ManageEngine
ADAudit Plus

Agent-based data collection guide

www.adauditplus.com

Table of contents

1. Overview 1

2. Installation prerequisites 1

2.1 Supported operating systems 1

2.2. Ports that need to be open 2

2.3. Privileges required 3

2.4. Disk space requirements 4

2.5 Windows .NET Framework 4

2.6 Remcom.exe 4

3. Agent installation 5

3.1 Installing the agent via ADAudit Plus' UI 5

3.2 Installing the agent manually 6

3.2.1 Server name, port, and protocol used by ADAudit Plus 6

3.2.2 Installing the agent via Group Policy 7

3.2.3 Installing the agent by running the MSI file on client computers 9

3.2.4 Installing the agent via command line 10

3.2.5 Installing the agent via Endpoint Central 11

4. Agent security settings 14

5. Agent configuration sync 15

6. Upgrading the agent 15

7. Agent uninstallation 16

7.1 Uninstalling the agent via ADAudit Plus' UI 16

7.2 Uninstalling the agent manually 17

7.2.1 Uninstalling the agent via Group policy 17

7.2.2 Uninstalling the agent via command line 17

7.2.3 Uninstalling the agent via Endpoint Central 17

7.2.4 Uninstalling the agent via the Control Panel in the target computer 18

8. Troubleshooting 18

9. List of errors that may arise while installing the agent and the solutions to resolve them 20

1. Overview

Why do I need to install an agent?

ADAudit Plus collects security information from configured computers on your network including domain controllers, file servers, Windows servers, and workstations. In case of larger networks that operate across wide area network (WAN) connections, deploying a client-side agent not only smooths out data collection, but also reduces bandwidth utilization considerably.

Even without an installed agent, log collection from domain controllers happens in real time; however, for file servers and Windows servers, real-time data collection can only be enabled by installing a client-side software agent. That said, neglecting to install an agent will not hinder ADAudit Plus' functionality.

The agent can be installed on the following types of machines:

1. Direct access
2. Persistent and non-persistent virtual desktop infrastructure (VDI)
3. Linked Clone and Full Clone VDI in virtual machine (VM)
4. Azure Virtual Desktop

When do I need to configure a NAT device?

To deploy ADAudit Plus securely over the internet, you can configure a network address translation (NAT) device to act as an intermediary between the client-side agent and the ADAudit Plus server.

2. Installation prerequisites

Please ensure that the following criteria are met to allow smooth installation of the agent on the target machine.

2.1 Supported operating systems

Windows Server operating systems: Windows Server 2008 and above

Windows operating systems: Windows 8 and above; Windows 7 and Windows Vista (EOLed by Microsoft)

2.2. Ports that need to be open

Agent to server communication			
Purpose 1. Sending audit data from agent to server 2. Syncing agent running status with server 3. Pulling all configurations periodically (every 60 minutes) from the server			
Port to be opened	**Protocol**	**Destination**	**Direction**
To find the port used by ADAudit Plus, log in to the **ADAudit Plus console**, navigate to the **Admin** tab > **General Settings > Connection > NAT.** • In case, you have not configured a NAT device between the ADAudit Plus agent and server, the port number adjacent to the **Central server** field should be opened in the agent installed machine (by default, ADAudit Plus uses port number 8555 for agent to server communication). • If you have configured a NAT device between the ADAudit Plus agent and server, find the port number adjacent to the NAT Device field.	HTTPS	Monitored computers	Outbound

Server-to-agent communication
Purpose 1. Automatically installing, uninstalling, and upgrading the agent via the product 2. Syncing server configuration with the agent when the agent has not communicated with the server for more than two hours: communication between the agent and server is checked once every 30 minutes 3. Immediately notifying the agent of the following actions: global exclude configuration changes, event collection schedule time and run-now changes, product port and protocol changes, enabling or disabling of servers, and more **Note:** The agent synchronizes server configurations by HTTPS communication. If HTTPS fails then the server attempts to sync all configurations with agent via RPC.

Port to be opened	Protocol	Destination	Direction
Dynamic ports (49152-65535) 445, and 135	RPC	Monitored computers	Inbound

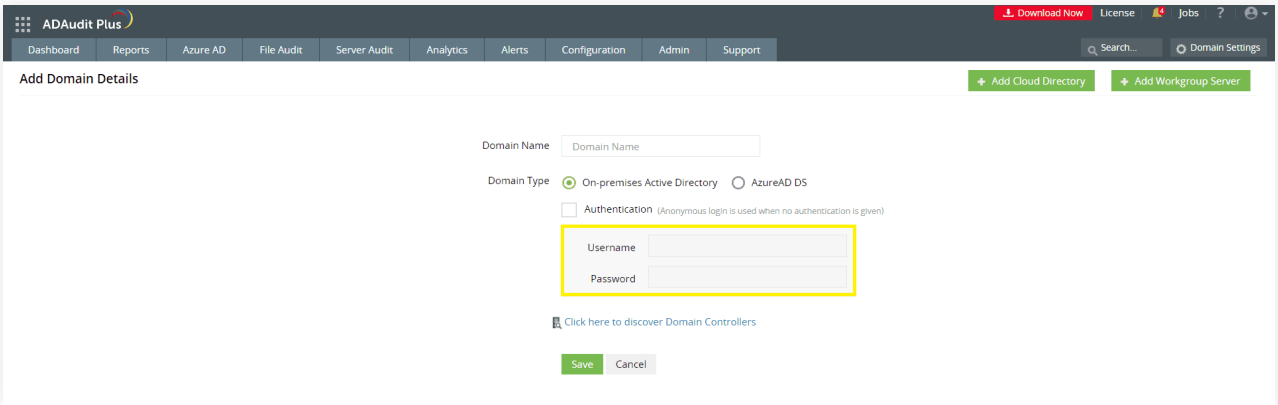
Ensure that the port used by ADAudit Plus are open on the client machine to establish successful communication from the Agent to ADAudit Plus server.

2.3. Privileges required

Make sure that the ADAudit Plus service account (the ADAudit Plus service account is the AD account used while configuring a domain in ADAudit Plus) is a member of the **Domain Admins group** so that ADAudit Plus can perform the following actions automatically:

1. Install, uninstall or update the agent
2. Start or stop the agent
3. Sync properties across the server and the agent

If you do not wish to use Domain Admin credentials, you can still perform the above tasks manually.



2.4 Disk space requirements

Ensure there is a minimum of 2GB of free disk space. This will allow the agent to save up to 2GB of event data when it is unable to forward data to server. Event collection will stop once the 2GB limit is reached. You can configure this setting in the product by navigating to **Admin > Agent settings > Event Data Settings > Maximum size of EventData directory.**

Note:

Make sure to keep the event data directory size less than 10GB to prevent disk space issues on the machine where the agent is installed.

2.5 Windows .NET Framework

The installation requires Windows .NET Framework version 4.5 or higher on the client machine.

By default, .NET Framework version 4.5 or higher is included with Windows Server 2012 or higher, as well as workstations running Windows 8 or higher. If you're running one of these operating systems, you can proceed with step 3: installing the agent.

If you're running an older version of Windows, please ensure that .NET Framework version 4.5 or higher need to be installed on the following operating systems: Windows 7, Windows Server 2008 R2, and Windows Server 2008.

You can check the .NET Framework version installed on a computer by opening Command Prompt, navigating to \%windir%\Microsoft.NET\FrameWork, and then going to the directory with the latest version number. Once in the directory with the latest version number, run the command .\MSBuild.exe -version.

Microsoft (R) Build Engine version 4.7.3056.0
[Microsoft .NET Framework, version 4.0.30319.42000]
Copyright (C) Microsoft Corporation. All rights reserved.
4.7.3056.0

The last line after the copyright information is the Windows .NET Framework version installed on the computer.

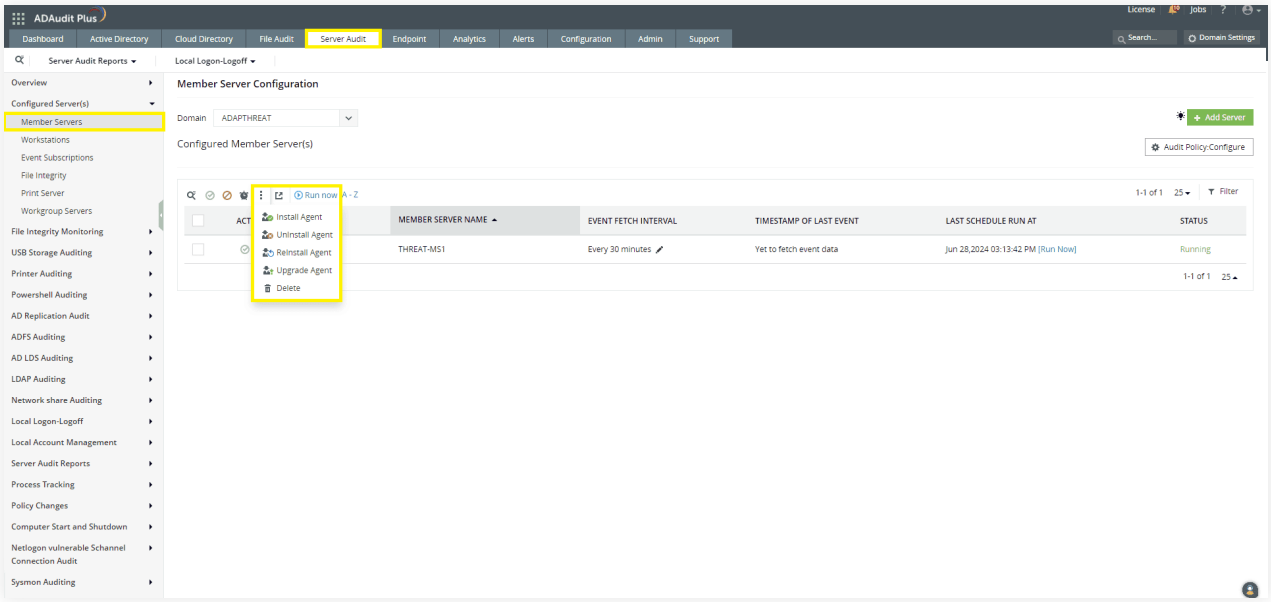
2.6 Remcom.exe

ADAudit Plus uses **remcom.exe** and **remcomsvc.exe** for installing and uninstalling the agent. To ensure unhindered functioning of ADAudit Plus, you need to add the remcom.exe file to the exception list of your antivirus software in the ADAudit Plus server and remcom.svc.exe file to the exception list of your antivirus software in the target computers in which the agent is to be installed.

