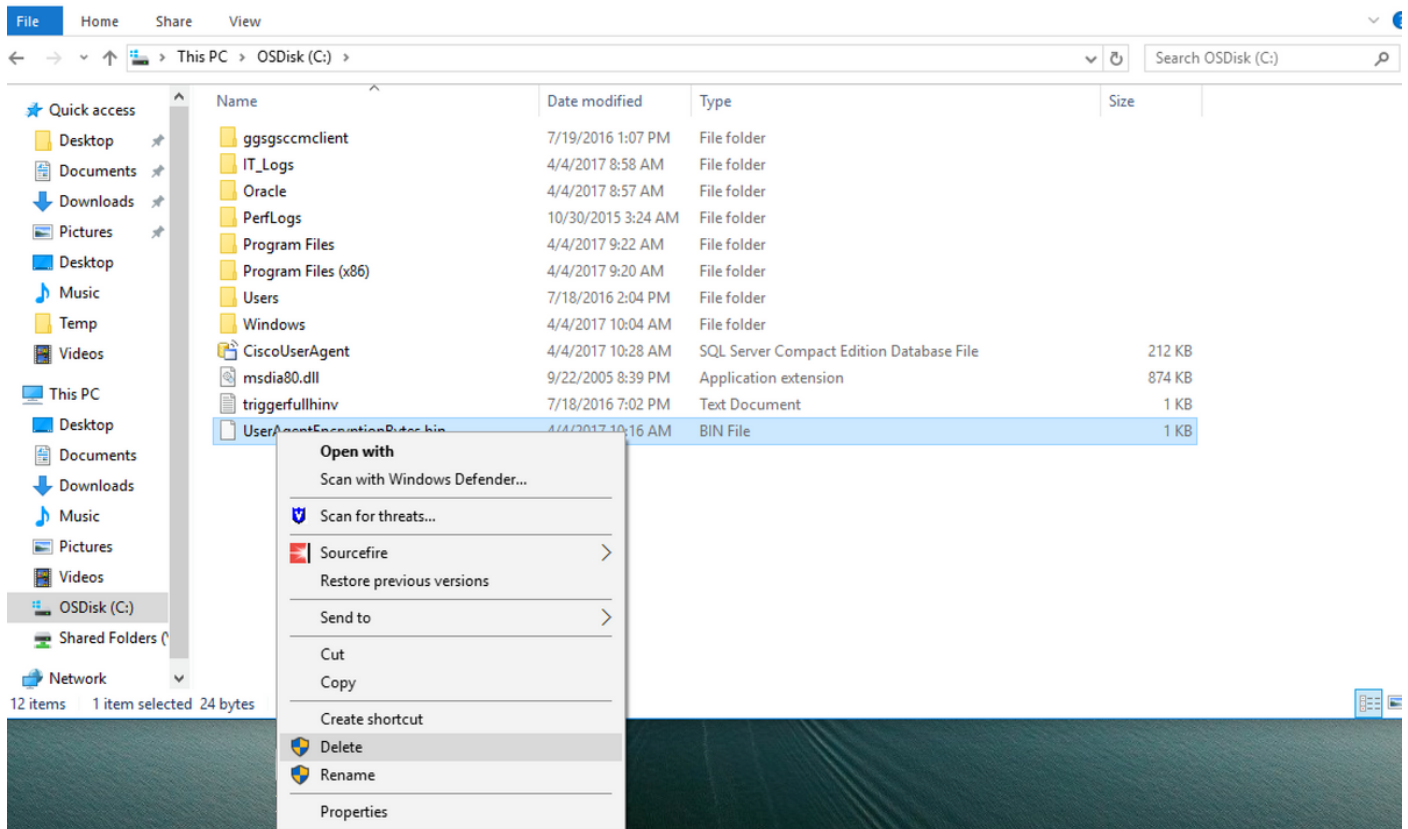
**Schritt 2:** Klicken Sie mit der rechten Maustaste auf den Cisco User Agent-Dienst, und wählen Sie **Stopp** aus, um den Dienst zu beenden.



