Solution to scan error "RPC server is not available".

For network scanning using AIT, the current IT infrastructure as well as the current security policies and configurations must be taken into account. In addition, it should be verified whether the PCs to be scanned are connected to the LAN directly or indirectly (VPN). The following is a procedure for troubleshooting scanning problems when you get the error "RPC server is not available".

Steps for the solution of this scanning error:

1. Depending on whether a domain name was specified at the time of scanning and if IP ranges were used, it is important to determine whether the IP address from which this error is reported is a Windows device or a network device or other, because if it is not a Windows device then AIT will not find the WMI service running and therefore it is normal to report this error.
2. If it is a Windows device reporting this error, it is important to understand if the PCs are available on the network i.e. if they respond to ping (ping works if ICMP protocol is enabled). To do this check we suggest using the following PowerShell script that allows to perform a mass ping taking as reference the AD_Computers.txt file created by AIT. Considering the approximate total number of PCs, compare the number of PCs that respond to the ping. If the number of PCs responding to the ping is low then the cause of the scan error may be that the PCs are not connected to the network or are in an unreachable VLAN. On the other hand, if the number of PCs responding to the ping is close to the total number of PCs, the cause of the scan error is due to port blocking by the firewall in use on each PC targeted by the scan.

```
$PCName = Get-Content "C:\ProgramData\Autodesk\AIT\AD_Computers.txt"
$Successfulping = New-Item c:\Successfulping.txt -ItemType "file" -force
$Failedping = New-Item c:\Failedping.txt -ItemType "file" -force

foreach ($PC in $PCName) {

        if (test-Connection -ComputerName $PC -Count 1 -Quiet ) {
            "$PC is Pinging "
             Add-Content -path $Successfulping -value "$PC is Pinging"

                    } else

                    {
                    "$PC not pinging"
                    Add-Content -path $Failedping -value "$PC not pinging"

                    }
}
```

3. When determining that the firewall is the cause of the scanning error it should be verified whether the firewall in use on each PC targeted by the scan is managed by Windows or is a different security solution to Windows as this determines where technical adjustments should be made to the existing firewall rules. AIT obtains the inventory of Autodesk products by querying various Windows operating system data points using WMI (Windows Management Instrumentation) which is the management infrastructure built into Windows operating systems. When AIT obtains the IP of each PC it attempts to connect to UDP ports 137,138, TCP 135,139 and 445 on each PC it attempts to scan. AIT connects to the RPC Endpoint Mapper service on TCP port 135 and RPC Endpoint Mapper tells it which WMI port it is listening under, the port number is random and can be between the ranges 1025-5000 or 49152-65535 . It must be ensured that the machines firewall is configured correctly to allow all WMI traffic. Opening specific ports is not sufficient, as traffic is sent through random ports as mentioned above.

4. If the firewall is managed by Windows, a quick check that can be performed is to locally enable the required port exceptions on a single PC and then launch a AIT scan directed only to that PC to verify if the network scan is successful. For this check the following commands must be executed as administrator in a command prompt window on that selected test PC

```
call netsh firewall set service RemoteAdmin enable
call netsh firewall add portopening protocol=tcp port=135 name=DCOM_TCP135
```

If after executing these commands and launching AIT a successful scan is obtained then it is verified that settings must be made in the Windows firewall of the PCs. To extend this setting to all PCs it is recommended to create an active directory group policy see group policy settings to allow inbound remote administration.

5. If the firewall is managed by a security solution other than Windows, you must log into the management console of that solution and edit the current firewall rule allowing PCs to receive requests on the ports required by AIT see AIT TCP/IP communication flow in network scans.

