



Preparing the Customer Network for Installation

These instructions provide information to help identify, troubleshoot, set up and configure the components of the customer network in order to obtain the best possible results from the installation of the MicroConvergent Sensor or Agent. The customer information we require is also identified.

Ports Required by the Sensor

Networks in which sensors and agents are deployed need to have the following outbound ports open:

- **HTTP (Port 80)** for software downloads (scripts, management tasks)
- **HTTPS (Port 443)** for secure data transmission between the agent/sensor and the Central MicroConvergent server
- **SSH (Port 22)** is required for device remote control

Configuring Windows Management Instrumentation (WMI) Permissions at the Domain Level

Many of the services in the Sensor (and asset discovery capabilities) use WMI to gather information. Unfortunately, in most cases, the Microsoft Personal Firewall is enabled by default, thereby causing WMI queries to fail. This section outlines how to set up a customer network to allow WMI queries. These steps should be completed before attempting to install a Sensor and setting up and implementing an asset discovery .

Accessing Group Policy

The steps required to access the group policy of the domain will vary depending on whether the domain controller is running Windows 2003 or Windows Small Business Server (SBS):

For **Windows SBS**, carry out the following:

1. Navigate to Start Menu > Administrative Tools > Server Management.
2. Expand the **Advanced Management** node.
3. Expand the **Group Policy Management** node.
4. Expand the **Forest: "Domain Name"** node, where "Domain Name" is the name of the domain you wish to modify.
5. Expand the **Domains** folder.
6. Right-click on the **"Domain Name"** node in the left-hand pane and select **"Create and Link a GPO Here..."** to link a group policy object (GPO).

7. Name the new policy "*WMI Permissions*".
 8. Click on the "**Domain Name**" node in the left-hand pane, ensure that the "*WMI Permissions*" policy is highlighted and click on the button until the policy has a Link Order of 1.
-

For **Windows 2003** with **Group Policy Management Console (GPMC)**, carry out the following:

1. Navigate to Start Menu > Administrative Tools > Group Policy Management.
 2. In the left-hand pane, navigate to **Forest: "Domain Name" -> Domains -> "Domain Name"**, where "Domain Name" is the name of the domain you wish to modify.
 3. Right-click on "**Domain Name**" in the left-hand pane and select "**Create and Link a GPO Here...**".
 4. Name the new policy "*WMI Permissions*".
 5. Ensure that the "*WMI Permissions*" policy is highlighted and click on the button until the policy has a Link Order of 1.
-

For **Windows 2003 without Group Policy Management Console (GPMC)**, carry out the following:

1. Navigate to **Start Menu > Administrative Tools > Active Directory Users and Computers**.
 2. Right-click on the name of your domain in the left-hand pane and select **Properties**.
 3. Click on the **Group Policy** tab.
 4. Click **New** and name the new policy "*WMI Permissions*".
 5. Ensure that the "*WMI Permissions*" policy is highlighted and click on the **Up** button.
-

Configuring Distributed Component Object Model (DCOM) Permissions

1. Navigate to the "*WMI Permissions*" group policy, either by the "**Group Policy Management**" plug-in or by the "**Active Directory Users and Computers**" plug-in.
2. Ensure that the "*WMI Permissions*" policy is highlighted and click on the **Edit** button.
3. Navigate to Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options.
4. In the right-hand UI pane, double-click on DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax.
5. Put a checkmark in the box beside **Define this policy setting**.
6. Click on the **Edit Security** button.

7. Click on the **Add** button; in the resulting pop-up window, specify the domain administrator account that is used by the MicroConvergent Windows Sensor (i.e. "microconvergensensor").
8. Click **OK**.
9. In the **Group or user names** field, select the domain administrator you specified in step #7.
10. In the **Permissions for Administrators** field, ensure that there is a checkmark in the **Allow** column for the **Remote Access** option.
11. Click **OK**.
12. Click **OK**.
13. In the right-hand UI pane, double-click on DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax.
14. Put a checkmark in the box beside **Define this policy setting**.
15. Click on the **Edit Security** button.
16. Click on the **Add** button; in the resulting pop-up window, specify the domain administrator account that is used by the MicroConvergent Windows Sensor
17. Click **OK**.
18. In the **Group or user names** field, select the domain administrator you specified in step #16.
19. In the **Permissions for Administrators** field, ensure that there is a checkmark under the **Allow** column for both **Remote Launch** and **Remote Activation**.
20. Click **OK**.
21. Click **OK**.
22. Close the Group Policy Object Editor window.
23. Click **OK** and close the **Active Directory Users and Computers** window.

Note: All steps outlined have been sourced from Microsoft articles available on the Internet.

Note: The specific security rights outlined are sourced from the Microsoft document titled [Securing a Remote WMI Connection](#).

Enabling the Remote Administration Exception in Windows Firewall

1. Navigate to the **Group Policy Management** plug-in and edit the “*WMI Permissions*” group policy, as outlined in the **Windows SBS** section or the **Windows 2003** section of these instructions.
2. Navigate to Computer Configuration -> Administrative Templates -> Network -> Network Connections -> Windows Firewall -> Domain Profile.
3. In the right-hand UI pane, double-click on Windows Firewall: Allow remote administration exception.
4. Under the **Settings** tab, click on the **Enabled** radio button.
5. In the Allow unsolicited incoming messages from: text field, input * to accept messages from anyone, or the IP address of your Windows Sensor.
6. Click **OK**.
7. Close the Group Policy Object Editor window.
8. Close the Active Directory Users and Computers window.