3. Agent installation

3.1 Installing the agent via ADAudit Plus' UI

Now that you have your environment set up to meet the installation prerequisites, you can install the agent on a target machine right from within ADAudit Plus' user interface as shown below:



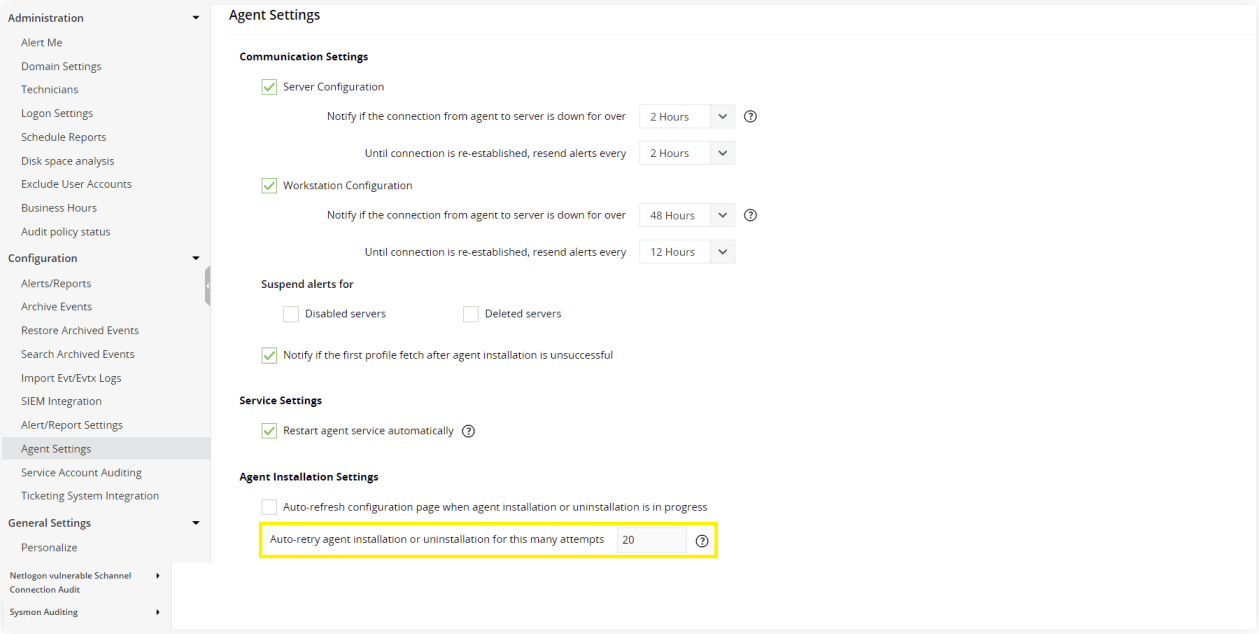
We recommend installing the agent using ADAudit Plus; if the installation fails on any computer, ADAudit Plus automatically retries installing the agent every 30 minutes for up to 10 failed attempts.

Please note that the service account used while configuring your domain in ADAudit Plus has to be a member of the **Domain Admins group** in order for the application to install the agent on a client.
If you do not want want to provide Domain Admin credentials, follow the steps in the next section (3.2) to install the agent manually.

Note:

- Reboot of server is not required after agent installation.

- Agent installation/uninstallation can be retried in case it fails, the maximum number of retries can be configured from the **Agent Settings** tab found under the **Admin** page in the product.
  The default setting for automatic agent installation or uninstallation is 20 times within the product.



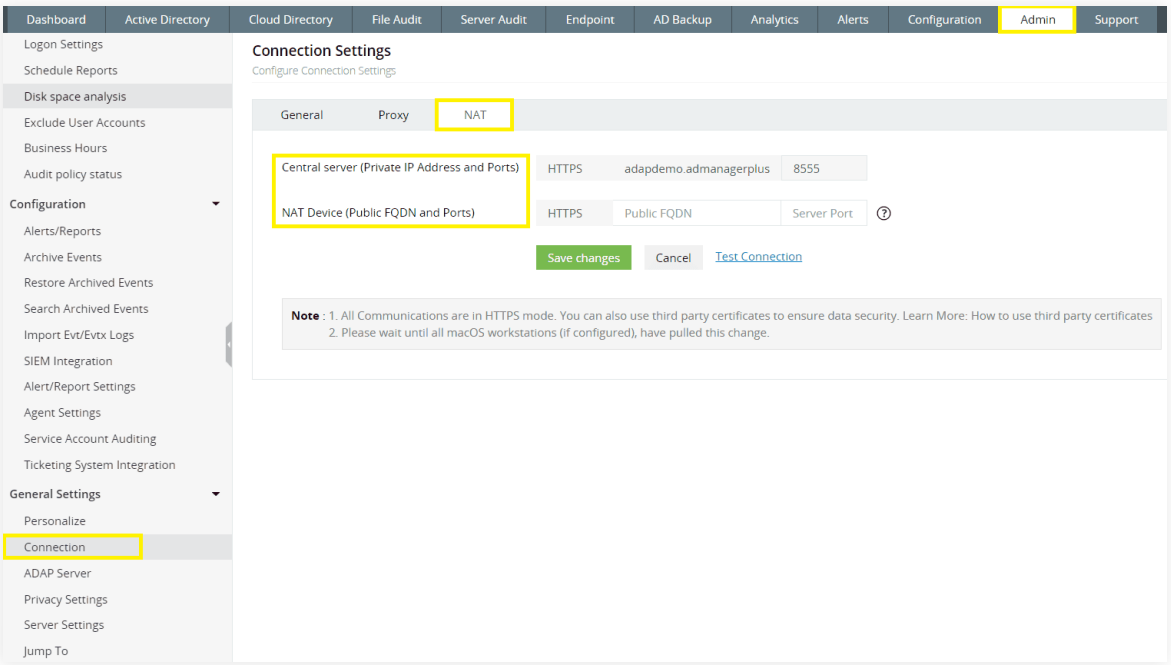
3.2 Installing the agent manually

3.2.1 Server name, port, protocol, and org access key used by ADAudit Plus

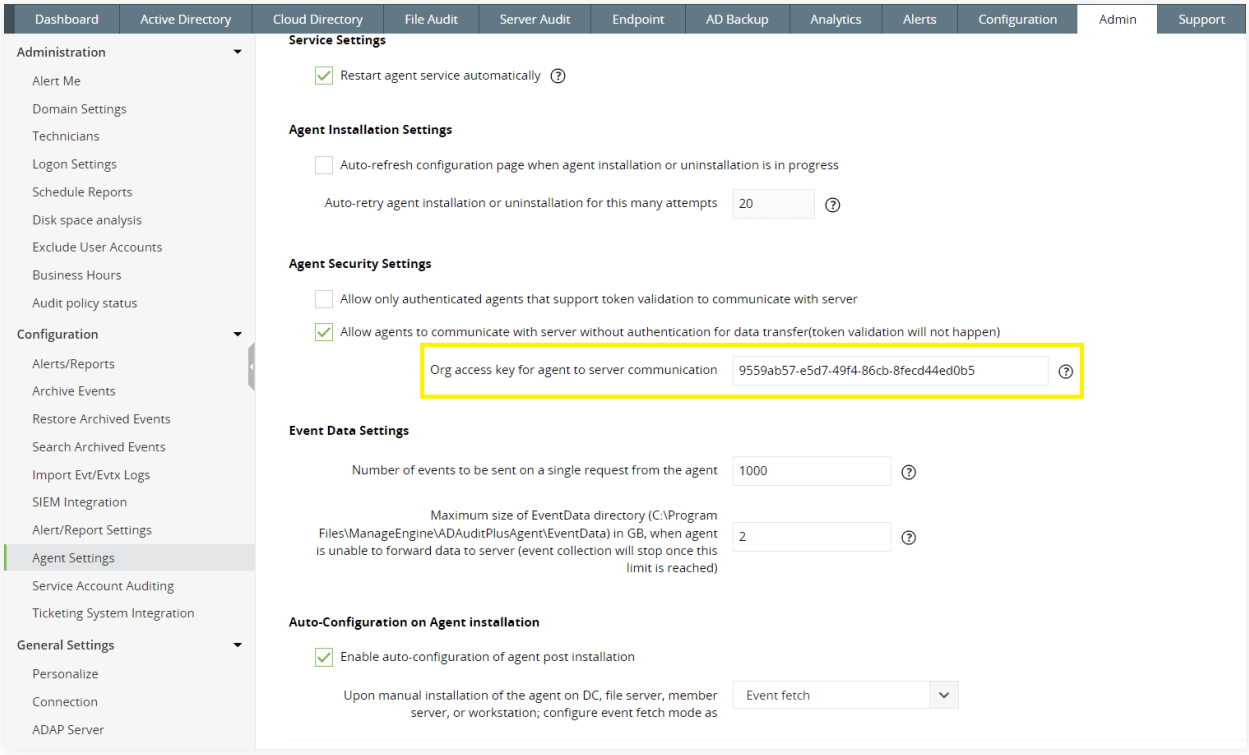
To find the server name, port, and protocol used by ADAudit Plus, log in to the ADAudit Plus console, navigate to the **Admin tab > General Settings > Connection > NAT.**

- If you have not configured a NAT device between the ADAudit Plus agent and server, you can find the details adjacent to the **Central server** field (by default, ADAudit Plus uses port number 8555 for agent to server communication).

