Cisco Firepower User Agent Database Service Does not Restart after a Stop

Contents

Introduction

A Cisco User Agent can monitor the Microsoft Active Directory (AD) server and reports login and logoff activities that are authenticated by an LDAP server. A Firepower Management Center (FMC) integrates these activities with the security events it collects from a Firepower managed device. This document provides a solution to an issue when the User Agent does not start after you stop its service.

Symptoms

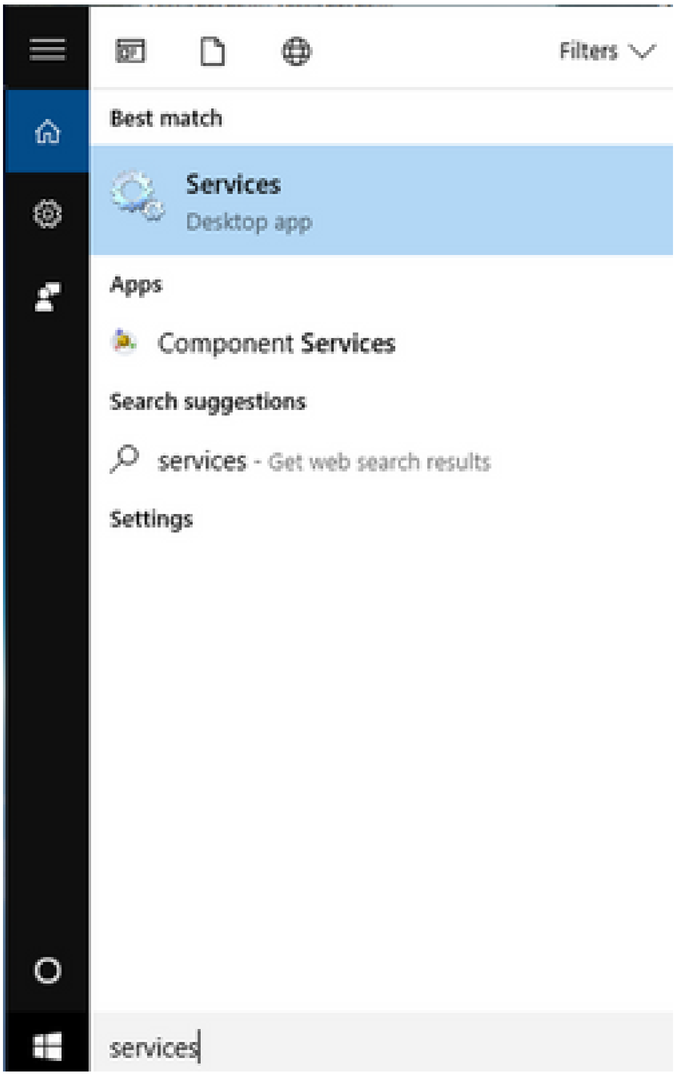
You can use the solution on this document if you notice the following symptoms with your User Agent service:

- User Agent interface shows the service as Not Running.
- The Windows Service Console, `services.msc, shows the Cisco User Agent status as blank, and fails to start the service.`
- The windows event log shows an error similar to "The trust relationship between the primary domain and the trusted domain failed"
- A file `UserEncryptionBytes.bin` is created at `C:\` with zero byte in size.
- The debug mode of a User Agent client shows the following error messages in the Log tab of the User Agent:

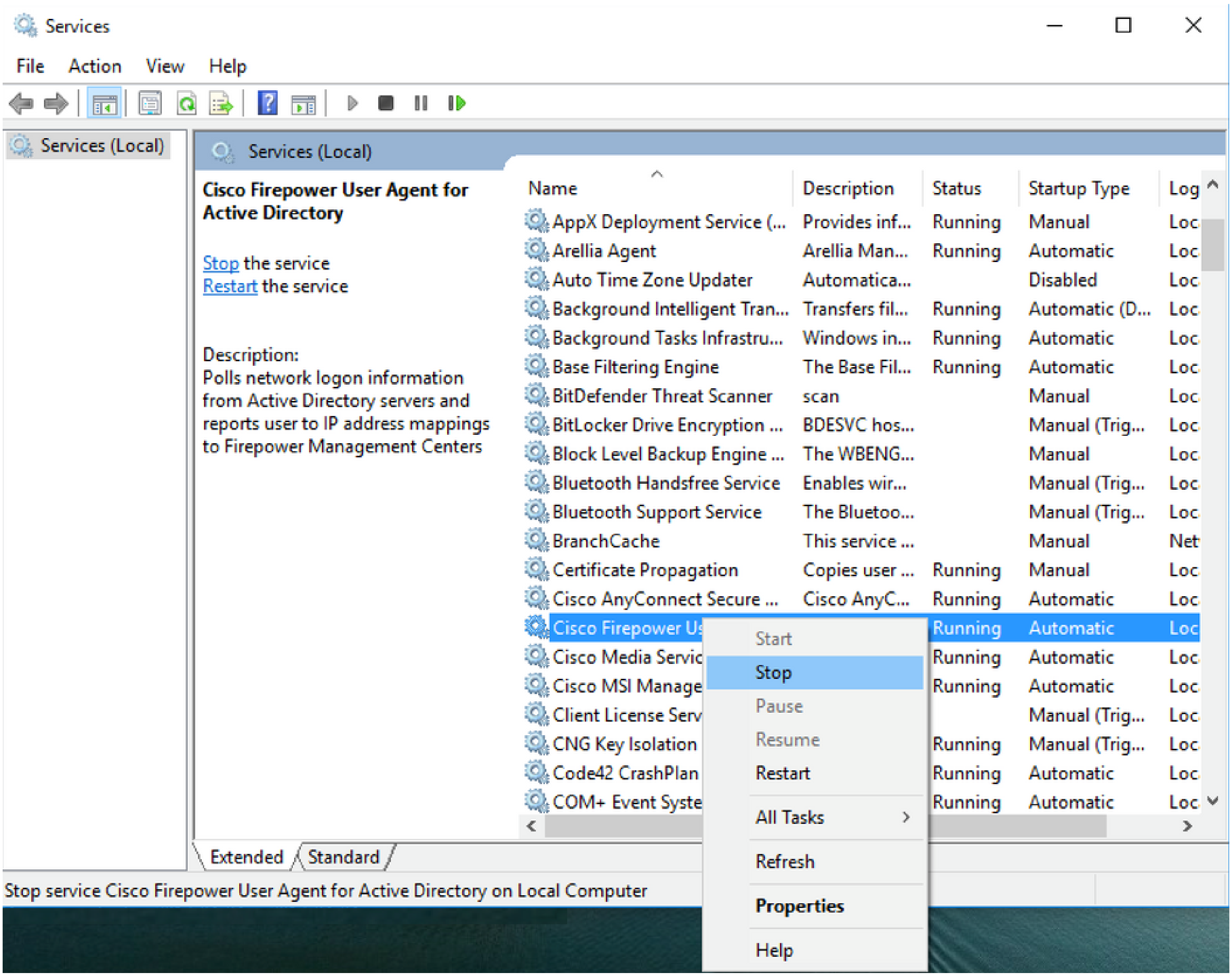
```
<Timestamp>,"debug","[0102] - An error occured while fetching encryption bytes from
'C:\UserAgentEncryptionBytes.bin':
The trust relationship between the primary domain and the trusted domain failed.."

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

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

Solution

Step 1: Run the Microsoft Windows Services Console, `services.msc. It allows you to disable or enable a Windows service.`



Step 2: Right click the Cisco User Agent service and select **Stop** to stop the service.



Cisco Firepower User Agent for Active Directory

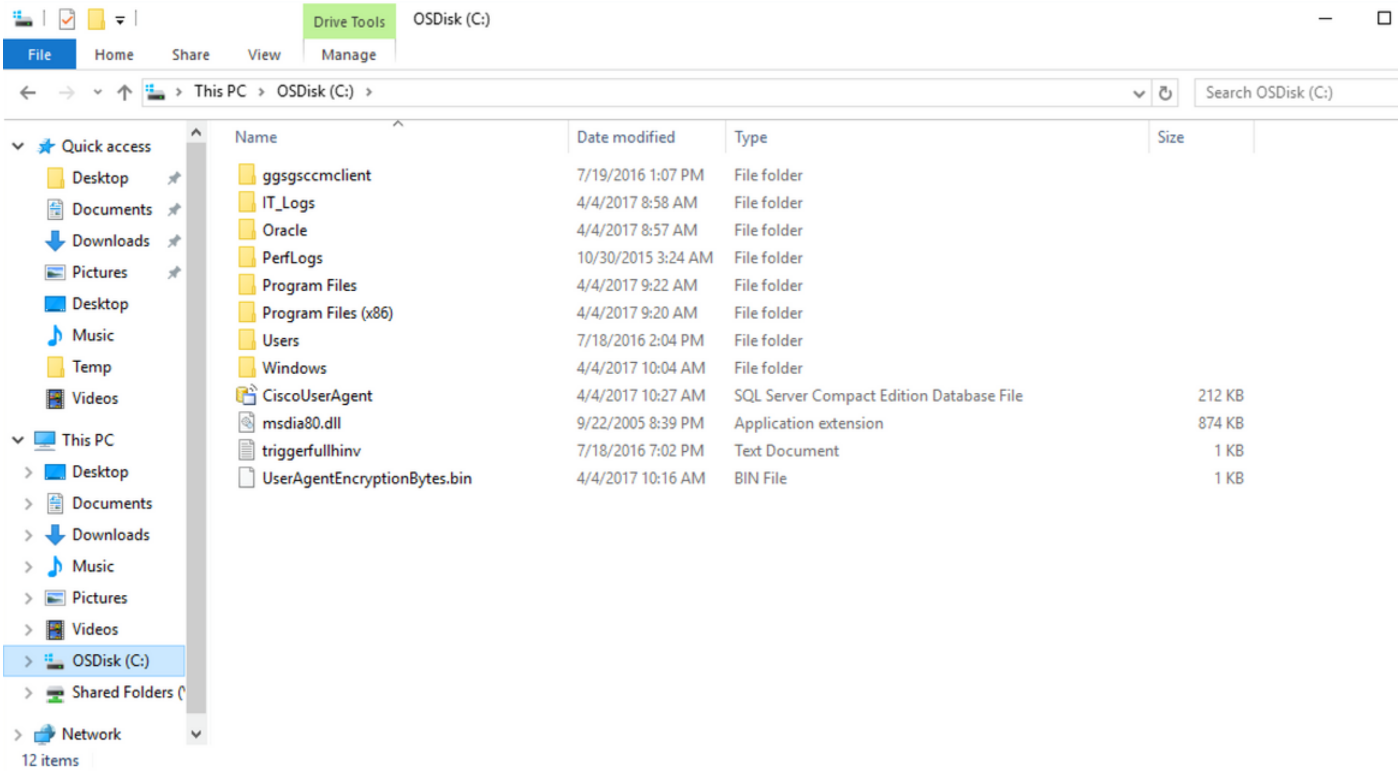
Stop the service
Restart the service

Description:
Polls network logon information from Active Directory servers and reports user to IP address mappings to Firepower Management Centers

Name	Description	Status	Startup Type	Log
AppX Deployment Service (...	Provides inf...	Running	Manual	Loc
Arellia Agent	Arellia Man...	Running	Automatic	Loc
Auto Time Zone Updater	Automatica...		Disabled	Loc