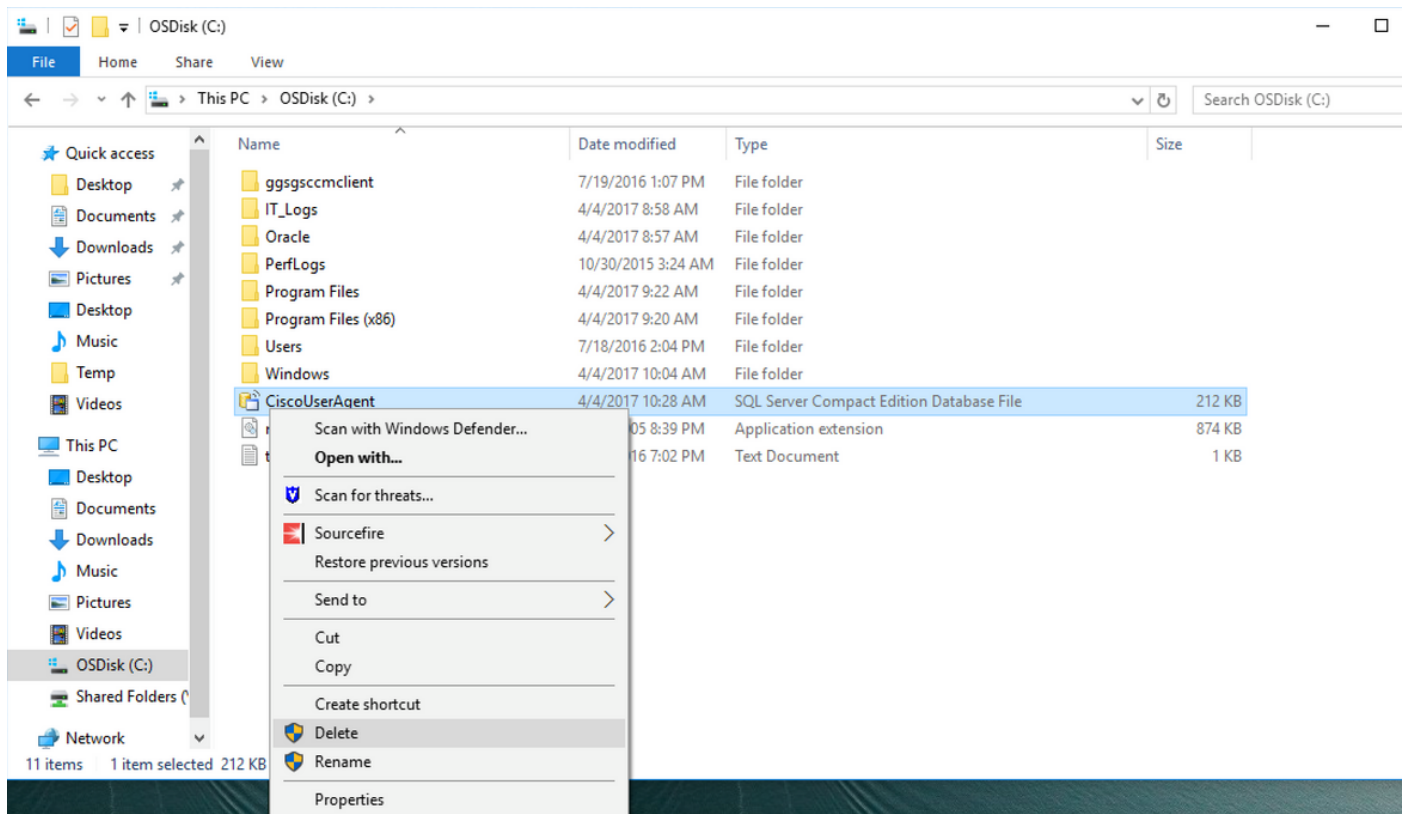
### Schritt 3: Navigieren Sie zu C: Laufwerk.