- If you have configured a NAT device between the ADAudit Plus agent and server, you can find the details adjacent to the **NAT Device** field.



To find the org access key used by ADAudit Plus, log in to the ADAudit Plus console, navigate to the **Admin** tab > **Configuration > Agent Settings > Agent Security Settings > Org access key for agent to server communication.**



3.2.2 Installing the agent via Group Policy:

1. Create an MST file

MST files are used by administrators to customize the behavior of an existing MSI file (MSI is an installer package file format used by Windows).

An MST file needs to be created using the ORCA tool, which is available under Windows SDK Components for Windows Installer Developers.

i. Open the ORCA tool > **File > Open** > Select the file- **ADAuditPlusAgent-x86.msi** or **ADAuditPlusAgent-x64.msi**

Note: The above files can be found under <ADAudit Plus installation directory>\webapps\adap\agent. If the target computer is running a 32-bit OS, choose **ADAuditPlusAgent-x86.msi.** If the target computer is running a 64-bit OS, choose **ADAuditPlusAgent-x64.msi.**

ii. Click on the **Transform** menu. Select **New Transform** and navigate to the panel on the left. Select **Registry** and enter the appropriate values for the fields—ServerName, ServerIP, Build, Protocol, Port, OrgAccessKey, and ServerFQDN.

Here, **ServerName** refers to the name of the server where ADAudit Plus/NAT device is hosted.

ServerIP refers to the IP address of the server where ADAudit Plus/NAT device is hosted.

Build refers to the build number of your ADAudit Plus installation.

The build number is a 4 digit number that can be found by clicking on the license button located on the top right corner of your ADAudit Plus console.

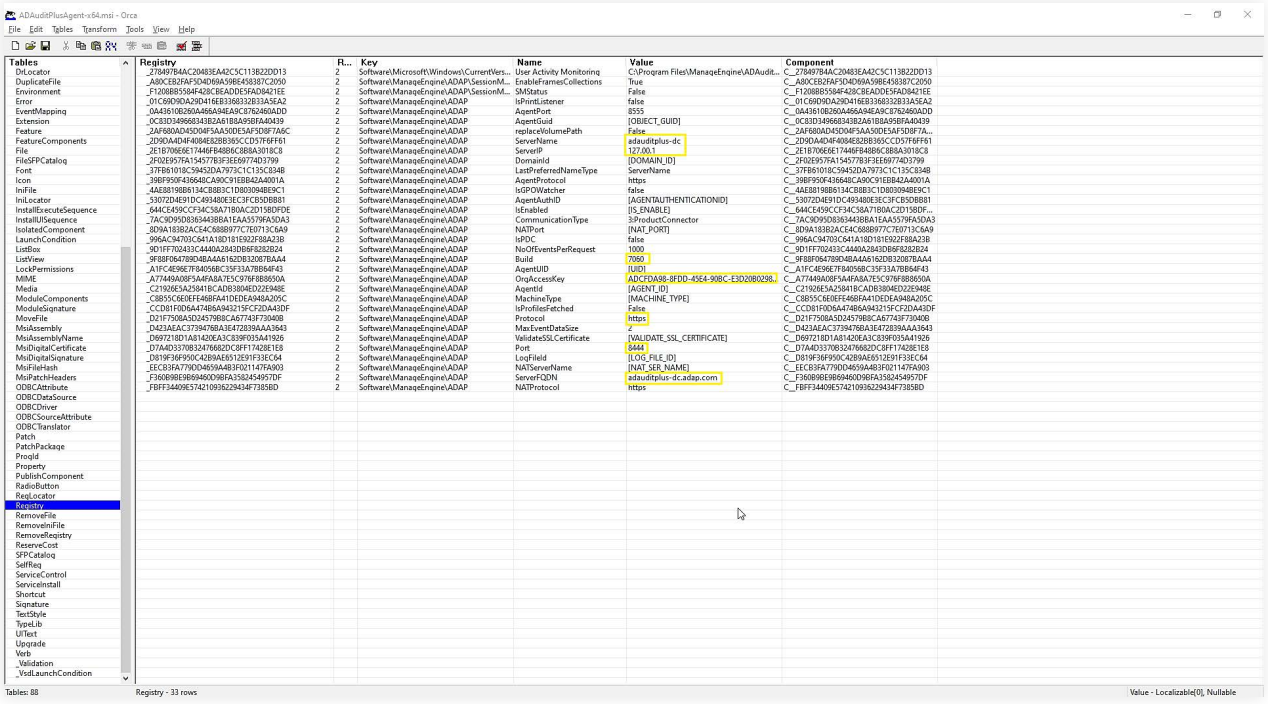
Protocol refers to the protocol used for agent to server communication (HTTPS by default).

Port refers to the port number used for agent to server communication (8555 by default).

OrgAccessKey refers to the key used for agent to server communication (unique to each organization).

ServerFQDN refers to the FQDN of the server where ADAudit Plus/NAT device is hosted. For example, if ADAudit Plus is hosted on a DC named adap-dc2 in the adap.internal.com domain, the ServerFQDN is adap-dc2.adap.internal.com.

Note: To find the ServerName, Port, Protocol, and OrgAccessKey used by ADAudit Plus, click here.



iii. Click the **Transform** tab and select **Generate Transform**. Name the transformation file **ADAP.mst** and **Save** it.

iv. Copy the following 2 files into a new folder-

a. **ADAuditPlusAgent-x86.msi or ADAuditPlusAgent-x64.msi**

Note: The above files can be found under <ADAudit Plus installation directory>\webapps\adap\agent. For 32-bit installations choose **ADAuditPlusAgent-x86.msi** and for 64-bit installations choose **ADAuditPlusAgent-x64.msi**.

b. **ADAP.mst** (the file generated using the ORCA tool)

v. Right-click the newly created folder, go to **Share with > Specific people** and type **Domain Computers** in the search box. Provide **Read** permission and click **Share.**

2. Install the agent via Group Policy

i. Log in to any computer that has the Group Policy Management Console (GPMC) with Domain Admin credentials. Open the **GPMC** and create a new GPO named **ADAuditPlusAgent**. Link this GPO to the audited computers.

ii. Right-click **ADAuditPlusAgent GPO** and select **Edit > Computer Configuration > Policies > Software Settings.** Right-click **Software Installation** and select **New > Package**. In the dialog box, type the full Universal Naming Convention (UNC) path of the ADAP MSI file.
Note: For 32-bit installations type the full UNC of **ADAuditPlusAgent-x86.msi** and for 64-bit installations type the full UNC of **ADAuditPlusAgent-x64.msi.**

For example, in the dialog box, enter: \\Server_name\Shared_folder\ADAuditPlusAgent-x64.msi
Here, Server_name refers to the name of the server on which the file resides.
Shared_folder refers to the folder created under step 4.1.1 iv.
Note: Ensure that you enter the full UNC path as opposed to the local/network path.

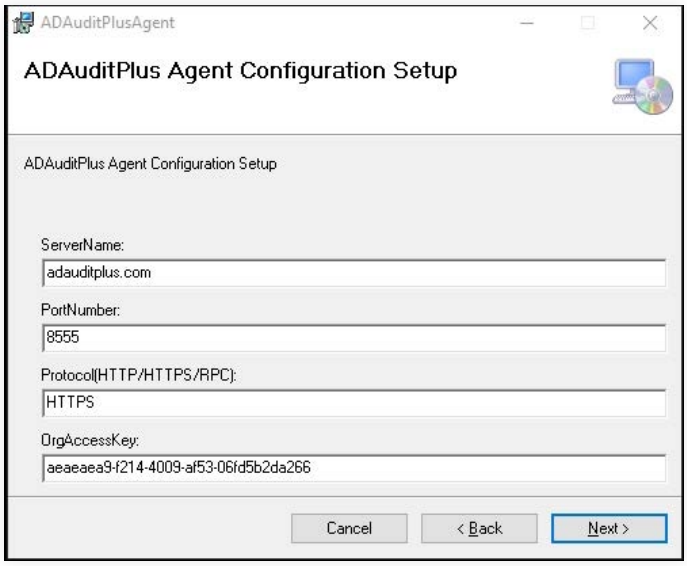
iii. In the **Deploy Software** pop-up, select **Advanced > Modifications > Add** and type the full Universal Naming Convention (UNC) path of the ADAP MST file.
Note: Again, ensure that you enter the full UNC path as opposed to the local/network path.