6. If after performing this procedure the error "RPC server is not available" persists, please undo any changes made and proceed to configure AIT with other methods:

- Logon / Startup Script Scan Setup
- Deploying with Microsoft System Center (SCCM)
- Zip File Scan Method

For more information about RPC and details about troubleshooting go to the following link: https://social.technet.microsoft.com/wiki/contents/articles/4494.windows-server-troubleshooting-rpc-server-is-unavailable.aspx

Group policy to allow inbound remote administration

1. On the Active Directory server, open the group policy manager
2. Right-click on the selected domain forest, or organizational unit, create a new GPO, for traceability, it is recommended to name it "Autodesk Inventory Tool"
3. Once the GPO is created, right click on it and select "Edit"
4. In the group policy editor go to the path: (check according to your operating system and language configured).

```
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Defender Firewall\Domain Profile
Computer Configuration\Administrative Templates\Network\Network Connections\Windows
Firewall\Domain Profile
```

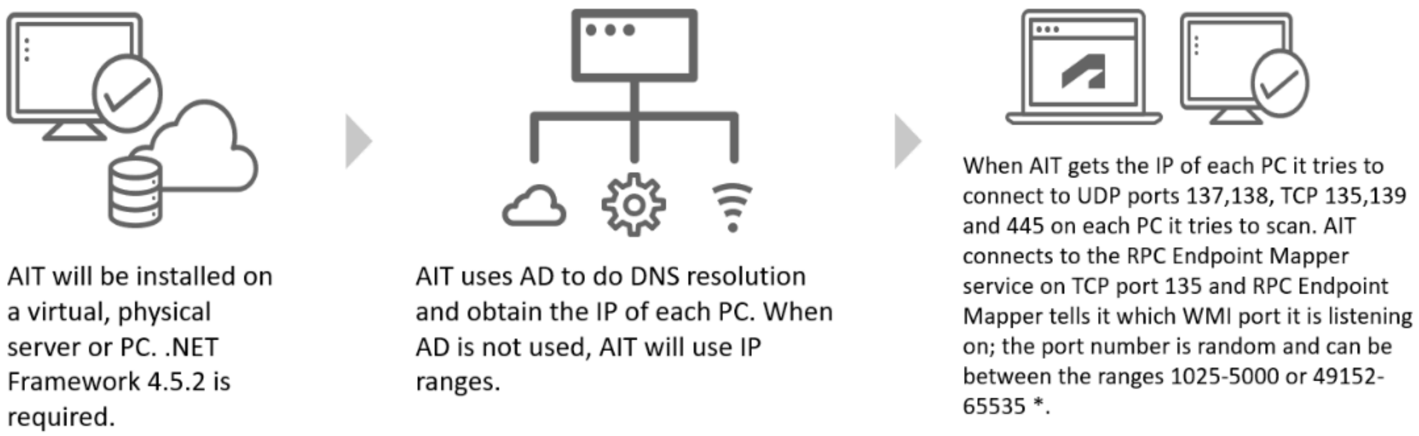
5. Once there, configure the GPO according to the operating system and language configured:

```
Windows Defender Firewall: Allow inbound remote administration exception
Windows Firewall: Allow inbound remote administration exception
Windows Firewall: Allow remote administration exception
```

6. Once selected right-click and select "Edit", in the configuration select "Enabled". In the configuration options where it says "Allow unsolicited incoming messages from these IP addresses" in the text box put the IP address of the server or PC where AIT is installed.

AIT TCP/IP communication flow in network scans

The following is a diagram of the network communication performed by AIT when scanning over the network



AIT will be installed on a virtual, physical server or PC. .NET Framework 4.5.2 is required.

AIT uses AD to do DNS resolution and obtain the IP of each PC. When AD is not used, AIT will use IP ranges.

When AIT gets the IP of each PC it tries to connect to UDP ports 137,138, TCP 135,139 and 445 on each PC it tries to scan. AIT connects to the RPC Endpoint Mapper service on TCP port 135 and RPC Endpoint Mapper tells it which WMI port it is listening on; the port number is random and can be between the ranges 1025-5000 or 49152-65535 *.

*To make the configuration secure, requests on these ports should be allowed only from the IP address of the PC or server where AIT is installed.