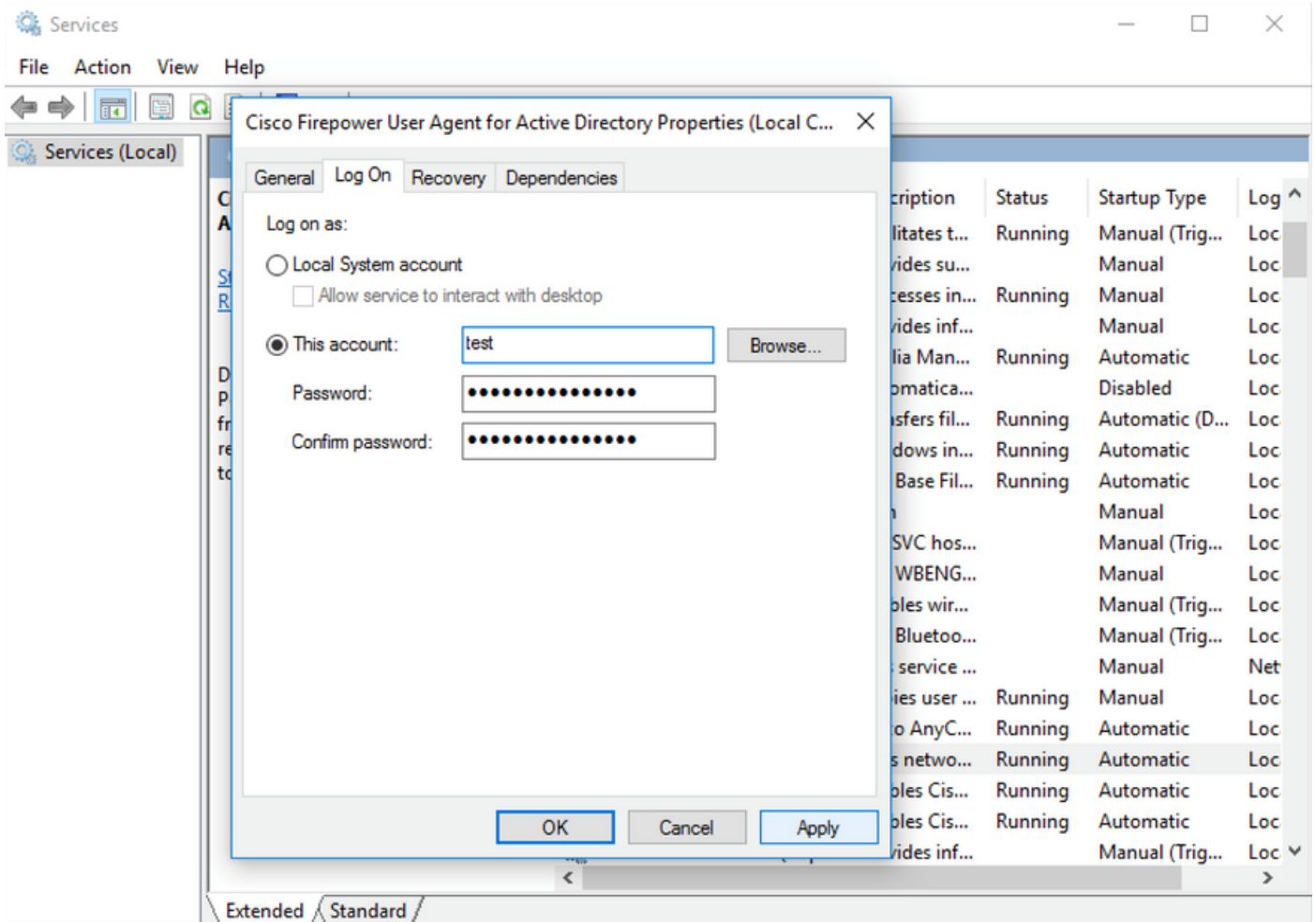
#### Schritt 4: Löschen Sie diese UserAgentEncryptionBytes.bin-Datei.