Background Intelligent Tran...	Transfers fil...	Running	Automatic (D...	Loc
Background Tasks Infrastru...	Windows in...	Running	Automatic	Loc
Base Filtering Engine	The Base Fil...	Running	Automatic	Loc
BitDefender Threat Scanner	scan		Manual	Loc
BitLocker Drive Encryption ...	BDESVC hos...		Manual (Trig...	Loc
Block Level Backup Engine ...	The WBENG...		Manual	Loc
Bluetooth Handsfree Service	Enables wir...		Manual (Trig...	Loc
Bluetooth Support Service	The Bluetoo...		Manual (Trig...	Loc
BranchCache	This service ...		Manual	Net
Certificate Propagation	Copies user ...	Running	Manual	Loc
Cisco AnyConnect Secure ...	Cisco AnyC...	Running	Automatic	Loc
Cisco Firepower Us		Running	Automatic	Loc
Cisco Media Servic		Running	Automatic	Loc
Cisco MSI Manage		Running	Automatic	Loc
Client License Serv			Manual (Trig...	Loc
CNG Key Isolation		Running	Manual (Trig...	Loc
Code42 CrashPlan		Running	Automatic	Loc
COM+ Event Syste		Running	Automatic	Loc

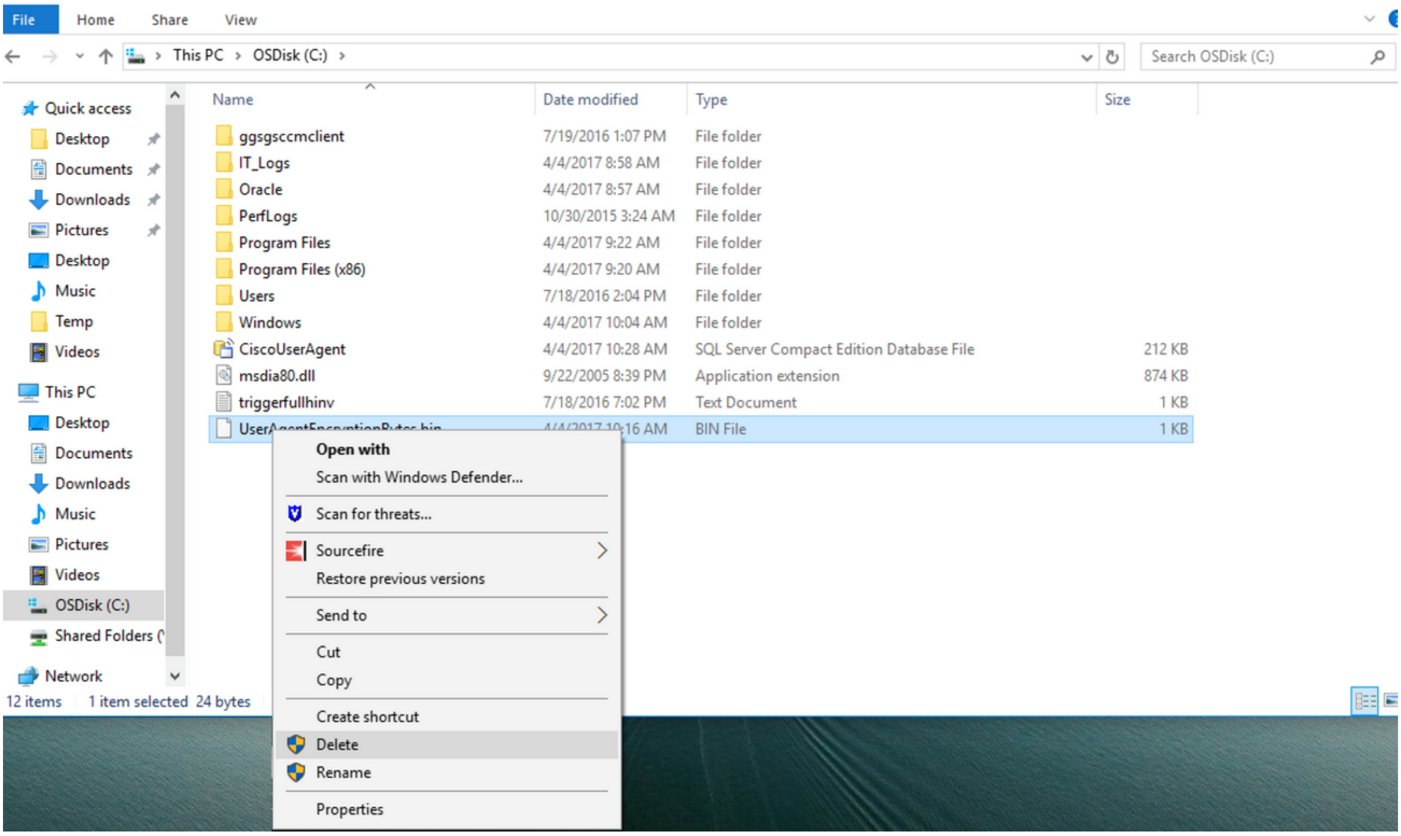
Stop service Cisco Firepower User Agent for Active Directory on Local Computer

Step 3: Navigate to the C: drive.