Once the computers restart, the ADAudit Plus agent will get automatically installed.
Note: Reboot of server is not required after agent installation.

3.2.3 Installing the agent by running the MSI file on client computers

Provide the below arguments while installing the agent:
Server name: The name of the server where ADAudit Plus/NAT device is hosted.
Port: The port number used for agent to server communication (8555 by default).
Protocol: The protocol used for agent to server communication (HTTPS by default).
OrgAccessKey refers to the key used for agent to server communication (unique to each organization).

Note: To find the ServerName, Port, Protocol, and OrgAccessKey used by ADAudit Plus, click here.



Note: Reboot of server is not required after agent installation.

3.2.4 Installing the agent via command line

On the target computer, open an elevated Command Prompt (right-click Command Prompt and select **Run as administrator**), and execute the below command:

msiexec /i "MSI file location" PROTOCOL=HTTPS PORT=8444 SERVERNAME=adap-dc2 SERVERFQDN =adap-dc2.adap.internal.com SERVERIP=192.168.225.33 OrgAccessKey=ADCFDA98-8FDD-45E4-90BC -E3D20B029870 /q

Copy MSI files from this location, <Installation_folder>\webapps\adap\agent, and save it on the target computer. Add the **MSI file location** (on the target computer) in the command above.
Note: Choose the appropriate MSI based on the OS version on your client computer.
For 32-bit versions: ADAuditPlusAgent-x86.msi
For 64-bit versions: ADAuditPlusAgent-x64.msi

Here, **ServerName** refers to the name of the server where ADAudit Plus/NAT device is hosted.
ServerIP refers to the IP address of the server where ADAudit Plus/NAT device is hosted.
Protocol refers to the protocol used for agent to server communication (HTTPS by default).
Port refers to the port number used for agent to server communication (8555 by default).
OrgAccessKey refers to the key used for agent to server communication (unique to each organization).
ServerFQDN refers to the FQDN of the server where ADAudit Plus/NAT device is hosted. For example, if ADAudit Plus is hosted on a DC named adap-dc2 in the adap.internal.com domain, the ServerFQDN is adap-dc2.adap.internal.com.

Note: To find the ServerName, Port, Protocol, and OrgAccessKey used by ADAudit Plus, click here.
Note: Reboot of server is not required after agent installation.

3.2.5 Installing the agent via Endpoint Central

1. Create an MSI package:

To install the ADAudit Plus agent via Endpoint Central, follow the below steps:

i. Log in to the **Endpoint Central console** as an administrator.

ii. Click **Software Deployment > Package creation > Packages > Add Package** and select **Windows** from the drop-down.

iii. Provide the below details:

- Beside *Package Name*, enter **ADAudit Plus Agent** or any other name of your choice.
- Beside *Package Type*, select **MSI/MSP.**
- Beside *License Type*, select **Commercial** from the drop-down.
- Beside *Location installable*, select **From Shared Folder.**

iv. **Install the package, using either one of these methods-**

iv **(a) Install package by using MST file**

- Create an MST file. MST files are used by administrators to customize the behavior of an existing MSI file (MSI is an installer package file format used by Windows). An MST file needs to be created using the ORCA tool, which is available under Windows SDK Components for Windows Installer Developers.

- Open the ORCA tool > **File > Open** > Select the file- **ADAuditPlusAgent-x86.msi** or **ADAuditPlusAgent-x64.msi**

  Note: The above files can be found under <ADAudit Plus installation directory>\webapps\adap\agent. If the target computer is running a 32-bit OS choose **ADAuditPlusAgent-x86.msi** and if it is running a 64-bit OS choose **ADAuditPlusAgent-x64.msi.**

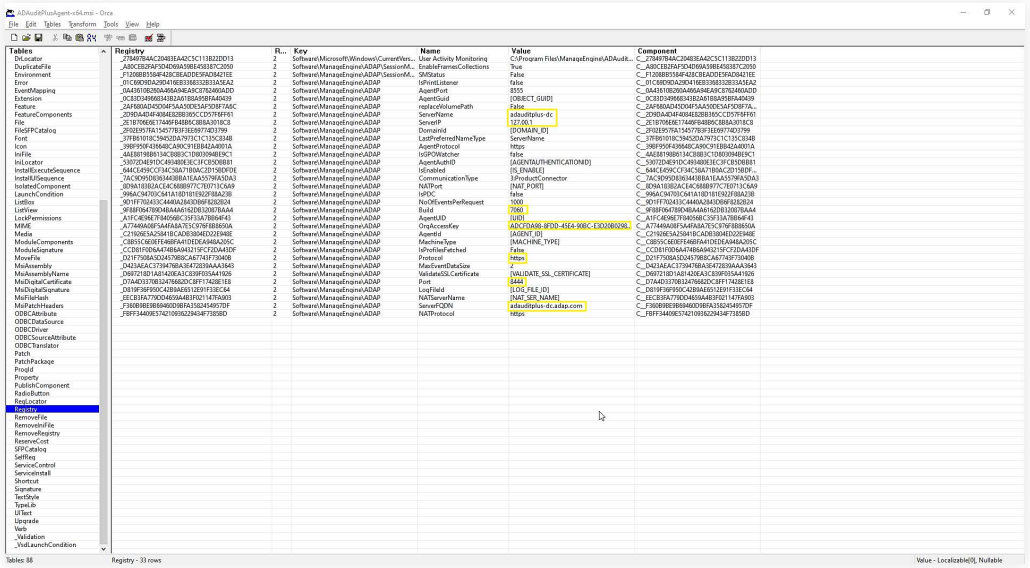
- Click the **Transform** menu > Select **New Transform** > Navigate to the panel on the left, select **Registry** > Enter appropriate values for the fields—ServerName, ServerIP, Build, Protocol, Port, OrgAccessKey, and ServerFQDN.

  Here, **ServerName** refers to the name of the server where ADAudit Plus/NAT device is hosted.
  ServerIP refers to the IP address of the server where ADAudit Plus/NAT device is hosted.
  Build refers to the build number of your ADAudit Plus installation.
  The build number is a 4 digit number that can be found by clicking on the license button located on the top right corner of your ADAudit Plus console.
  Protocol refers to the protocol used for agent to server communication (HTTPS by default).
  Port refers to the port number used for agent to server communication (8555 by default).

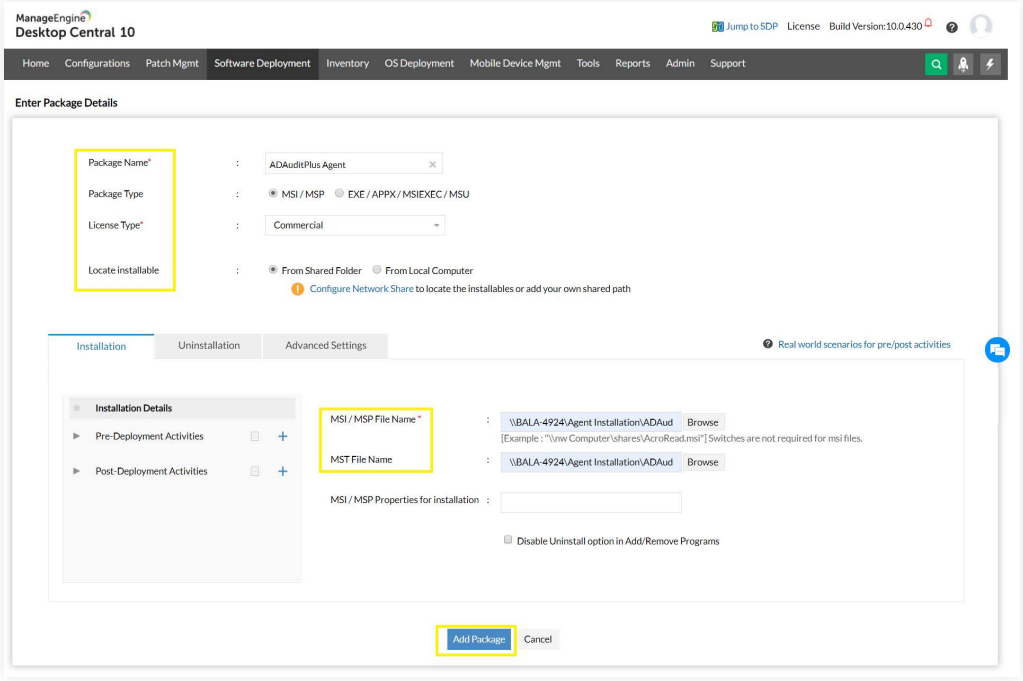
OrgAccessKey refers to the key used for agent to server communication (unique to each organization).
ServerFQDN refers to the FQDN of the server where ADAudit Plus/NAT device is hosted. For example, if ADAudit Plus is hosted on a DC named adap-dc2 in the adap.internal.com domain, the ServerFQDN is adap-dc2.adap.internal.com.

Note: To find the ServerName, Port, Protocol, and OrgAccessKey used by ADAudit Plus, click here.