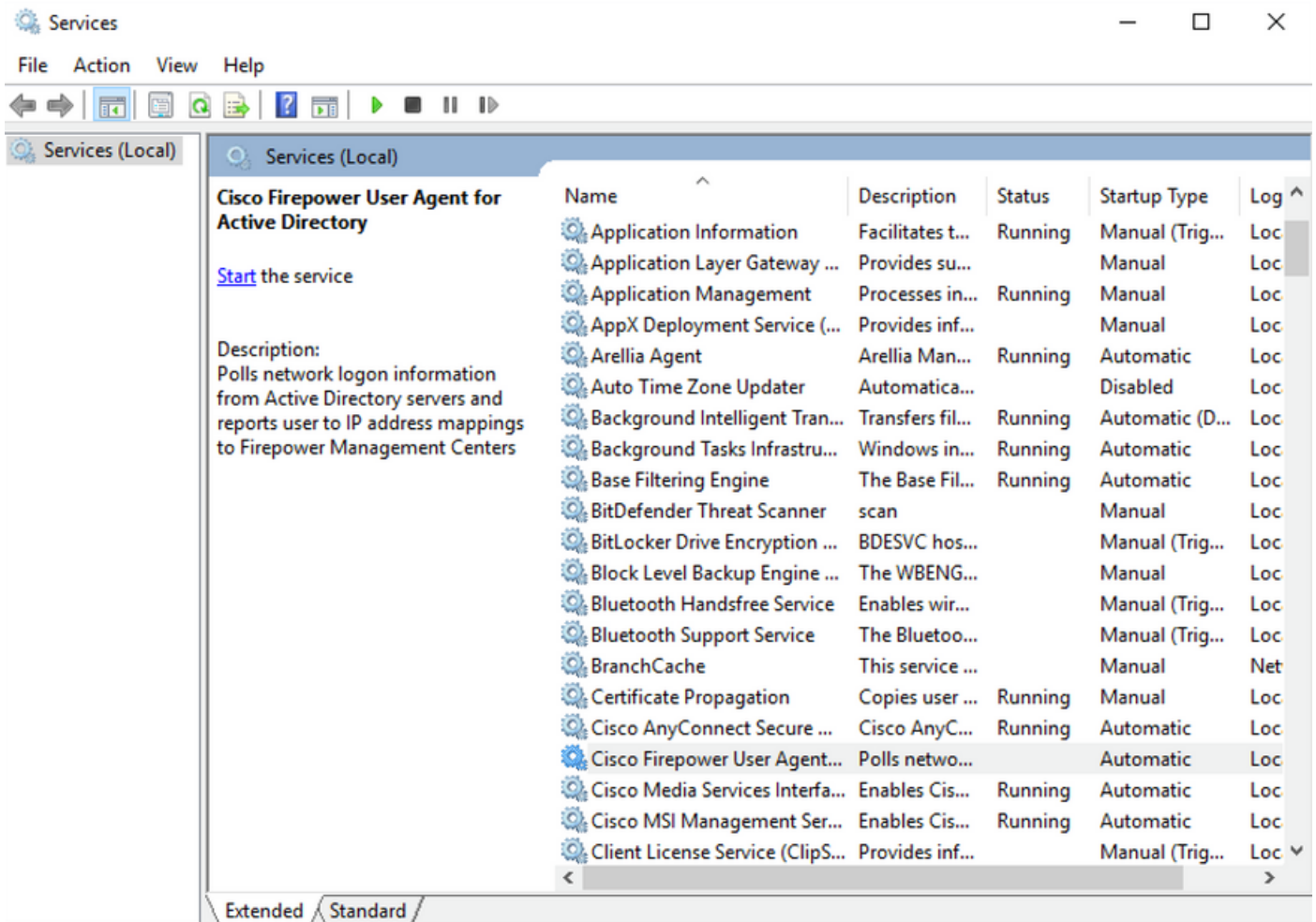
#### Schritt 5: Löschen Sie die CiscoUserAgent-Datei, die eine SQL Server Compact Edition-Datenbankdatei ist.



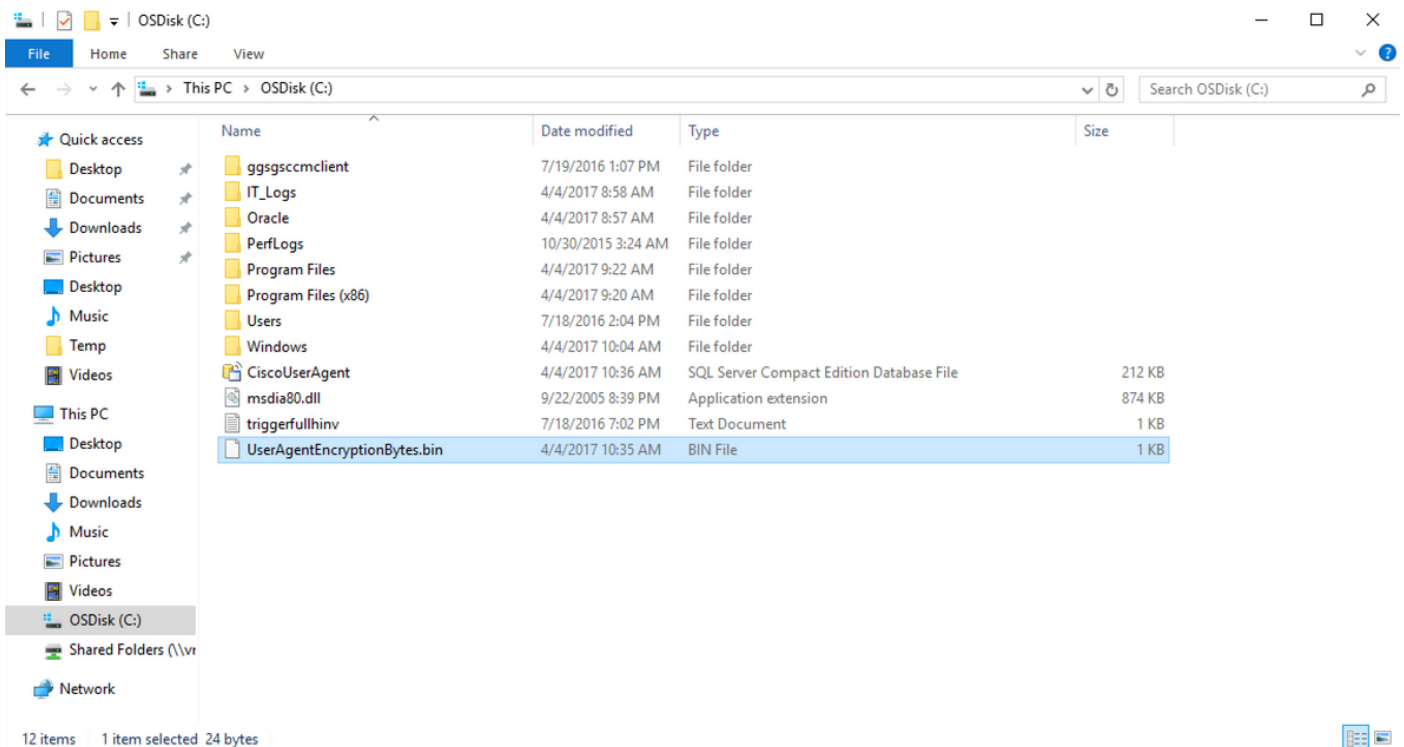
#### Schritt 6: Wechseln Sie zurück zu services.msc. Klicken Sie mit der rechten Maustaste auf den Cisco User Agent-Dienst, wählen Sie **Eigenschaften aus**, wählen Sie dann die Registerkarte **Anmelden** aus, und konfigurieren Sie einen Benutzer als AD-Benutzeranmeldung. Klicken Sie abschließend auf **Übernehmen**.



**Schritt 7:** Klicken Sie in services.msc auf **Start** für den **Cisco Firepower User Agent** für den Active Directory-Dienst.