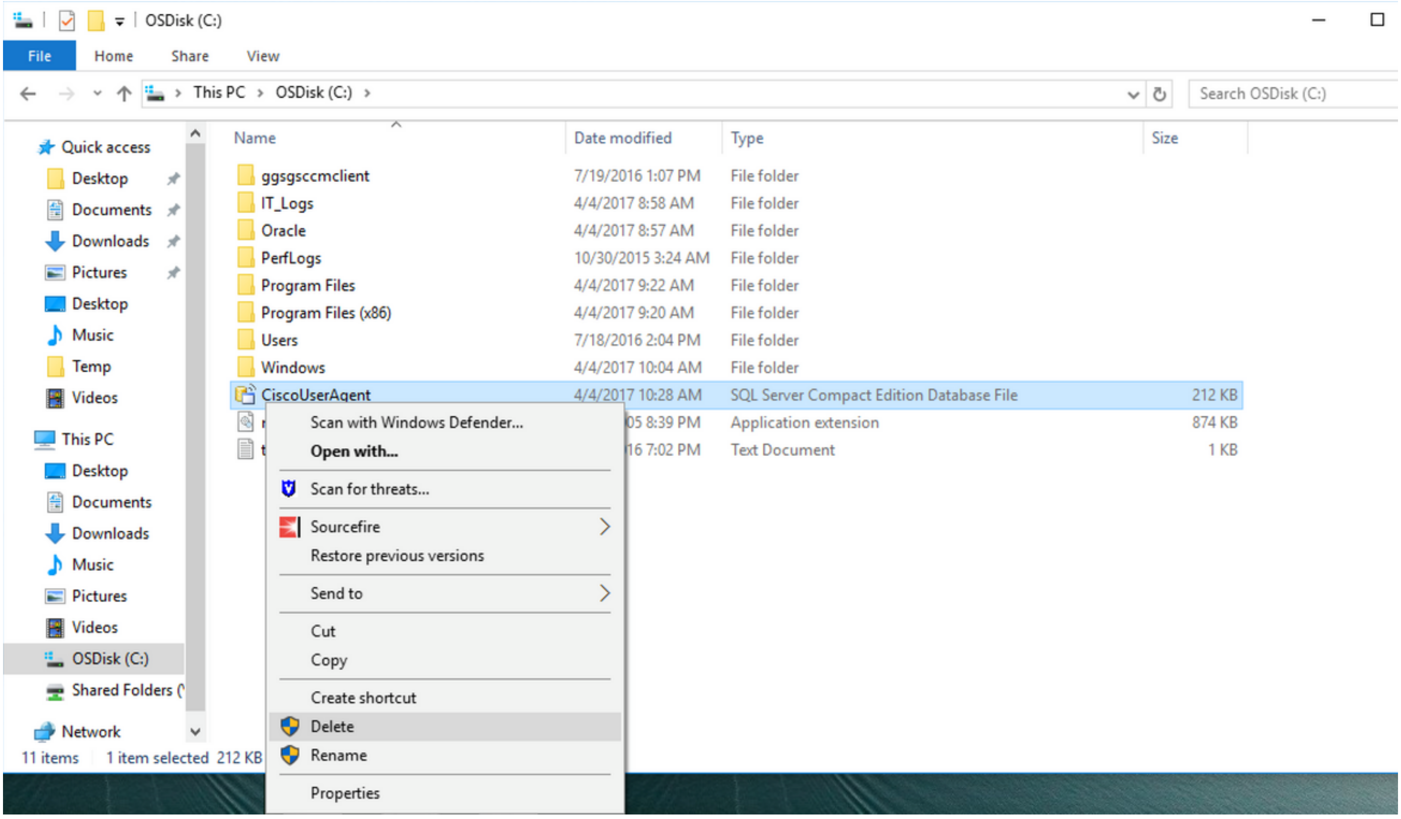
Name	Date modified	Type	Size
ggsgsccmclient	7/19/2016 1:07 PM	File folder	
IT_Logs	4/4/2017 8:58 AM	File folder	
Oracle	4/4/2017 8:57 AM	File folder	
PerfLogs	10/30/2015 3:24 AM	File folder	
Program Files	4/4/2017 9:22 AM	File folder	
Program Files (x86)	4/4/2017 9:20 AM	File folder	
Users	7/18/2016 2:04 PM	File folder	
Windows	4/4/2017 10:04 AM	File folder	
CiscoUserAgent	4/4/2017 10:27 AM	SQL Server Compact Edition Database File	212 KB
msdia80.dll	9/22/2005 8:39 PM	Application extension	874 KB
triggerfullhinv	7/18/2016 7:02 PM	Text Document	1 KB
UserAgentEncryptionBytes.bin	4/4/2017 10:16 AM	BIN File	1 KB

Step 4: Delete this `UserAgentEncryptionBytes.bin` file.