- Click the **Transform** tab > **Generate Transform**. Name the transformation file and click **Save.**



- Click **Browse** and select the MSI and MST files.
- Click **Add Package.**



iv **(b) Install the package by using installation properties**

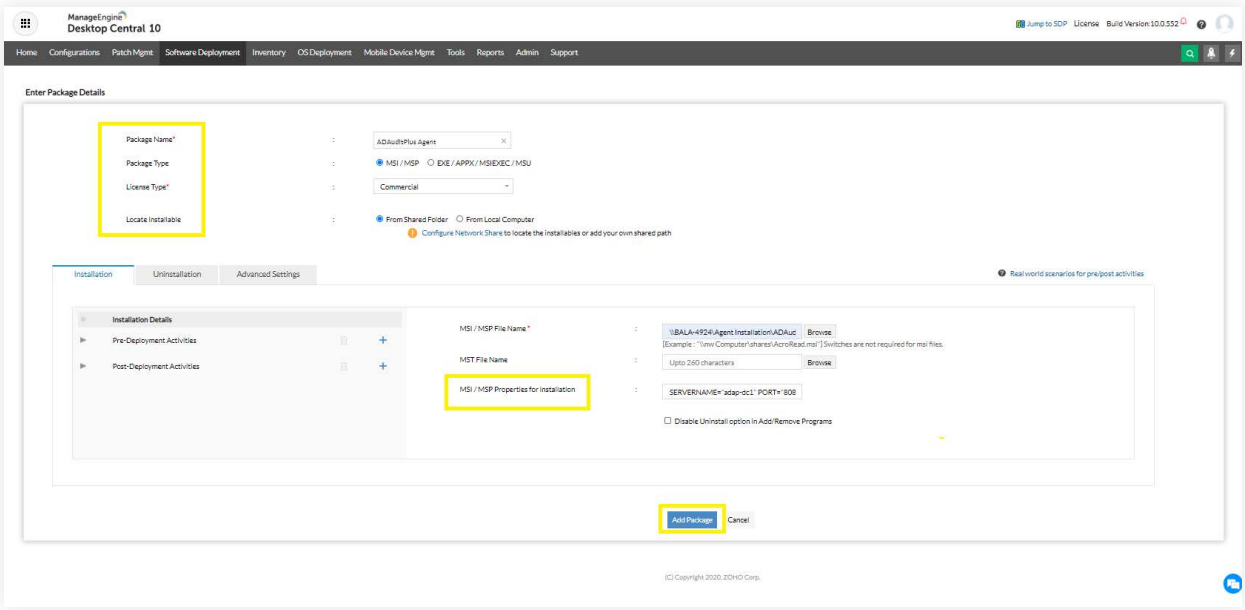
- beside **MSI/MSP Properties for installation:**

For example, msiexec /i \\Steven-10123\ADAuditPlusAgent-x64.msi PROTOCOL=HTTPS PORT=8444 SERVERNAME=Steven-10123 SERVERFQDN=Steven-10123.adap.internal.com SERVERIP=192.168.225.33 OrgAccessKey=ADCFDA98-8FDD-45E4-90BC-E3D20B029870 /q

Here, **ServerName** refers to the name of the server where ADAudit Plus/NAT device is hosted.
ServerIP refers to the IP address of the server where ADAudit Plus/NAT device is hosted.
Protocol refers to the protocol used for agent to server communication (HTTPS by default).
Port refers to the port number used for agent to server communication (8555 by default).
OrgAccessKey refers to the key used for agent to server communication (unique to each organization).
ServerFQDN refers to the FQDN of the server where ADAudit Plus/NAT device is hosted. For example, if ADAudit Plus is hosted on a DC named adap-dc2 in the adap.internal.com domain, the ServerFQDN is adap-dc2.adap.internal.com.

Note: To find the ServerName, Port, Protocol, and OrgAccessKey used by ADAudit Plus, click here.

- Click **Add Package.**



2. Deploy the MSI package

i. In the Endpoint Central console, click **Software Deployment > Install/Uninstall Software > Windows > Computer Configuration.**

ii. Provide the below details:

Beside *Name,* enter **ADAudit Plus deployment** or any other name of your choice.

Beside *Package Name*, select the **package.**

Beside *Operation Type*, select **Install** from the drop-down.

Beside *Define Target*, select the **Remote Office/Domain** and specify the **Computer.**

iii. Click **Deploy.**

Note: Reboot of server is not required after agent installation.

4. Agent security settings

Agent to server communication can be secured via token based authentication from build 7060 onwards. These are the 2 agent security settings that can be configured:

1. Disallow unauthenticated agent to server communication

All agent to server communication prior to build 7060 happens without authentication.

To disallow unauthenticated agent to server communication:
Navigate to the **Admin** tab > **Configuration > Agent Settings > Agent Security Settings** > Tick the checkbox against **Disallow unauthenticated agent to server communication.**

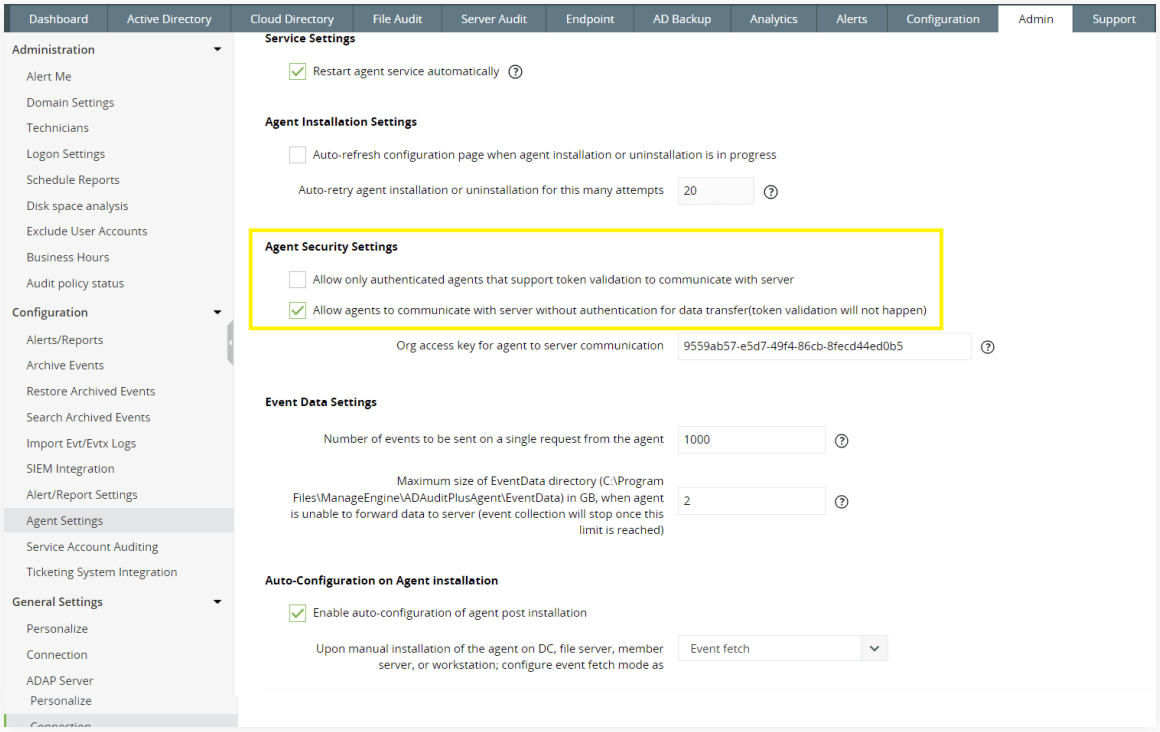
Note: If you tick this checkbox (Disallow un-authenticated agent to server communication), all the agents in your environment must be upgraded to version 7060 and above.

2. Allow the agent to forward data without authentication

Authentication has been disabled for data forwarding by default, to avoid performance issues.

To disallow the agent to forward data without authentication :
Navigate to the **Admin** tab > **Configuration > Agent Settings > Agent Security Settings** > Untick the checkbox against **Allow the agent to forward data without authentication.**

Note: If you untick this checkbox (Allow the agent to forward data without authentication), you might face performance issues.



5. Agent configuration sync

ADAudit Plus immediately syncs any configuration change occurring on the server with the agent, and checks if configurations are in sync every 30 minutes.
ADAudit Plus checks the agent service status every 30 minutes and restarts the service if it has stopped.

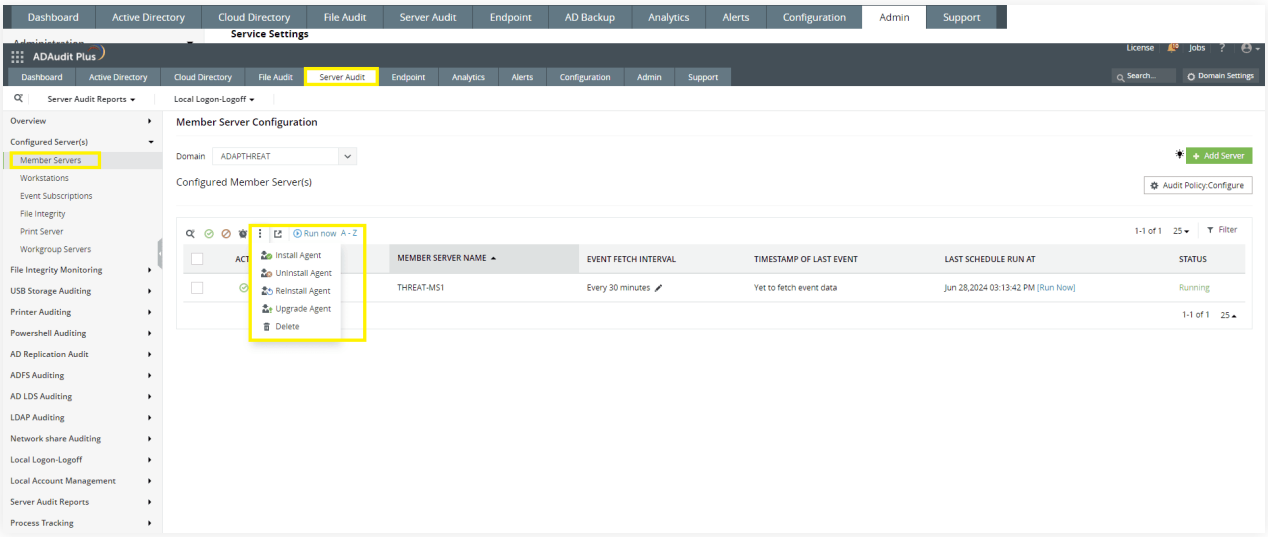
Note: Automatic restart in case service goes down, can be configured from the **Agent Settings** tab found under the Admin page in the product console.

