The Local Windows Firewall is Enabled and Nothing can be Managed

This article describes the establishment of certain firewall rules relevant to the Windows firewall to permit remote management.

Windows systems ship with their local software-based firewall enabled out of the box. Unless the firewall is turned off or opened up a little, no remote management of such a system can occur.

While the firewall can be disabled, this is not always an option for many clients. The next logical choice is to open the firewall to permit management from the Privileged Identity host servers (console, deferred processors, zone processors) to the various sub-systems on a target Windows machine.

The following sub-sections refer to:

- Basic Management and Services - Account discovery, password change, Windows services
- Remote COM/DCOM
- Internet Information Services (IIS)
- Windows Scheduled Tasks

Basic Management and Services

Windows will permit some basic management while only opening up the remote administration port, port 445. Specific toPrivileged Identity, you will be able to:

- Perform a basic refresh of the target system
- Obtain a list of user accounts and their properties
- Manage passwords of local users
- Manage Windows services

The firewall rule will have these basic elements:

> ***Note:*** *For the purposes of the rules below, Privileged Identity refers to the machine(s) that run a management console or deferred/zone processor that performs management of the target Windows system.*

Friendly Name	Program to Allow	Local Address	Remote Address	Protocol	Local Port	Remote Port
Remote Management (SMB)	Any	Any	Privileged Identity	TCP	445	Any

Remote COM/DCOM

To remotely manage remote COM/DCOM on a Windows machine you can install the application server role and enable the option for **COM Network Access**. You can also modify the registry to achieve the same goal:

1. In the registry, locate and then click the following subkey: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\COM3**
2. Locate the key: **RemoteAccessEnabled**
3. Right-click **RemoteAccessEnabled**, and then click **Modify**.
4. In the **Edit DWORD** Value dialog box, type *1* , and then click **OK**.

Alternatively, a group policy can be used to make the same settings. Apply a group policy to the container in Active Directory that contains the target Windows systems.

1. Navigate through the group policy to: **Computer Configuration | Preferences | Windows Settings | Registry**.
2. Right-click and select **New | registry Wizard**.
3. Follow the Wizard to modify the following registry: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\COM3\RemoteAccessEnabled**
4. Once the policy is added, double-click the **RemoteAccessEnabledValue** and change **Value data** to: **00000001**.

In addition to enabling COM Network Access, you will also need to allow access through the firewall for the following two items from the Privileged Identity console/deferred processor or zone processors that will manage the target Windows servers:

> ***Note:*** *For the purposes of the rules below, Privileged Identity refers to the machine(s) that run a management console or deferred/zone processor that performs management of the target Windows system.*

Friendly Name	Program to Allow	Local Address	Remote Address	Protocol	Local Port	Remote Port
COM/DCOM In	%SystemRoot%\System32\dllhost.exe	Any	Privileged Identity	Any	Any	Any
COM Port Mapper In	Any	Any	Privileged Identity	TCP	135	Any

Internet Information Services (IIS) (Privileged Identity always or RPM during web site deployment)

For IIS 6 and 7+, the rules are slightly different and the process names have changed since Windows 2003 was released. In addition to allows the COM Port Mapper (port 135) you will also need to allow access to the IIS processes.

Friendly Name	Program to Allow	Local Address	Remote Address	Protocol	Local Port	Remote Port
IIS 6 Rmt Admin	%windir%\system32\inetsrv\iisrstas.exe	Any	Privileged Identity	Any	RPC Dynamic Ports	Any
IIS 7-8 Rmt Admin	%windi%\system32\inetsrv\inetinfo.exe	Any	Privileged Identity	Any	RPC Dynamic Ports	Any
COM Port Mapper In	Any	Any	Privileged Identity	TCP	135	Any

Windows Scheduled Tasks

Windows Scheduled tasks run under a different, albeit COM-based interface that is controlled by svchost.exe. Managing Windows Scheduled tasks will require three rules: one for the COM end point mapper, and two for scheduled tasks.

The firewall rule will have these three elements:

> ***Note:*** *For the purposes of the rules below, Privileged Identity refers to the machine(s) that run a management console or deferred/zone processor that performs management of the target Windows system.*

Friendly Name	Program to Allow	Local Address	Remote Address	Protocol	Local Port	Remote Port
Scheduled Tasks Management (RPC)	%systemRoot%\system32\svchost.exe	Any	Privileged Identity	Any	RPC Dynamic Ports	Any
Scheduled Tasks Management (RPC-EPMAP)	%systemRoot%\system32\svchost.exe	Any	Privileged Identity	Any	RPC Endpoint Mapper	Any
COM Port Mapper In	Any	Any	Privileged Identity	TCP	135	Any

Other Notes

If these policies are generated and applied through group policy, it may be up to a few hours before the policies apply to all machines, but there will be no need to restart any machines. If desired, on a target machine, from an administrative command prompt, one can run the following command to force group policies to update immediately: **gpupdate /force /target:computer**.