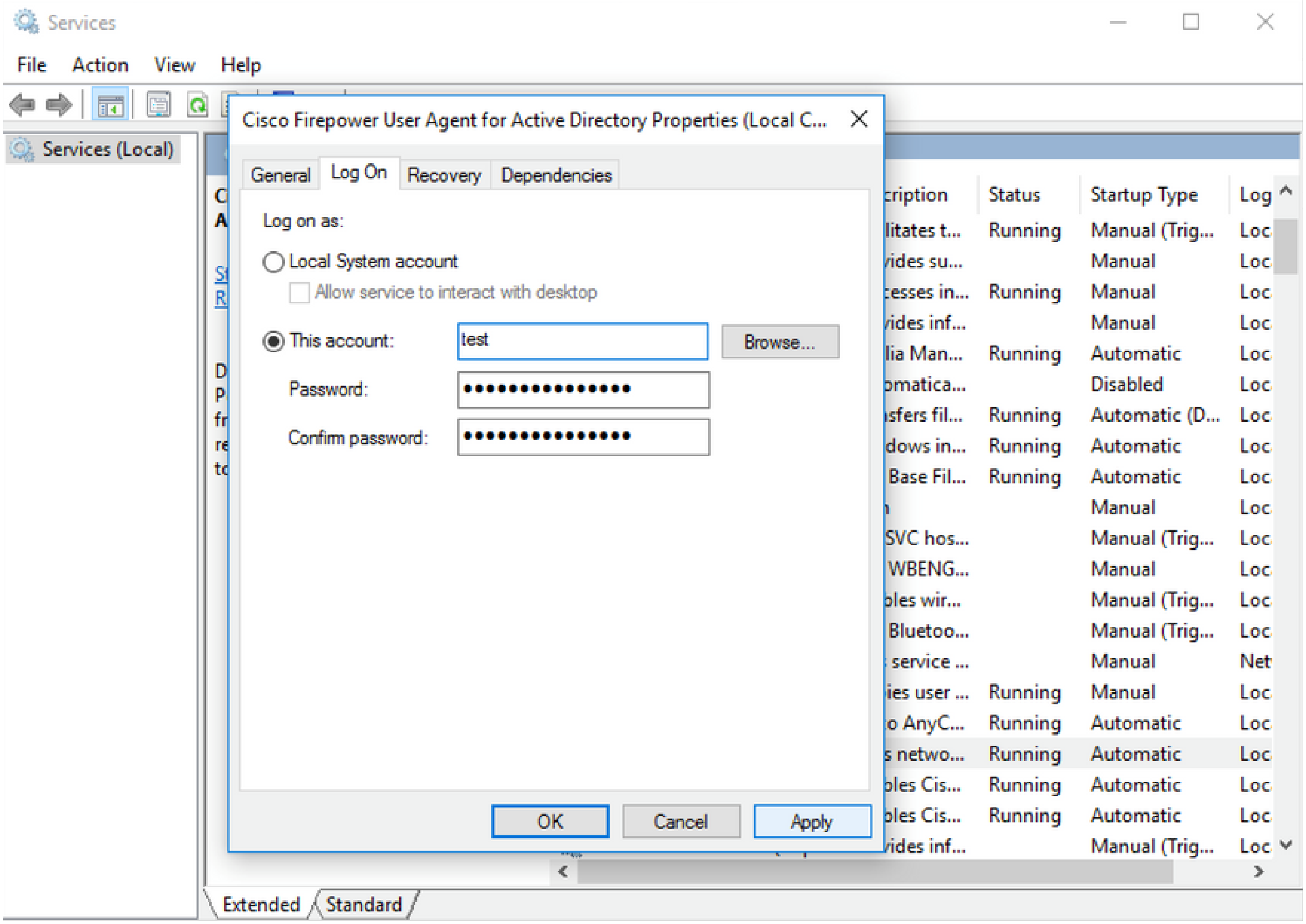
Name	Date modified	Type	Size
ggsgsccmclient	7/19/2016 1:07 PM	File folder	
IT_Logs	4/4/2017 8:58 AM	File folder	
Oracle	4/4/2017 8:57 AM	File folder	
PerfLogs	10/30/2015 3:24 AM	File folder	
Program Files	4/4/2017 9:22 AM	File folder	
Program Files (x86)	4/4/2017 9:20 AM	File folder	
Users	7/18/2016 2:04 PM	File folder	
Windows	4/4/2017 10:04 AM	File folder	
CiscoUserAgent	4/4/2017 10:28 AM	SQL Server Compact Edition Database File	212 KB
msdia80.dll	9/22/2005 8:39 PM	Application extension	874 KB
triggerfullhinv	7/18/2016 7:02 PM	Text Document	1 KB
UserAgentEncryptionBytes.bin	4/4/2017 10:16 AM	BIN File	1 KB

Step 5: Delete the `CiscoUserAgent` file, which is an SQL Server Compact Edition Database File.