6. Upgrading the agent

If there is a newer version of the agent available, ADAudit Plus automatically attempts to upgrade the agent, but this requires the service account to be a member of the ***Domain Admins*** group.

If the service account does not have Domain Admin privileges, then you need to manually upgrade the agent by uninstalling the current agent and installing the new version by following step 3.2.
Please check the release notes to find the newest version of the agent.

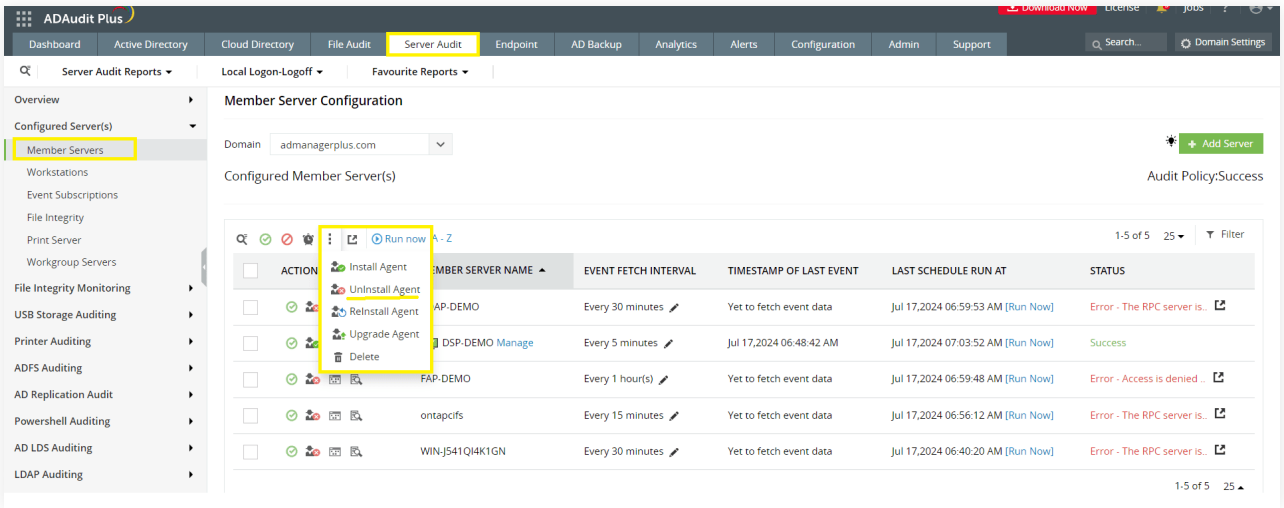
Note: You can also initiate the agent upgrade manually from the relevant configuration tab in the product.



7. Agent uninstallation

7.1 Uninstalling the agent via ADAudit Plus' UI

The agent can be uninstalled by selecting the computers you wish to uninstall the agent from as shown in the image below.



7.2 Uninstalling the agent manually

7.2.1 Uninstalling the agent via Group policy

i. Log in to any computer that has the Group Policy Management Console (GPMC), with Domain Admin credentials > Open the GPMC.

ii. Navigate to your domain > If the agent was deployed through a GPO, right-click the GPO. If the agent was deployed through any other means, create a new GPO and right-click > Select **Edit > Computer Configuration > Policies > Software Settings > Software Installation** > Navigate to the right pane, right-click the software package, click Remove.

iii. In the **Remove Software** dialog box, check **Immediately uninstall the software from users and computers,** and click **OK.**
The agent will uninstall when the client computers are restarted.

7.2.2 Uninstalling the agent via command line

On the target computer, open an elevated Command Prompt (right-click Command Prompt and select **Run as administrator**). Execute:
msiexec /x {7AFB5C7B-DAD9-49A3-BA7E-DF7432E78E5C} /q (for 32-bit) or
msiexec /x {3D502EF5-54BD-426E-A183-0724645371B3} /q (for 64-bit).

7.2.3 Uninstalling the agent via Endpoint central

Note: Refer to the steps shown in the create an MSI package via Endpoint Central section of this guide to uninstall the agent using package creation details.

To uninstall the agent, you need to create an MSI package using the below steps.
(i) Log in to your Endpoint Central console as an administrator and click **Software Deployment.**
(ii) In the left pane, under **Deployment**, select **Install/Uninstall software > Windows > Computer Configuration.**
(iii) Beside *Name*, enter **ADAudit Plus uninstallation** or any other name of your choice.
(iv) Under **Install/Uninstall Windows Software > Package Settings**, do the following:
- Beside *Operation type*, choose **Uninstall.**
- Beside *Package Name*, select the **ADAPAgent** package.

(v) Under **Define Target**, select the name of the **Domain** to which the target server belongs.
(vi) Click the **filter icon** beside the *Remote Office/Domain* field to include and/or exclude target computers based on your requirements.
(vii) Click **Deploy** to uninstall the agent.

7.2.4. Uninstalling the agent via the Control Panel in the target computer

To uninstall the ADAudit Plus agent locally:

(i) Go to **Control Panel > Programs > Uninstall a program.**

(ii) Right-click **ADAuditPlusAgent.**

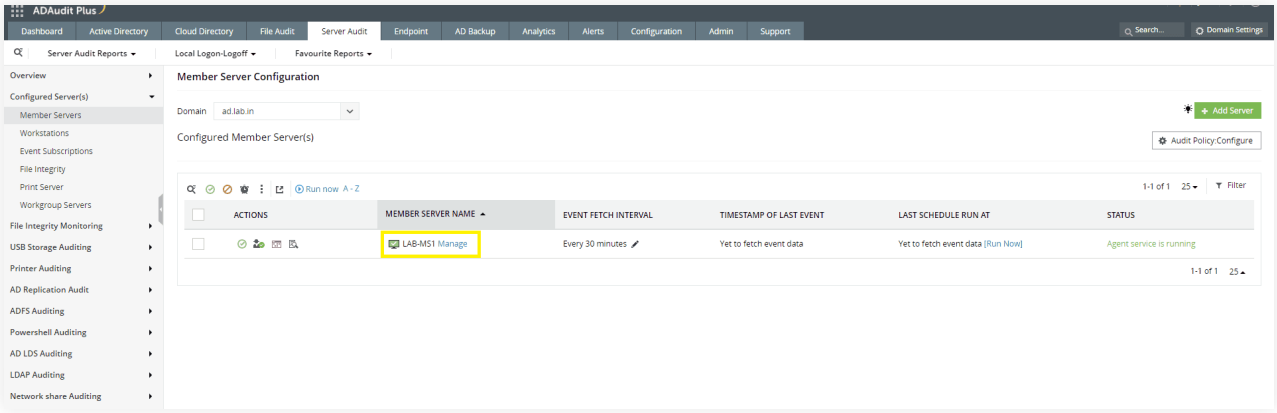
(iii) Select **Uninstall.**

8. Troubleshooting

The **Manage Agent** page allows you to monitor and manage the installed agent.

Please check the following while troubleshooting the agent service.

1. Check if the agent service is installed and running on the desired computer.
   a. Under *Configured Servers*, click **Manage** to bring up the **Manage Agent** page.



   b. Refresh the **Agent Service table.**
   c. Check the **Agent Service table.**
   d. If the service has stopped, start the **service.**

   (**Note:** The ADAudit Plus service account should be a member of the **Domain Admins** group in order to get the service status.)

2. Check if the agent is able to communicate with the ADAudit Plus server.
   a. Go to the **Agent Communication table.**
   b. Refresh the **Agent Communication table.**
   c. Check if communication is established.