Note: This section does not need to be followed if Windows Firewall is not enabled on the network.

Note: The steps outlined in the above section are sourced from the Microsoft document titled [Enable or Disable the Remote Administration Exception](#).

Any changes made to the group policy of a domain will not be applied by members of the domain until one of the following conditions is met:

- The computer is rebooted, or
- The default update interval has been exceeded (90 minutes on domain members, and five minutes for domain controllers), or
- The following command is run on the domain member: **gpupdate /Target: computer**.

Note: Information regarding the group policy update interval and the gpupdate command is sourced from the Microsoft knowledge base document titled [A Description of the Group Policy Update Utility](#).
Working with Proxy Servers

Agents and Sensors are capable of communicating through non-authenticating proxy servers, clear-text authenticating proxy servers, and Internet Security and Acceleration (ISA) 2000/2004 proxy servers. If a proxy server resides on your customer's network, you may need to configure the MicroConvergent Agent/Sensor software so that it can pass information through the proxy server to our Central Server.

To configure an agent/sensor to use a proxy string, specify the proxy string during the creation of the agent/probe in the MicroConvergent UI. The next three sections will outline the appropriate proxy string to enter, based on the type of proxy server implemented in our customer's network.

Non-authenticating Proxies

The proxy string must have the following format:

http://<server name>:<port number>
https://<server name>:<port number>

Example: https://192.168.0.10:8080

Clear-text Authenticating Proxies

The proxy string must have the following format:

http://<proxy user>:<proxy password>@<server name>:<port number>
https://<proxy user>:<proxy password>@<server name>:<port number>

Example: https://jmroz:Password@192.168.0.10:8080

ISA 2000/2004 Proxies

The proxy string must have the following format:

https://<domain of the proxy>\<proxy user in domain>:<proxy password in domain>@<server name>:<port number>

Example: https://OFFICE\jmroz:Password@192.168.0.10:8080

Note: Basic HTTP authentication must be turned on for this to work, refer to the Microsoft Knowledge Base document titled [How to Allow Third-Party Internet Application Connections through ISA Server 2000](#) (specifically, Method 2: Enable Basic Authentication for Outgoing Web Requests).

Caution: The procedure explained above and in the Microsoft KB document should be reviewed, approved and implemented by a Microsoft Certified Professional holding a “Microsoft Certified Systems Engineer + Internet” or equivalent designation or experience.

Confirm with our customer that the following operations are considered permissible. **Do not proceed without customer consent.** It is also possible to configure an ISA server to permit direct access which will allow the agents and sensors to communicate with the MicroConvergent Central Server.

Advanced: Working with Simple Network Management Protocol (SNMP)

SNMP information can be gathered from Windows devices, non-Windows devices (for example, Linux, or UNIX), networking gear (for example, routers, or switches which are SNMP enabled) and printers.

How the Sensor Obtains SNMP Data

There are two SNMP commands that the Sensor on the customer network can send or receive to obtain information from an SNMP-enabled device:

- The **get** command collects statistics on SNMP devices by polling individual Object Identifiers (OID). Information collected via **get** is well suited for performance trending as the actual OID values are collected and maintained over time.
- The **trap** command is sent by the target device to the Sensor, and reports unusual events that occur on the device. The Sensor is capable of receiving SNMP traps that originate from devices.

Events generated by traps are better suited for exception management as very little trended information is maintained by the system.

Note: Either a Windows Sensor or a Hardware Sensor is required in the customer's network in order for SNMP-based metrics to be gathered. Agents do not gather SNMP based metrics.

Verifying SNMP on Remote Devices

(THIS SECTION IS FOR INFORMATIONAL PURPOSES ONLY. WE WILL CORRECT THIS ISSUE FROM THE TECH CENTER IF IT OCCURS.)

You should verify that the SNMP agent on the target device is properly configured. This can be accomplished using one of a number of freely available SNMP access tools. For example purposes, the tool Getif will be used.

Note: Getif is referenced in this document but MicroConvergent does not make or endorse this tool. It is simply included as a reference to assist partners.

After downloading (www.wtcs.org/snmp4tpc/getif.htm) and installing Getif on the Sensor, verify SNMP access to the remote device by supplying the device's IP address and its SNMP read community string. If the SNMP Sensor has been configured properly, you will receive a response from the device. On most devices, the default community string will be "public" (without the double-quotes).

If no response is received from the remote device, please consult the vendor's documentation for further assistance in enabling SNMP functionality and changing (verifying) the public community string. Once SNMP has been enabled and the response confirmed within Getif, you have successfully verified that SNMP functionality has been enabled.

Note: Not all SNMP-enabled devices provide all necessary metrics for all MicroConvergent SNMP-based services.



MicroConvergent, LLC
10752 Deerwood Park Blvd. South, Suite 100 | Jacksonville, FL 32256-4849
Office: 904.394.2980 | Fax: 904.394.2979 | Toll Free: 877.322.6967