Name	Date modified	Type	Size
ggsgsccmclient	7/19/2016 1:07 PM	File folder	
IT_Logs	4/4/2017 8:58 AM	File folder	
Oracle	4/4/2017 8:57 AM	File folder	
PerfLogs	10/30/2015 3:24 AM	File folder	
Program Files	4/4/2017 9:22 AM	File folder	
Program Files (x86)	4/4/2017 9:20 AM	File folder	
Users	7/18/2016 2:04 PM	File folder	
Windows	4/4/2017 10:04 AM	File folder	
CiscoUserAgent	4/4/2017 10:28 AM	SQL Server Compact Edition Database File	212 KB
r	05 8:39 PM	Application extension	874 KB
t	16 7:02 PM	Text Document	1 KB

Step 6: Go back into `services.msc. Right click on the Cisco User Agent service, select` **Properties**, then select **Log On** tab, and configure a user as an AD user login. Click **Apply** when done.



Cisco Firepower User Agent for Active Directory Properties (Local C...

Log on as:

○ Local System account

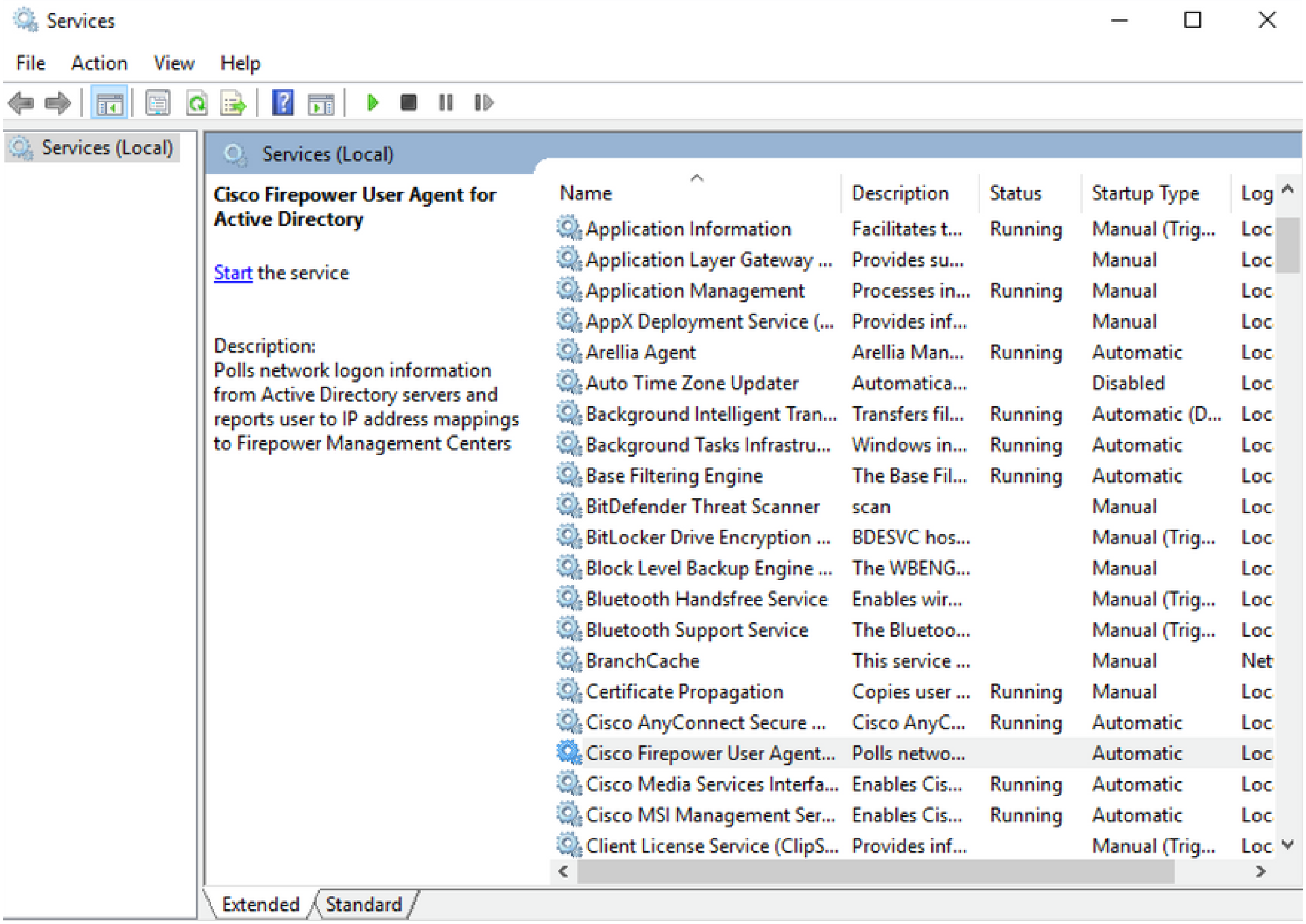
□ Allow service to interact with desktop

● This account: test

Password: •••••••••••••••

Confirm password: •••••••••••••••

Step 7: On the `services.msc, click` **Start** for the **Cisco Firepower User Agent** for Active Directory service.