   Note:

   i. An RPC connection is required to sync configuration settings on the agent with the ADAudit Plus server.

   ii. An HTTP connection needs to be established in order for the agent to forward event data to the ADAudit Plus server.

d. If an error persists, test RPC and HTTP communication by clicking on the corresponding icons under **Actions.**

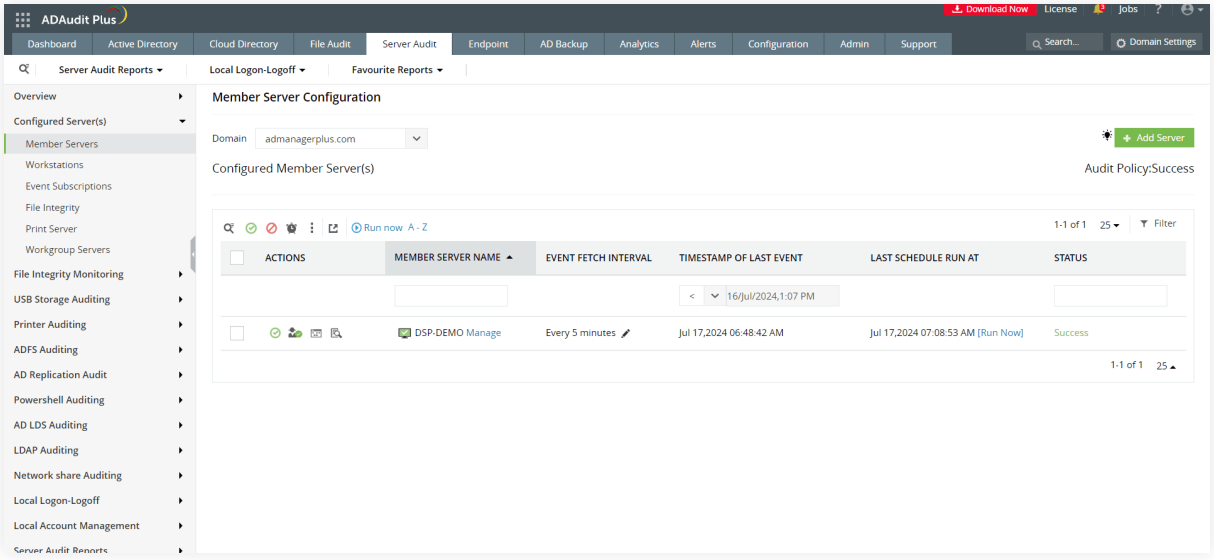
e. If HTTP communication fails, open the machine on which the ADAudit Plus agent is installed, and connect to the ADAudit Plus server via a web browser. Enter **ADAuditPlus_Protocol://ADAuditPlus_server_name:ADAuditPlus_running_port_number** (eg. HTTPS://server_name:8081) in a web browser to connect to the ADAudit Plus server.

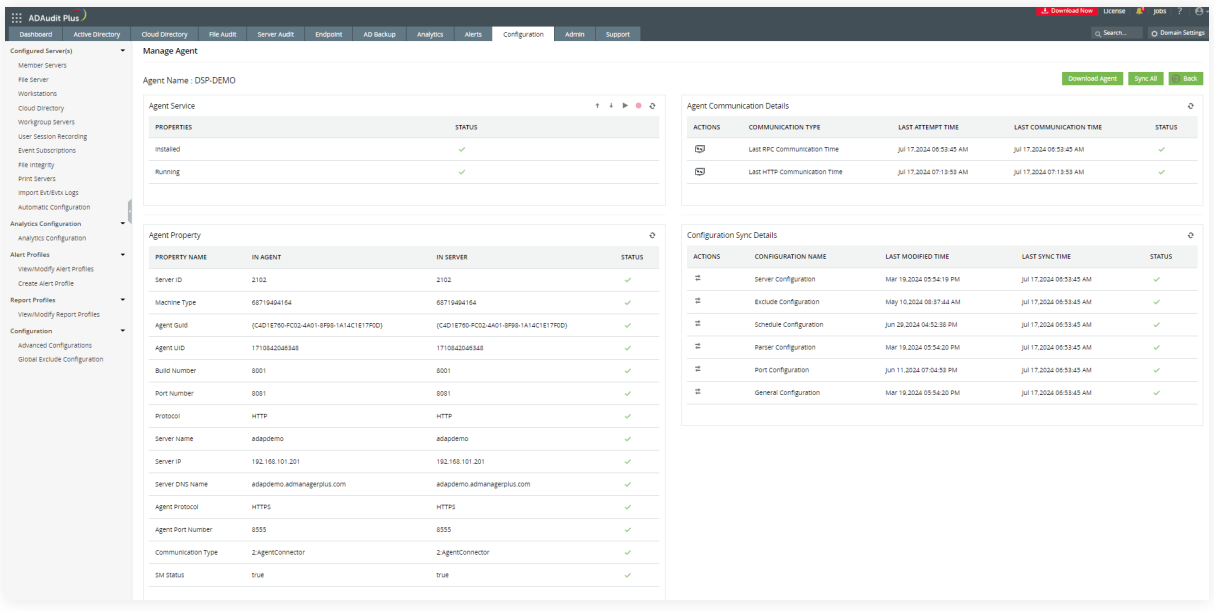
   i. If you are unable to connect to the ADAudit Plus server, check the firewall settings (outbound) on the machine where the agent is installed.

f. If communication is established, refresh the **Agent Property table** to check if the agent properties match the properties on the server.

   i. If you are unable to refresh the **Agent Property table** check the **Remote Registry Service** status on the machine where the agent is installed, and if it has been stopped, start the service.

   ii. Also, refresh and check the **Configuration Sync Details table** to ensure that the most recent changes have been synced.





If the error persists, please contact support, and one of our technicians will help you resolve the issue.

9. List of errors that may arise while installing the agent and the solutions to resolve them:

1. The network path was not found

2. Couldn't copy ADAuditPlusAgent.msi / Access Denied: failed to connect to ADMIN$ share

3. Another installation is already in progress (0x652)

4. The system cannot find the file specified (0x2)

5. Fatal error occurred (0x643)

6. "RemCom.exe' is not recognized as an internal or external command, operable program or batch file

7. Could not install client software

8. Could not connect to the machine

9. Initiating connection to remote service failed

10. Logon failure: The target account name is incorrect

11. Logon failure: unknown user name or bad password

12. Could not start remote service

13. Another version of the product is already installed (0x666)

14. Product is uninstalled (0x64E)

15. No communication available from agent to server. Last event read time:{recent event time}

16. No communication available from agent to the server (initial profile fetch not happening)

17. Incorrect function

18. Hexadecimal value 0x05, is an invalid character

1. The network path was not found

Causes:

This error occurs when:

- The target computer cannot be contacted.

- The service account used to run ADAudit Plus does not have sufficient privileges to access the admin share (\\server_name\admin$) on the target computer.

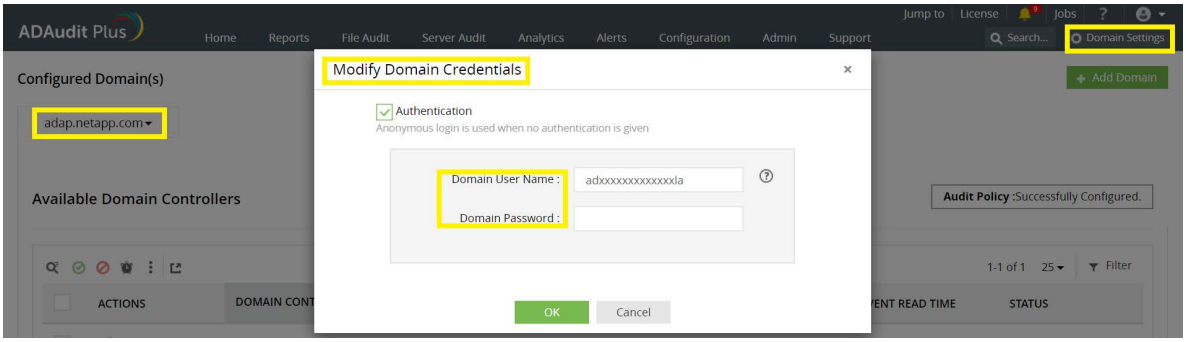
Solution:

- Ensure that there are no connectivity issues between the server (where ADAudit Plus has been installed) and the target computer.

- Check if you are able to access the admin share on the target computer, using the service account used to run ADAudit Plus. If you are unable to, configure **Domain Settings** (in the ADAudit Plus console) and the **Log on** tab (of ADAudit Plus service) with a user account that has privilege to access the admin share (\\server_name\admin$) on the target computer.

Note:

- To configure user account in Domain Settings page, log in to the ADAudit Plus console > **Domain Settings.** Hover over the relevant domain, click **Modify Credentials**, and enter the credentials.



- To configure user account in Log on tab, click the **Start** icon, select **Services**, navigate to **ManageEngine ADAudit Plus**, right-click **Properties > Log On > This account** and enter the credentials.

2. Couldn't copy ADAuditPlusAgent.msi / Access Denied: failed to connect to ADMIN$ share

Causes:

This error occurs when:

- The service account used to run ADAudit Plus does not have sufficient privileges to access the admin share (\\server_name\admin$) on the target computer.

- The ADMIN$ share access limit has been exceeded.

Solution:

- Check if you are able to access the admin share on the target computer, using the service account used to run ADAudit Plus. If you are unable to, configure the **Domain Settings** (in the ADAudit Plus console) and the **Log on** tab (of ADAudit Plus service) with a user account that has privilege to access the admin share (\\server_name\admin$) on the target computer.

- Navigate to **Shared Folders Microsoft Management Console (MMC)** snap-in > **Shares > ADMIN$ > Properties**, and set an appropriate value for the **User limit.**

Note:

- To configure user account in Domain Settings page, log in to the ADAudit Plus console > Domain Settings, hover over the relevant domain, click Modify Credentials, and enter the credentials.

- To configure user account in Log on tab, click the Start icon, select Services, navigate to ManageEngine ADAudit Plus, right-click Properties > Log On > This account and enter the credentials.

3. Another installation is already in progress (0x652)

Causes:

- This error occurs when the installation of another MSI file is in progress on the target computer.

Solution:

- Wait for a few minutes and try to install the agent again.