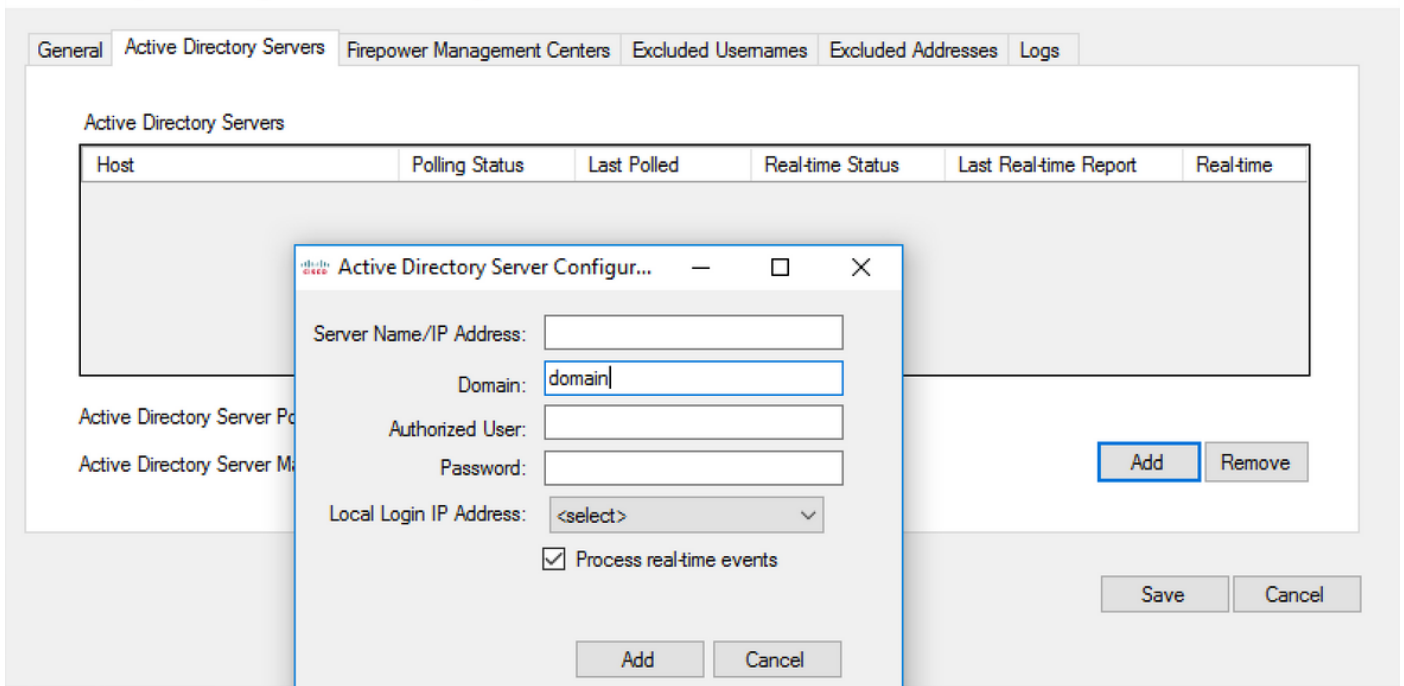


**Schritt 8:** Überprüfen Sie die Größe der Datei UserAgentEncryptionBytes.bin. Der Wert darf nicht 0 KB sein.



**Schritt 9:** Fügen Sie die Domänencontroller und das FirePOWER Management Center dem Benutzer Agent Client hinzu. Stellen Sie sicher, dass Sie die Domänencontroller/den lokalen Host hinzufügen, bevor Sie das Firepower Management Center dem Benutzer-Agent hinzufügen.





## Referenzen

- [Konfigurationsanleitung für Firepower User Agent, 2.3](#)
- [Benutzer-Agent stoppt die Deragierung, wenn es das Dienstkonto nicht in SecurityIdentifier übersetzen kann \(CSCuw20184\)](#)
- [Erteilen von Mindestberechtigungen für ein Active Directory-Benutzerkonto, das vom Sourcefire Benutzer-Agent verwendet wird](#)