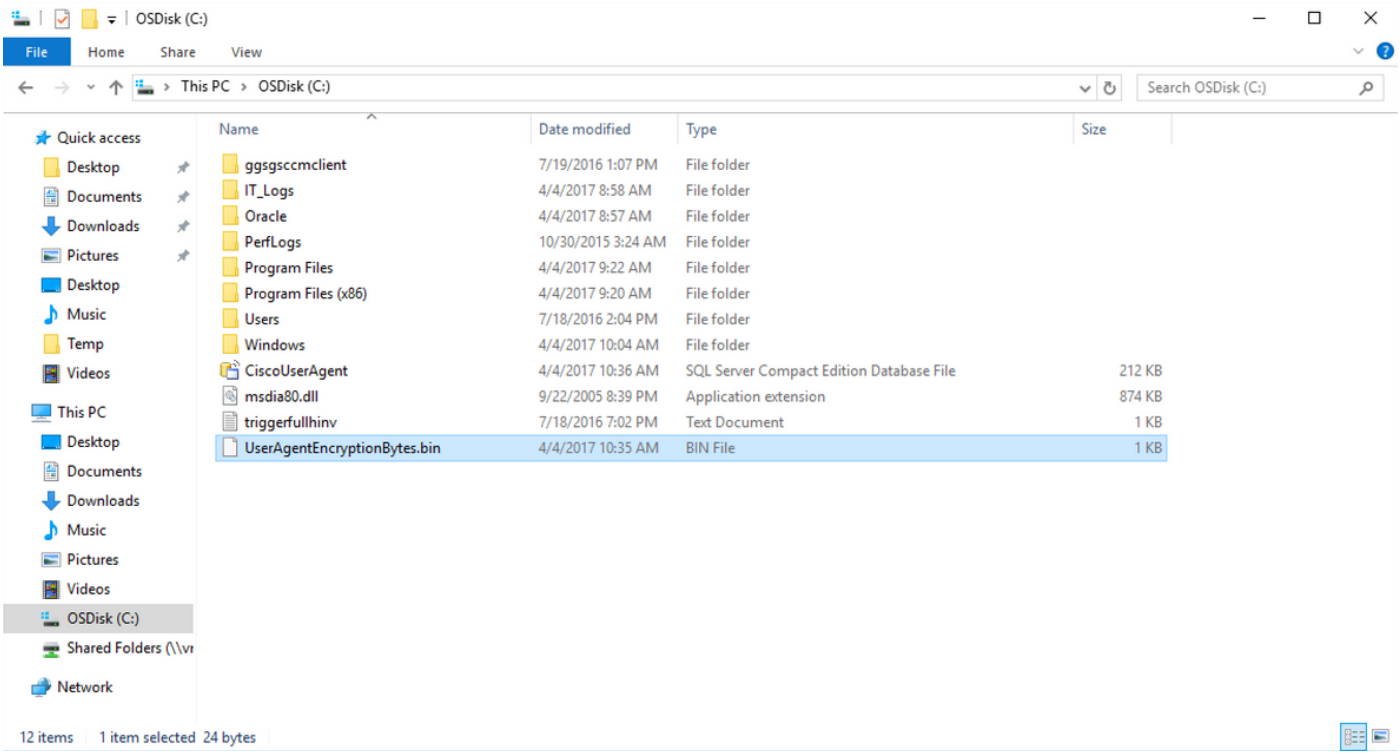
Cisco Firepower User Agent for Active Directory

Start the service

Description:
Polls network logon information from Active Directory servers and reports user to IP address mappings to Firepower Management Centers

Name	Description	Status	Startup Type	Log
Application Information	Facilitates t...	Running	Manual (Trig...	Loc
Application Layer Gateway ...	Provides su...		Manual	Loc
Application Management	Processes in...	Running	Manual	Loc
AppX Deployment Service (...	Provides inf...		Manual	Loc
Arellia Agent	Arellia Man...	Running	Automatic	Loc
Auto Time Zone Updater	Automatica...		Disabled	Loc
Background Intelligent Tran...	Transfers fil...	Running	Automatic (D...	Loc
Background Tasks Infrastru...	Windows in...	Running	Automatic	Loc
Base Filtering Engine	The Base Fil...	Running	Automatic	Loc
BitDefender Threat Scanner	scan		Manual	Loc
BitLocker Drive Encryption ...	BDESVC hos...		Manual (Trig...	Loc
Block Level Backup Engine ...	The WBENG...		Manual	Loc
Bluetooth Handsfree Service	Enables wir...		Manual (Trig...	Loc
Bluetooth Support Service	The Bluetoo...		Manual (Trig...	Loc
BranchCache	This service ...		Manual	Net
Certificate Propagation	Copies user ...	Running	Manual	Loc
Cisco AnyConnect Secure ...	Cisco AnyC...	Running	Automatic	Loc
Cisco Firepower User Agent...	Polls netwo...		Automatic	Loc
Cisco Media Services Interfa...	Enables Cis...	Running	Automatic	Loc
Cisco MSI Management Ser...	Enables Cis...	Running	Automatic	Loc