- If you have not initiated the installation of any software, you can also run this command in the command prompt: **taskkill /im /f msiexec.exe** to kill any MSI installation running on the target compute.r

4. The system cannot find the file specified (0x2)

Causes:

- This error occurs when the service account is unable to locate the ADAuditPlusAgent-x86.msi or ADAuditPlusAgent-x64.msi files.

Solution:

- Check if you are able to access the admin share on the target computer, using the service account used to run ADAudit Plus. If you are unable to, configure **Domain Settings** (in the ADAudit Plus console) and the **Log on** tab (of ADAudit Plus service) with a user account that has privilege to write files to the SYSTEMDRIVE\Windows directory on the target computer.

Note:

- To configure user account in Domain Settings page, log in to the **ADAudit Plus console > Domain Settings**, hover over the relevant domain, click **Modify Credentials**, and enter the credentials.

- To configure user account in Log on tab, click on the **Start** icon > **Services**, navigate to **ManageEngine ADAudit Plus,** right-click **Properties > Log On > This account**, and enter the credentials.

- Also, ensure that ADAuditPlusAgent-x86.msi or ADAuditPlusAgent-x64.msi file is present in SYSTEMDRIVE\Windows directory on the target computer.

Note: For 32-bit versions, it is ADAuditPlusAgent-x86.msi and for 64-bit versions, it is ADAuditPlusAgent-x64.msi.

5. Fatal error occurred (0x643)

Causes:

This error could occur due to multiple reasons:

- The drive that contains the folder that you are trying to install the package to is accessed as a substitute drive.

- Windows Installer is attempting to install an app that is already installed on your PC.

- The SYSTEM account does not have Full Control permissions on the folder that you are trying to install the Windows Installer package to.

Solution:

- **On the target computer, ensure the following:**
  - .Net 4.5 framework and above is installed.
  - ADAudit Plus has already not been installed.

- Check if you are able to access the admin share on the target computer, using the service account used to run ADAudit Plus. If you are unable to, configure **Domain Settings** (in the ADAudit Plus console) and the **Log on** tab (of ADAudit Plus service) with a user account that has privilege to write files to the SYSTEMDRIVE\Windows directory.

Note:

- To configure user account in Domain Settings page, log in to the **ADAudit Plus console > Domain Settings**, hover over the relevant domain, click **Modify Credentials**, and enter the credentials.

- To configure user account in Log on tab, click on the **Start** icon, select **Services**, navigate to **ManageEngine ADAudit Plus**, right-click **Properties > Log On > This account**, and enter the credentials.

Next, start and re-register Microsoft Installer service on the target computer. To do this, press **Windows + R**, type **msiexec /unregister** and hit **Enter**. Again press **Windows + R**, type **msiexec /register** and hit **Enter.**

If the issue persists, try resolving it using the Program Install and Uninstall troubleshooter.

6. RemCom.exe' is not recognized as an internal or external command, operable program or batch file

Causes:

- This error occurs when the Remcom.exe file, which is used to install the agent on target computer, has been flagged and deleted by an antivirus software.

Solution:

- Check if the Remcom.exe file exists in the bin folder of ADAudit Plus Installation directory (<Installation-directory>bin) on the target computer. If not, check if your antivirus software has removed the file. If yes, configure your antivirus software to trust the Remcom.exe file. Then, contact support to get the Remcom.exe file.

7. Could not install client software

Causes:

- This error occurs because of a network timeout while installing the agent.

Solution:

- Ensure that the network connection is re-established and try to install the software again.

8. Could not connect to the machine

Causes:

- This error occurs when the target computer cannot be contacted.

Solution:

- Check if you are able to ping the target computer from the server where ADAudit Plus has been installed. If you aren't able to, fix the underlying connectivity issue. If you are able to ping the target computer, contact support for further assistance.

9. Initiating connection to remote service failed

Causes:

- This error occurs when the service cannot be created on the target computer.

Solution:

- Check if you are able to ping the target computer from the server where ADAudit Plus has been installed. If you aren't able to, fix the underlying connectivity issue.

- If you are able to ping the target computer, ensure that Remote Registry service is running on the target computer.

- Next, check if you are able to access the admin share on the target computer, using the service account used to run ADAudit Plus. If you are unable to, configure **Domain Settings** (in the ADAudit Plus console) and the **Log on** tab (of ADAudit Plus service) with a user account that has privilege to create a service on the target computer.

Note:

- To configure user account in Domain Settings page, log in to the **ADAudit Plus console > Domain Settings**, hover over the relevant domain, click **Modify Credentials**, and enter the credentials.

- To configure the user account in the Log on tab, click the **Start** icon, select **Services**, navigate to **ManageEngine ADAudit Plus**, right-click **Properties > Log On > This account**, and enter the credentials.

If the issue still persists, contact support.

10. Logon failure: The target account name is incorrect

Causes:

- This error occurs when the service account used to run ADAudit Plus is locked or disabled or its password has been changed.

Solution:

- Check if you are able to access the admin share on the target computer, using the service account used to run ADAudit Plus. If you are unable to, configure **Domain Settings** (in the ADAudit Plus console) and the **Log on** tab (of ADAudit Plus service) with appropriate user account credentials.

Note:

- To configure user account in Domain Settings page, log in to the **ADAudit Plus console > Domain Settings**, hover over the relevant domain, click **Modify Credentials**, and enter the credentials.

- To configure the user account in the Log on tab, click the **Start** icon, select **Services**, navigate to **ManageEngine ADAudit Plus**, right-click **Properties > Log On > This account**, and enter the credentials.

11. Logon failure: Unknown user name or bad password

Causes:

- This error occurs when the name or password of the service account used to run ADAudit Plus is incorrect.

Solution:

- Check if you are able to access the admin share on the target computer, using the service account used to run ADAudit Plus. If you are unable to, configure **Domain Settings** (in the ADAudit Plus console) and the **Log on** tab (of ADAudit Plus service) with appropriate user account credentials.

Note:

- To configure user account in Domain Settings page, log in to the **ADAudit Plus console > Domain Settings**, hover over the relevant domain, click **Modify Credentials**, and enter the credentials.

- To configure the user account in the Log on tab, click the **Start** icon, select **Services**, navigate to **ManageEngine ADAudit Plus**, right-click **Properties > Log On > This account**, and enter the credentials.

12. Could not start remote service

Causes:

- This error occurs when the service account used to run ADAudit Plus does not have the privileges to start the service in the target computer.

Solution:

- Check if you are able to access the admin share on the target computer, using the service account used to run ADAudit Plus. If you are unable to, configure **Domain Settings** (in the ADAudit Plus console) and the **Log on** tab (of ADAudit Plus service) with a user account that has Domain Admin privileges.

Note:

- To configure user account in Domain Settings page, login to the **ADAudit Plus console > Domain Settings** > Hover over the relevant domain, click on **Modify Credentials** > Enter credentials.

- To configure user account in Log on tab, click the **Start** icon, select **Services**, navigate to **ManageEngine ADAudit Plus**, right-click **Properties > Log On > This account**, and enter the credentials.

13. Another version of the product is already installed (0x666)

Causes:

- This error occurs when another version of the agent is already installed in the target computer.

Solution:

- Uninstall the existing agent from the target computer by clicking on the **Uninstall** icon under the relevant configuration page in the ADAudit Plus console. Then, retry the current installation.

14. Product is uninstalled (0x64E)

Causes:

- This error occurs when the agent has already been uninstalled by some other method, such as manual uninstallation.

Solution:

Install the agent via the ADAudit Plus UI. Then, try to uninstall the agent again.

15. No communication available from agent to server. Last event read time:{recent event time}

Causes:

- This error occurs when there is no communication from agent to server, for past 'N' hours.

Solution:

- On the target computer, check if you are able to access the ADAudit Plus web console via a browser. To do this, open any web browser and in the address bar, type: **Protocol://ServerName:Port**

Here, **ServerName** refers to the name of the server where ADAudit Plus/NAT device is hosted.
Protocol refers to the protocol used for agent to server communication (HTTPS by default).
Port refers to the port number used for agent to server communication (8555 by default).

Note:

- To find the ServerName, Port, and Protocol used by ADAudit Plus, click here.

- If the issue persist, contact support.

16. No communication available from agent to the server (initial profile fetch not happening)

Causes:

- This error occurs when there is no communication from the agent to the server, immediately after installation.

Solution:

- On the target computer, check if you are able to access the ADAudit Plus web console via a browser. To do this, open any web browser and in the address bar, type: **Protocol://ServerName:Port**

Here, **ServerName** refers to the name of the server where ADAudit Plus/NAT device is hosted.
Protocol refers to the protocol used for agent to server communication (HTTPS by default).
Port refers to the port number used for agent to server communication (8555 by default).

Note:

- To find the ServerName, Port, and Protocol used by ADAudit Plus, click here.
- If the issue persist, contact support.

17. Incorrect function

Causes:

If the installation process gets quit abruptly, it could be due to the following two reasons:

- Shutdown/log off of the target computer has been initiated even while the installation is in progress.
- There is not enough space in the target computer to install the software.

Solution:

- Ensure shutdown/log off is not initiated in the target computer, while the agent is getting installed.
- Ensure there is sufficient hard disk space available in the target computer before initiating agent installation.

18. Hexadecimal value 0x05, is an invalid character

Causes:

- This error occurs when the agent is unable to read events.

Solution:

- Upgrade to the any build on or above 6058, if the error persists, contact support.