Client License Service (ClipS...	Provides inf...		Manual (Trig...	Loc

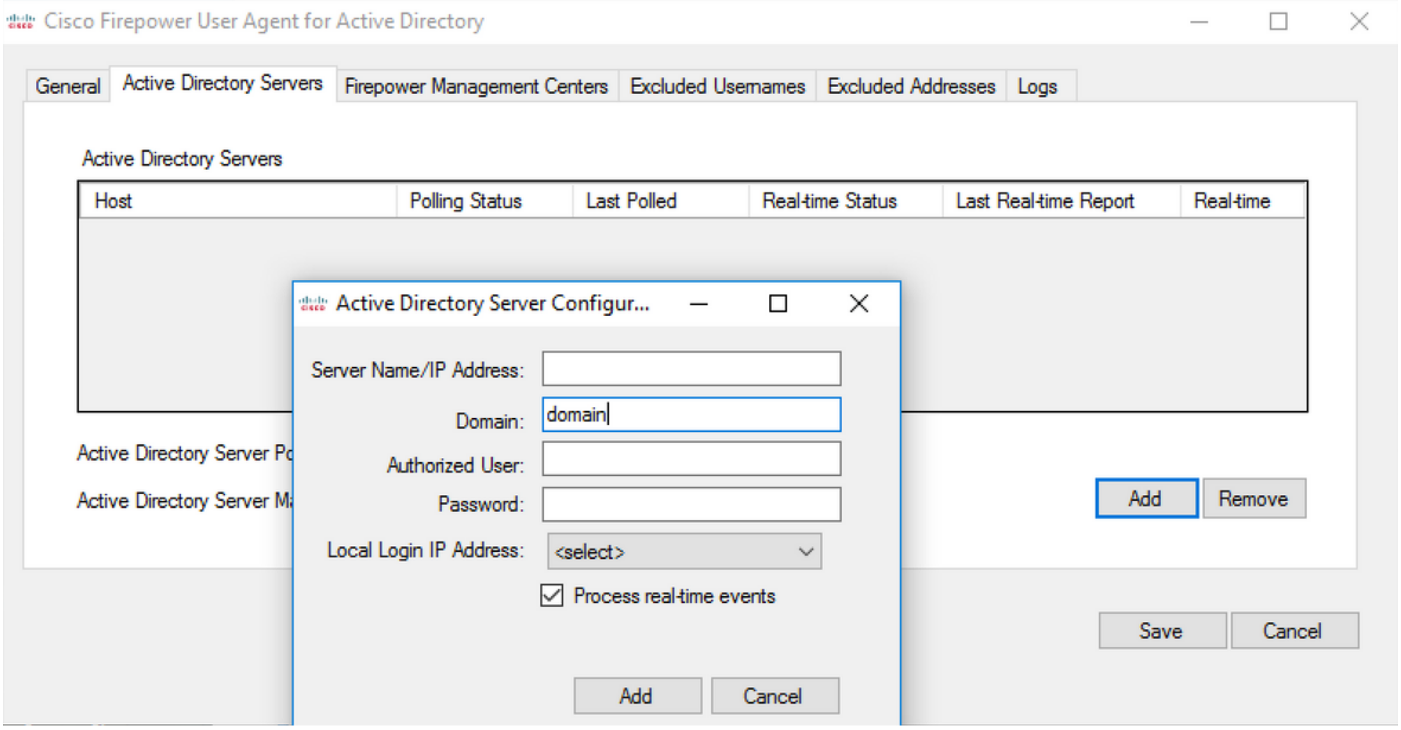
Step 8: Verify the size of the `UserAgentEncryptionBytes.bin` file. It should not be 0 KB.



Name	Date modified	Type	Size
ggsgsccmclient	7/19/2016 1:07 PM	File folder	
IT_Logs	4/4/2017 8:58 AM	File folder	
Oracle	4/4/2017 8:57 AM	File folder	
PerfLogs	10/30/2015 3:24 AM	File folder	
Program Files	4/4/2017 9:22 AM	File folder	
Program Files (x86)	4/4/2017 9:20 AM	File folder	
Users	7/18/2016 2:04 PM	File folder	
Windows	4/4/2017 10:04 AM	File folder	
CiscoUserAgent	4/4/2017 10:36 AM	SQL Server Compact Edition Database File	212 KB
msdia80.dll	9/22/2005 8:39 PM	Application extension	874 KB
triggerfullhinv	7/18/2016 7:02 PM	Text Document	1 KB
UserAgentEncryptionBytes.bin	4/4/2017 10:35 AM	BIN File	1 KB

12 items 1 item selected 24 bytes

Step 9: Add the Domain Controllers and Firepower Managmenet Center to the User Agent Client. Please be sure to add the Domain Controllers/local host before adding the Firepower Management Center to the User Agent.



Server Name/IP Address:

Domain: domain

Authorized User:

Password:

Local Login IP Address: <select>

☑ Process real-time events

References

- Firepower User Agent Configuration Guide, 2.3
- User Agent Stops Derailing If It Cannot Translate Service Account to SecurityIdentifier (CSCuw20184)
- Grant Minimum Permission to an Active Directory User Account Used by the Sourcefire User Agent